

Security Bulletin 30 September 2026

Generated on 30 September 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-2026-96257	A flaw has been found in Fast FAC1203R Gigabit Edition 2.0.4. Affected by this issue is the function copy_msg_element of the component Device Discovery Service. Executing a manipulation can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	10.0	More Details
CVE-2026-59167	SunEditor is a lightweight and powerful WYSIWYG editor in vanilla JavaScript with no dependencies. Prior to 2.47.11, the sanitizer in src/lib/core.js does not consistently reject namespaced or custom HTML elements, allowing event-handler attributes to remain on crafted elements. When an application renders attacker-controlled editor content and a user interacts with the element, the retained handler can execute script in the application's browser origin, enabling stored cross-site scripting, data exposure, or unauthorized browser-context actions. This issue is fixed in version 2.47.11.	10.0	More Details
CVE-2026-61732	Decepticon is an autonomous hacking agent for red teams. Versions prior to 1.1.17 wrap web crawl results — the output of agent reconnaissance against target services — into LLM messages without neutralizing ChatML special-token literals. Under the BYOK (Bring Your Own Key) deployment model, users configure their own LLM credentials to any OpenAI-compatible endpoint. Most open-source and self-deployed model providers (vLLM, SGLang, Ollama, LM Studio, text-generation-webui, etc.) do not filter special-token literals from user content in their default configurations. Those literals are parsed into structural role-boundary token IDs, meaning an attacker string planted in a target web page forges a new operator turn the model treats as authoritative, bypassing Decepticon's agent guardrails and resulting in arbitrary command execution inside the Kali Linux sandbox. Version 1.1.17 patches the issue.	10.0	More Details
CVE-2026-97359	HFS2 version 2.4.0 and earlier contains a template injection vulnerability in the multipart upload handler that allows unauthenticated attackers to achieve remote code execution by embedding malicious template syntax in a filename. Attackers can craft a filename containing a closing template quoting sequence followed by an exec macro, which bypasses the authorization check in the dispatcher to execute arbitrary commands on the underlying host system.	10.0	More Details
CVE-2026-86708	ZohoCorp ManageEngine Applications Manager versions 182200 and below were vulnerable to exposure of a Google Cloud service-account private key in the Applications Manager installer, which could allow an unauthenticated attacker to impersonate the service account and access or modify associated cloud resources.	10.0	More Details
CVE-2026-97360	HFS2 version 2.4.0 and earlier contains an unauthenticated arbitrary file access vulnerability that allows unauthenticated attackers to read, write, append, and delete files anywhere the HFS service account has filesystem access outside the shared folder. Attackers can exploit the macro dispatcher's lack of authorization model combined with the path resolver's failure to confine absolute paths to manipulate the template engine and compromise the confidentiality, integrity, and availability of the host.	10.0	More Details
CVE-2026-93577	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 19.2 before 19.2.7, 19.3 before 19.3.3, and 19.4 before 19.4.1 that under certain conditions could have allowed an authenticated user to execute arbitrary code on the GitLab server due to an integer overflow issue when compiling a specially crafted regular expression in a CI/CD configuration.	9.9	More Details
CVE-2026-77602	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. From 5.1.0 until 7.3.0, authenticated non-administrator users can write content under targets_modified/ that is later executed by multiple configuration paths below the intended code-execution privilege tier. Table and command or telemetry definitions are processed through ConfigParser, PacketConfig, GENERIC_READ_CONVERSION, or GENERIC_WRITE_CONVERSION, allowing ERB rendering or Ruby and Python evaluation, while openc3-cosmos-script-runner-api/scripts/run_suite_analysis.rb executes suite procedure files through require. Storage uploads, screen saves, and script creation can place content in the overlay, and triggering table processing, a cmd/tlm reload, or suite analysis executes the content in cmd-tlm-api, decom microservices, or Script Runner with access to internal credentials and data. This issue is fixed in version 7.3.0.	9.9	More Details
CVE-2026-	kyverno before 1.19.1 fails to properly validate URL-encoded path segments in Policy apiCall urlPath, allowing namespace tenants to bypass the per-namespace clamp and create objects in other namespaces as the admission-controller ServiceAccount. Attackers can exploit this by using percent-encoded directory traversal sequences to create	9.9	More Details

100706	MutatingWebhookConfiguration objects cluster-wide or PolicyException objects in the kyverno namespace, enabling privilege escalation to cluster admin.		
CVE-2026-84474	A flaw was found in Red Hat Ansible Automation Platform's automation- controller. The provisioning-callback secret (host_config_key) is exposed to users holding only the read-level view_jobtemplate permission -- both in the job template API representation and in the activity stream -- and the provisioning callback endpoint trusts a client-supplied X-Forwarded-For header to determine the calling host when the controller is deployed behind the AAP gateway with an empty proxy allow-list. By reading the secret and spoofing X-Forwarded-For to match any host in the job template's inventory, a minimally privileged or unauthenticated remote attacker can launch the job template against arbitrary managed hosts using the job template's credentials, resulting in privilege escalation and remote code execution on managed hosts.	9.9	More Details
CVE-2026-89078	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 19.2 before 19.2.7, 19.3 before 19.3.3, and 19.4 before 19.4.1 that under certain conditions could have allowed an authenticated user to execute arbitrary code on the GitLab server due to a double free issue when parsing a specially crafted regular expression in a CI/CD configuration.	9.9	More Details
CVE-2026-84502	A flaw was found in Red Hat Ansible Automation Platform's automation- controller. The Project scm_url field is not validated against values that begin with a dash and is stored and passed verbatim to the git SCM module. Because the module runs git ls-remote with the URL as a positional argument and without a "--" separator, a git project URL such as "--upload-pack=<command>:x" is interpreted by git as the --upload-pack option and executed via a shell. A user with permission to create or modify a project in a single organization can thereby execute arbitrary commands on the control-plane task pod, with output reflected through the project update stdout endpoint, leading to cross-tenant compromise and in-cluster lateral movement	9.9	More Details
CVE-2026-19599	ZohoCorp ManageEngine OpManager MSP versions 12.8.709 and below were vulnerable to a Remote Code Execution vulnerability in the Notification Profile module.	9.9	More Details
CVE-2026-100716	Froxlor is a server administration panel. In versions 2.3.10 and earlier, the customer data-export (DataDump) cron fails to validate intermediate path components of the export destination: Froxlor\FileDir::makeCorrectDir() contains an off-by-one in its path-component walk that skips the first segment below the customer home directory, and the guard in ExportCron.php checks only the final component with is_link(). An authenticated customer whose account has the export feature enabled can schedule an export into a genuine subdirectory of their own webspace, then replace an intermediate path component with a symlink before the root-owned cron runs. The cron's `chown -R` then recursively changes ownership of the linked directory tree — for example /etc — to the customer's UID, yielding host root and cross-tenant compromise. Exploitation is deterministic and requires no race. This is an incomplete fix of GHSA-75h4-... The issue is fixed in Froxlor 2.3.12.	9.9	More Details
CVE-2026-84719	A flaw was found in the Ansible Automation Platform automation-controller. When a WorkflowJobTemplate is copied, the deep-copy permission sanitizer validates only the inventory, unified_job_template, and credentials of each cloned node and fails to check the instance_groups (and execution_environment and labels) that were preserved from the original. A user with organization workflow-admin permission but no role on the referenced instance groups can copy a workflow, become its administrator, and launch jobs pinned to instance groups they are not authorized to use — including the control-plane instance group — bypassing the InstanceGroup use_role boundary and causing attacker-influenced automation to run in the control-plane execution context.	9.9	More Details
CVE-2026-100717	froxlor is a server administration panel. In versions 2.3.10 and earlier, Validate::validateUrl rejects carriage return and line feed characters only in the path, query and fragment components returned by parse_url, and never inspects the userinfo (user:pass@) components. This is an incomplete fix for GHSA-c3p2. An authenticated low-privilege customer with subdomain-create rights (no admin or change_serversettings privilege required) can supply a subdomain redirect URL that carries a CR/LF payload in the userinfo portion (e.g. http://user%0areturn 200 "pwned";%0a@evil.com/). The value passes validation, survives IDNA encoding, and is written verbatim into the generated nginx or Apache vhost configuration, allowing the attacker to break out of the emitted directive and inject arbitrary web-server configuration lines. froxlor regenerates and reloads the web-server configuration as root, so the injected directives take effect server-wide and can hijack responses or read local files. The issue is fixed in version 2.3.12.	9.9	More Details
CVE-2026-93425	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the patch.readRepoDirectories tRPC procedure passes the user-controlled repoPath value from apps/dokploy/server/api/routers/patch.ts into a shell command in packages/server/src/services/patch-repo.ts without safe argument quoting. An authenticated organization member with service:read permission can inject shell metacharacters into repoPath and execute arbitrary commands through child_process.exec as root in the Dokploy container. The supplied service identifier is used only to resolve the server and does not constrain repoPath. Because the standard deployment mounts /var/run/docker.sock, container-root command execution can be used to control Docker and compromise the host and its managed applications. This issue is fixed in version 0.29.13.	9.9	More Details
CVE-2026-19072	Velociraptor stores the compiled VQL in the hunt object internally to avoid having to recompile the artifacts for each endpoint in the hunt. Although the field "compiled_collector_args" is an internal field, Velociraptor allowed the field to be set from a user API call. This allows another user who can schedule a hunt (minimal role of "investigator") to set the compiled VQL statements for the hunt bypassing any ACL checks that would normally be applied. This flaw can then be escalated to allow the "investigator" user to run arbitrary VQL statements as an administrator user on the Velociraptor server.	9.9	More Details
CVE-2026-100075	In the Linux kernel, the following vulnerability has been resolved: RDMA/srpt: Fix srpt_alloc_rw_ctxs() unwind counters When srpt_alloc_rw_ctxs() fails partway through a multi-buffer indirect descriptor, the unwind path destroys RDMA contexts but leaves stale n_rw_ctx and n_rdma values (and a dangling rw_ctxs pointer). Later sq_wr_avail accounting in srpt_queue_response() or srpt_write_pending() can then subtract the wrong number of send queue credits. Reset the counters and clear rw_ctxs after freeing the heap allocation before returning an error.	9.8	More Details
CVE-2026-12227	The Visual Composer Website Builder plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 45.16.0 via the `vcv-template` parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary 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 images and other “safe” file types can be uploaded and included.	9.8	More Details
CVE-2026-78308	Improper Authentication vulnerability in DIAEnergie allows Authentication Bypass. This issue affects DIAEnergie: before 1.11.00.022.	9.8	More Details
CVE-2026-96891	A vulnerability was identified in D-Link DIR-825 3.00b32. Affected is the function tunnel_set_params of the file tunnel.c of the component rp-i2tp. The manipulation of the argument peer_hostname leads to out-of-bounds write. The attack may be initiated remotely.	9.8	More Details
	The Paytium: Mollie payment forms & donations plugin for WordPress is vulnerable to Privilege Escalation in all versions up to,		

CVE-2026-18467	and including, 5.0.3. The 5.0.3 patch introduced a wp_hash()/hash_equals() signature gate on the pt-paytium-user-data field, but left a second filter — pt_cf_checkout_meta(), registered on the pt_meta_values hook after the signed builder — that copies every \$_POST['pt_form_field'][*] key verbatim into the payment meta array without any signature verification; this allows the pt-user-role value it copies to overwrite the signed path's output, after which paytium_user_data_processing() reads the persisted _pt-user-role post meta and passes it directly as the role argument to wp_insert_user(). This makes it possible for unauthenticated attackers to register a new WordPress account with the administrator role and fully take over the site. Exploitation requires submitting a payment through a publicly-exposed [paytium] shortcode form and completing the resulting payment flow, after which the attacker can seize the new administrator account via the standard lost-password flow on their supplied email address.	9.8	More Details
CVE-2026-82901	The Ultra Addons for Contact Form 7 plugin for WordPress is vulnerable to Arbitrary File Upload due to insufficient file type validation in the 'uacf7_wpcf7_mail_components' function in all versions up to, and including, 3.5.50. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. Note: This is only exploitable when the plugin's PDF Generator module is enabled, which is disabled by default.	9.8	More Details
CVE-2026-82331	Improper link resolution before file access ('link following') vulnerability in the `tar` source plugin of Apache BuildStream running on Python < 3.12 allows malicious source tarballs to write files on the host, with the privileges of the user running BuildStream, via symlinks as part of source fetching. The impact of this issue is mitigated by: * BuildStream projects should only use trusted sources in their elements as otherwise the build output can also not be trusted * Tracking a source tarball pins its SHA256 hash, which prevents MITM attacks of users that are fetching an already tracked project * When running on Python >= 3.12, BuildStream >= 2.3.0 already makes use of the Python `tarfile` filter functionality, which blocks the symlink escape Users are recommended to upgrade to version 2.8.1, which fixes this issue.	9.8	More Details
CVE-2026-14281	The Automation Web Platform – Notifications and OTP for WooCommerce, Advanced Country Code plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 4.8.6. This is due to missing permission enforcement on the publicly accessible REST route `POST /wp-json/wawp/v1/signup/<op>` and the absence of a key allowlist in the `finish_registration_logic` function, which copies the attacker-controlled `wawp_custom_fields` parameter directly into `update_user_meta()` — allowing sensitive meta keys such as `wp_capabilities` and `wp_user_level` to be set by the caller. This makes it possible for unauthenticated attackers to register a new account with the administrator role and gain full administrative access to the site. When OTP verification is enabled at signup, the OTP session token (`otp_transient`) is returned in plaintext in the HTTP response body, and the `handle_magic_link_request()` handler marks that token as verified on any unauthenticated GET request containing it without ever checking the OTP code value — making the OTP step trivially bypassable with no inbox or SMS access required.	9.8	More Details
CVE-2026-51996	An issue in geelen mcp-remote 0.1.16 through 0.1.38 allows a remote attacker to execute arbitrary code via the src/lib/utls.ts and the getServerUrlHash function	9.8	More Details
CVE-2026-88351	An integer overflow vulnerability exists in the MPack Node API in MPack 1.1.1 on 32-bit platforms. When parsing a specially crafted MessagePack array32 or map32 object with an excessively large element count, the page allocation size calculation in mpack_tree_parse_array32() can overflow size_t and produce an undersized allocation. Subsequent parsing writes mpack_node_data_t records beyond the allocated heap buffer, resulting in heap-buffer-overflow, memory corruption, and denial of service.	9.8	More Details
CVE-2026-88365	minimp3 commit ea99364f contains an integer overflow vulnerability in mp3dec_skip_id3v1() when parsing the APEv2 tag-size field.	9.8	More Details
CVE-2026-93207	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: Zero rpc_gss_wire_cred at svcauth_gss_decode_credbody() entry svcauth_gss_decode_credbody() writes the caller's rpc_gss_wire_cred field by field and assigns gc_ctx.len only on the success tail. The caller storage is svcddata->clcred, which lives in the per-svc_rqst gss_svc_data and is reused across requests. Early decode failures leave partially decoded state mixed with residue from the prior request. The trailing body_len tightness check is the sharpest case: xdr_stream_decode_opaque_inline() has already written gc_ctx.data with a borrowed inline pointer into the current request's XDR pages, but gc_ctx.len retains its prior value. Once the request pages are released the pooled clcred carries a dangling pointer paired with a stale length. Zero the caller's rpc_gss_wire_cred at function entry so that every early-return path leaves a deterministic all-zero cred. On the trailing tightness-check path, gc_ctx.len is now zero instead of stale, which neuters length-driven consumers such as gss_svc_searchbyctx() that would otherwise walk the dangling data pointer.	9.8	More Details
CVE-2026-97230	IO::Socket::SSL::SelfCertificate versions 1.00 for Perl contains malware which executes Python code from an obfuscated URL. The generate_certificate runs a Python script saved as a certificate file. The python script attempts to retrieve code from a hardcoded http URL that is obfuscated with base64 encoding and run the response body directly. The impact is that arbitrary code can be invoked as the user, without a dropped script being saved on the affected host. The releases have no test scripts nor build hooks. The intention may have been to trigger the payload after installation. The dropper script is in lib/Crypt/SelfCertificate/sample/cert.pem. This is similar to CVE-2026-95831 for the module Crypt::SelfCertificate. The SHA-256 digests of the files are ba24ee8ec3b7f47f65bed62e16fb413ace50653cf44bd8ea90914390922831e0 IO-Socket-SSL-SelfCertificate-1.00.tar.gz 821d38830e5eb8607738421c25ac25f59fff02a6ab67daa32fbd020429454dac IO-Socket-SSL-SelfCertificate-1.00/lib/IO/Socket/SSL/SelfCertificate/sample/cert.pem d483cb7b23b7271cb11cf242bff4a2e1c02df0b9525eb0429abeea8961c399d5 IO-Socket-SSL-SelfCertificate-1.00-upload.tar.gz	9.8	More Details
CVE-2026-88378	QuickJS commit 04be24600 contains a heap out-of-bounds write condition in JS_ReadFunctionTag().	9.8	More Details
CVE-2026-92609	Session fixation in HTTP management authentication allows remote attackers to gain unauthorized access to an authenticated management session via reuse of a session identifier retained across successful authentication. This issue affects Apache Qpid Broker-J: through 10.1.0. Users are recommended to upgrade to version 10.1.1, which fixes the issue.	9.8	More Details
CVE-2026-6730	IBM Concert 1.0.0 through 3.0.0 is vulnerable to a buffer overflow, caused by improper bounds checking. A local user could overflow the buffer and execute arbitrary code on the system.	9.8	More Details
CVE-2026-93352	Laravel-Mediable 7.0.0 before 7.0.2 contains an incomplete patch for CVE-2026-49972 in which the .pht extension is absent from the forbidden_extensions blacklist in config/mediable.php. The blacklist introduced to address CVE-2026-49972 includes phpt but omits pht, which Apache executes as PHP via the default FilesMatch directive on Debian and Ubuntu systems. An attacker can upload a .pht file that passes all validation in MediaUploader::verifyExtension() and File::sanitizeFileName() because pht is not present in the blacklist, causing the file to be written to disk and executed as PHP when requested, enabling remote code execution with the privileges of the web server process.	9.8	More Details
CVE-2026-	orval before 8.29.0 fails to escape OpenAPI media-type keys when emitting them into single-quoted Content-Type string literals in generated code. Attackers can inject JavaScript through crafted media-type keys in OpenAPI specifications that executes	9.8	More Details

96757	when generated fetch operations or mock resolvers are invoked.		
CVE-2026-85984	The miniOrange OTP Login, Verification and SMS Notifications plugin for WordPress is vulnerable to Authentication Bypass via the <code>mo_wp_login_intent</code> parameter in all versions up to, and including, 5.5.5. This is due to a missing password-intent guard in the <code>skip_pass_fallback</code> -enabled configuration branch of the <code>mo_by_pass_login()</code> function, which treats administrator role membership alone as sufficient authentication whenever the unauthenticated, unverified POST parameter <code>mo_wp_login_intent</code> is submitted with the value <code>otp</code> , causing <code>mo_get_user()</code> to skip <code>wp_authenticate_username_password()</code> and resolve a <code>WP_User</code> purely from a username lookup. This makes it possible for unauthenticated attackers to log in as any existing administrator account by supplying only a known username and an empty password alongside <code>mo_wp_login_intent=otp</code> , with no password or OTP verification required. Exploitation is conditional on a site administrator having simultaneously enabled the following plugin options: WP Login OTP, Login with Only OTP, Allow Users to Login with Username and Password, and Admin OTP Bypass.	9.8	More Details
CVE-2026-86248	CLIENT_CERT authentication does not fail as expected for some scenarios when soft fail is disabled vulnerability in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M14 through 11.0.25, from 10.1.22 through 10.1.59, from 9.0.92 through 9.0.121. Users are recommended to upgrade to version 11.0.26, 10.1.60 or 9.0.122, which fix the issue.	9.8	More Details
CVE-2026-76183	Authentication Bypass by Alternate Name vulnerability in Apache Tomcat allowed the security constraints for any WebSocket endpoint to be bypassed. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.25, from 10.1.0-M1 through 10.1.59, from 9.0.0.M1 through 9.0.121. The following versions were EOS at the time the CVE was created but are known to be affected: from 8.5.0 through 8.5.100, from 7.0.43 through 7.0.109. Other unsupported versions may also be affected. Users are recommended to upgrade to version 11.0.26, 10.1.60 or 9.0.122, which fix the issue.	9.8	More Details
CVE-2026-96560	LightLLM through 1.2.0 contains a remote code execution vulnerability in the KV-transfer worker when started with <code>--pd_trans_mode nccl</code> , which exposes an unauthenticated RPyC control channel that deserializes attacker-supplied data. Attackers can send malicious pickled objects to the exposed RPyC ThreadedServer to execute arbitrary code with the privileges of the LightLLM service account.	9.8	More Details
CVE-2025-63564	SQL injection vulnerability in Moodle Socialwall plugin v.3.0 through v.3.3 allows an attacker to execute arbitrary code via crafted HTTP requests	9.8	More Details
CVE-2026-96754	orval versions before 8.29.0 contain a code injection vulnerability in the <code>@orval/hono</code> generator that fails to escape OpenAPI path values in single-quoted route literals. Attackers can craft an OpenAPI document with an apostrophe in a static path segment to inject arbitrary JavaScript code that executes when the generated TypeScript module is imported.	9.8	More Details
CVE-2026-6928	IBM Concert 1.0.0 through 3.0.0 references or accesses memory after it has been freed. This allows an attacker who can influence program execution or input may exploit this condition to corrupt memory, cause application crashes, or execute arbitrary code.	9.8	More Details
CVE-2026-96755	orval versions 8.14.0 through 8.28.1 contain a code injection vulnerability in the <code>@orval/effect</code> generator that converts OpenAPI schema defaults into template literals. Attackers can inject arbitrary JavaScript expressions via schema defaults containing <code>\${...}</code> syntax, which are executed at module scope when the generated code is built or imported.	9.8	More Details
CVE-2026-96758	orval <code>@orval/core</code> before 8.28.0 contains a code injection vulnerability in the form-data serializer that fails to escape multipart property names in generated template literals. Attackers can inject <code>\${...}</code> expressions into OpenAPI schema property names that execute as live interpolation when the generated client builds FormData bodies with consumer process privileges.	9.8	More Details
CVE-2026-96759	orval before 8.29.0 fails to escape the <code>operationId</code> parameter when emitting it into generated TanStack Query mutator options metadata objects. Attackers can inject arbitrary JavaScript code through a crafted <code>operationId</code> in an OpenAPI specification that executes when generated hooks are called.	9.8	More Details
CVE-2026-18143	The Request a Quote for WooCommerce plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 2.9.2 via the <code>`afrfq_submit_quote_via_popup()`</code> function. This is due to missing file extension and MIME type validation in the popup upload handler, which uses the raw attacker-supplied filename directly as the destination for <code>`move_uploaded_file()`</code> . This makes it possible for unauthenticated attackers to upload executable files, such as PHP files, to a web-accessible temporary RFQ upload directory when a public quote rule with the multi-page popup flow is enabled.	9.8	More Details
CVE-2026-92161	FriendsOfFlarum OAuth allows users to log in to Flarum with GitHub, Twitter, Facebook, and other providers. Prior to 1.7.4 and 2.0.0-beta.4, the Discord OAuth provider does not check the verified field returned for an OAuth email before passing the address to Flarum core as trusted through <code>provideTrustedEmail()</code> . When Discord sign-in is enabled, an unauthenticated attacker who knows the email address of a Flarum user can configure a Discord account with that unverified address and a verified phone number, then sign in to cause Flarum to match the trusted address, link the attacker-controlled Discord identity to the existing user, and authenticate as the victim without a password or victim interaction. Exploitation requires that the victim's email address is not already associated with a Discord account, or it can compromise administrator accounts. Other bundled providers were not confirmed to be practically exploitable by this method because their relevant authentication flows return only verified or confirmed email addresses. This issue is fixed in versions 1.7.4 and 2.0.0-beta.4.	9.8	More Details
CVE-2026-93643	When OnlyOffice/Document Editing is available, an unauthenticated remote attacker with access to an existing supported public Briefcase document can abuse unsigned save fields to perform path-traversal writes and execute commands as zimbra.	9.8	More Details
CVE-2026-6721	IBM Concert 1.0.0 through 3.0.0 allows an unauthenticated remote attacker can supply specially crafted input that is incorporated into OS commands, resulting in arbitrary command execution on the underlying system. Successful exploitation allows remote code execution with the privileges of the affected application.	9.8	More Details
CVE-2026-13249	An unauthenticated Remote Code Execution via Arbitrary File Upload vulnerability in the web management interface in Honeywell PD45 Industrial Printer version F10.19.010040, allows upload of attacker controlled files without requiring authentication. An attacker could potentially exploit this vulnerability, leading to the execution of malicious files and commands. Honeywell also recommends updating to the most recent firmware version, Honeywell PD45 Industrial Printer firmware F10.22.030745, which includes a fix for this vulnerability.	9.8	More Details
CVE-2026-97413	In the Linux kernel, the following vulnerability has been resolved: RDMA/rtrs-srv: Fix integer underflow in <code>process_read</code> and <code>process_write</code> <code>usr_len</code> is read from a network-supplied message field (<code>le16_to_cpu</code>) and used to compute <code>data_len = off - usr_len</code> without validating that <code>usr_len <= off</code> . A malicious RDMA client can send <code>usr_len > off</code> causing an integer underflow, resulting in <code>data_len</code> wrapping to a huge <code>size_t</code> value which is then passed to the <code>rdma_ev</code> callback as a memory length, leading to out-of-bounds memory access. Fix by reading and validating <code>usr_len <= off</code> before <code>rtrs_srv_get_ops_ids()</code> in both <code>process_read()</code> and <code>process_write()</code> , ensuring the early return path acquires no reference and has no resource leak.	9.8	More Details
	Froxlор through 2.3.10 is vulnerable to arbitrary file deletion via symlink following in the FTP data deletion cron task. Cron task 8		

CVE-2026-100715	(deleteFtpData), queued when an FTP account is deleted, calls FileDir::makeCorrectDir() without the \$fixed_homedir argument, so the symlink component walk is skipped, and then executes 'rm -rf' as root on the resulting path with string-level guards only. Because makeCorrectDir() appends a trailing slash, GNU rm dereferences a symlink used either as an intermediate path component or as the final component. An authenticated customer who can write to the FTP home directory can plant a symlink between task insertion and cron execution, causing the root cron job to recursively delete arbitrary directory trees, resulting in cross-tenant data destruction and host denial of service. This issue is fixed in Froxlor 2.3.12.	9.6	More Details
CVE-2026-95699	Prior to 9/18/2026, the iSteamX mobile application's AWS policy could grant authenticated users access to wildcard MQTT topics, which can expose other users' device data and allow the attacker to start and stop other connected users' devices. This risked exposing user profile information and potential scalding due to unintended device activation.	9.6	More Details
CVE-2026-81549	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to obtain sensitive information due to improper validation of the X-Forwarded-Proto header.	9.6	More Details
CVE-2026-85724	Moquette is a lightweight Java MQTT broker. Prior to 0.18.1, when pattern-based ACL rules are configured, AuthorizationsCollector.canDoOperation substitutes client ID and username values directly into rules containing %c or %u and then treats the result as an MQTT topic filter. A client that uses + or # in either identity can broaden the substituted filter and gain cross-tenant read and write access. A # identity can also produce an invalid filter that triggers a NullPointerException in Topic.match and disrupts session processing. This issue is fixed in version 0.18.1.	9.6	More Details
CVE-2026-93291	Omni C20 lacks proper certificate validation which could allow an attacker to perform a man-in-the-middle attack which could allow them to execute arbitrary code.	9.4	More Details
CVE-2026-61741	http4s-scala-xml provides `EntityDecoder[F, scala.xml.Elem]` instances that parse XML message bodies. Prior to versions 0.24.1 and 1.0.0-M39, these decoders used a `javax.xml.parsers.SAXParserFactory` obtained from `SAXParserFactory.newInstance` without any security configuration. With the JDK's default settings, the parser resolves DOCTYPE declarations, external general and parameter entities, and external DTDs. An application that uses these decoders to parse untrusted XML is vulnerable to XML External Entity (XXE) attacks. An attacker can craft a request that discloses local files readable by the service process, performs server-side request forgery (SSRF) against internal network resources, and/or causes denial of service through entity expansion. Versions 0.24.1 and 1.0.0-M39 fix the issue.	9.3	More Details
CVE-2026-93641	An unauthenticated sender can forge a share notification that triggers stored XSS when a signed-in Zimbra Classic recipient clicks Accept Share, allowing the attacker to access mailbox data and act as the victim.	9.3	More Details
CVE-2026-18872	IBM Financial Transaction Manager (FTM) for RedHat OpenShift is vulnerable to stored cross-site scripting (CWE-79) in the FTM UI NetworkAcknowledgement React component (NetworkAcknowledgement.jsx:42). A malicious actor can inject script into stored network acknowledgement data that executes in authenticated operator browsers, enabling session hijacking and unauthorized operator-level payment actions.	9.3	More Details
CVE-2026-95601	Unauthenticated SQL Injection in Product Filter by WBW <= 3.1.7 versions.	9.3	More Details
CVE-2026-93642	An unauthenticated sender can forge a share notification that triggers stored XSS when a signed-in Zimbra Modern recipient clicks Accept Share, allowing the attacker to access mailbox data and act as the victim.	9.3	More Details
CVE-2026-93647	An unauthenticated calendar sender can place active markup in a COUNTER message's RFC From address. Selecting the message in Zimbra Classic triggers stored XSS, allowing the attacker to access mailbox data and act as the victim.	9.3	More Details
CVE-2026-89055	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.120.0. 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 permanently delete arbitrary attachments from the Media Library — including administrator-owned product images, logos, and documents — by injecting their IDs into a review that is later trashed and purged. Exploitation requires a public review-form link (a 13-hex formId distributed to customers via e-mail), which exposes the nonce needed to reach the handler without any WordPress account or session.	9.1	More Details
CVE-2026-93399	The Bookly plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 28.2 via the 'bookly_get_form_id', 'bookly_render_complete', 'bookly_add_to_calendar' and 'bookly_rollback_order' AJAX actions. This is due to the 'bookly_get_form_id' handler blindly storing the attacker-controlled 'order_id' from the submitted form_data into a new booking session, which the 'bookly_render_complete' handler then trusts to look up and return the corresponding Order's secret token without verifying that the current session created that order. This makes it possible for unauthenticated attackers to enumerate sequential order IDs, disclose other customers' order tokens, retrieve calendar/appointment information via 'bookly_add_to_calendar' and permanently delete arbitrary non-completed bookings via 'bookly_rollback_order', which cascade-deletes the customer_appointment and (when no other customers are attached) the underlying appointment.	9.1	More Details
CVE-2026-86246	Initialization of a resource with an insecure default vulnerability in Apache Tomcat Native enabled insecure options by default including ALLOW_CLIENT_RENEGOTIATION, NO_EXTENDED_MASTER_SECRET, IGNORE_UNEXPECTED_EOF and ALLOW_NO_DHE_KEX. This issue affects Apache Tomcat Native: from 2.0.0 through 2.0.15, from 1.3.0 through 1.3.8. Earlier unsupported versions may also be affected. Users are recommended to upgrade to version 2.0.16 or 1.3.9, which fix the issue.	9.1	More Details
CVE-2026-79766	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. From 2.4.1 until 2.5.1, an authenticated Termix administrator can store attacker-controlled domain and email values through PATCH /users/acme-ssl-settings and trigger their interpolation into a certbot shell command through POST /users/acme-ssl-request. In src/backend/database/routes/acme-ssl-routes.ts, child_process.execSync invokes /bin/sh -c with those values only wrapped in double quotes, so shell metacharacters can execute arbitrary operating-system commands as the Termix backend process. Both HTTP webroot and DNS Cloudflare challenge modes are affected, and compromise exposes Termix databases, process secrets, stored credentials, and network reachability. This issue is fixed in version 2.5.1.	9.1	More Details
CVE-2026-93228	In the Linux kernel, the following vulnerability has been resolved: svcrdma: Reject Write/Reply chunks with segcount 0 A peer can send a Write or Reply chunk whose segcount field is zero. xdr_check_write_chunk() only rejects segcount > rc_maxpages, so zero passes the range check, and xdr_inline_decode(stream, 0) returns the current (non-NULL) cursor without advancing. The function returns true and pcl_alloc_write() then links a struct svc_rdma_chunk with ch_segcount == 0 onto rc_write_pcl or rc_reply_pcl. An earlier patch in this series made pcl_for_each_segment() safe for ch_segcount == 0, so this no longer drives the memory walk it used to. Rejecting the malformed frame at the decode boundary is still worthwhile as defense in depth: it keeps degenerate zero-segment chunks off the parsed chunk lists entirely, so any future consumer that walks ch_segments directly cannot observe one, and it makes the zero-floor easy to backport to trees where the macro change is more intrusive. RFC 8166 has no meaning for a Write/Reply chunk that describes no remote buffer, so no legitimate client is affected.	9.1	More Details

	xdr_check_reply_chunk() funnels Reply chunks through xdr_check_write_chunk() and inherits the same rejection. pcl_alloc_write() also links each chunk onto the parsed chunk list before filling its segment array. If a future change weakens the segcount-0 rejection, an incomplete chunk is visible to consumers during the fill loop. Reorder so that list_add_tail() follows the segment fill loop, ensuring only fully-populated chunks appear on the list.		
CVE-2026-95848	Moquette is a lightweight Java MQTT broker. Prior to 0.18.1, when a configured authenticator or authorizer class cannot be loaded, Server.initializeAuthenticator and Server.initializeAuthorizerPolicy treat the failure as though no custom class was configured and fall back to AcceptAllAuthenticator or PermitAllAuthorizerPolicy. A misspelled class name, missing dependency, constructor failure, or classpath problem can therefore start the broker with authentication or authorization disabled even though the operator configured those controls. This issue is fixed in version 0.18.1.	9.1	More Details
CVE-2026-100714	Froxlor before 2.3.12 does not restrict or escape the system.letsencryptchallengepath setting: unlike sibling settings hardened in GHSA-33mp, the field has no string_regexp or required_otp guard, and its value is concatenated unescaped into the acme.sh command line built in lib/Froxlor/Cron/Http/LetsEncrypt/AcmeSh.php and executed by the root cron via FileDir::safe_exec. Because safe_exec only blacklists shell metacharacters such as ; & > \ \$ ~ ? , spaces and quotes survive and the value is word-split into additional acme.sh arguments. An administrator, or any actor able to write settings (for example through the settings-import API), can therefore inject acme.sh options such as --renew-hook, --pre-hook or --post-hook to obtain arbitrary command execution as root at the next Let's Encrypt cron run, or use --config-home/--cert-home for arbitrary file writes. Versions up to and including 2.3.10 are affected; the issue is fixed in 2.3.12.	9.1	More Details
CVE-2026-86930	An out-of-bounds read vulnerability in FileMaker Server for Linux allowed an attacker uploading a specially crafted image file to a container field to disclose process memory during thumbnail generation in FileMaker WebDirect. This vulnerability is addressed in FileMaker Server version 26.0.3.	9.1	More Details
CVE-2026-86934	An authorization bypass vulnerability in the FileMaker Server Web Publishing Engine allowed requests containing an extended privilege header to bypass the disabled Custom Web Publishing with XML setting and access the XML Web Publishing interface. This vulnerability is addressed in FileMaker Server version 26.0.3.	9.1	More Details
CVE-2026-97064	X-SpringBoot through 6.0 ships with a hardcoded static master login verification code 172839 enabled by default in the database seed. Unauthenticated attackers can authenticate as any user by submitting the public master code to the emailOrMobileLogin endpoint with a known email or mobile number.	9.1	More Details
CVE-2026-97063	X-SpringBoot through 6.0 returns login verification codes in HTTP responses from unauthenticated endpoints GET /sys/mobile/code and GET /sys/email/code without sending them to account owners. Attackers can request codes using known mobile numbers or email addresses, read them from responses, and authenticate as victims via POST /sys/emailOrMobileLogin/login to hijack accounts.	9.1	More Details
CVE-2026-92288	Lemonldap::NG::Portal versions from 2.20.0 before 2.21.6, from 2.22.0 before 2.23.4 for Perl allow unauthenticated OAuth2 token introspection because checkEndPointAuthenticationCredentials does not verify the client secret of a public Relying Party. checkEndPointAuthenticationCredentials() skips the secret comparison for a Relying Party marked public and still returns the authentication method deduced from the request, client_secret_basic or client_secret_post. introspection() rejects a caller only when that method is missing or none, so a request carrying a public client_id and an arbitrary or empty secret passes the endpoint's authentication check. An attacker who holds an access token and knows the client_id of any public Relying Party can confirm the token is active and read its metadata, including scope, audience, expiry and the sub claim. The sub claim is computed with the calling Relying Party's user identifier attribute, so an attacker can translate a user identifier from one Relying Party to another, defeating per-client and pseudonymous identifiers.	9.1	More Details
CVE-2026-62262	Piwigo is a full featured open source photo gallery application for the web. In 17.0.0beta1 and earlier, when rating is enabled, an unauthenticated guest can call pwg.images.filteredSearch.create with a crafted ratings[] value and then open the returned search URL. include/ws_functions/pwg.images.php stores the unvalidated value in the search rules, and include/functions_search.inc.php integer-casts only the lower rating bound while concatenating the raw value as the SQL upper bound. This allows error-based or blind extraction of database information and database-dependent time delays through the public search flow. No fixed version is available as of this review.	9.1	More Details
CVE-2026-42322	Piwigo is a full featured open source photo gallery application for the web. Prior to 16.4.0, admin/themes_standard_pages.php validates uploaded logo content by MIME type but reuses the attacker-controlled extension from std_pgs_logo when constructing the stored filename. An authenticated administrator can upload image content with a server-executable final extension, causing the file to be placed in the web-accessible logo directory and executed when requested if the web server handles that extension. This can permit arbitrary command execution, data disclosure, modification, persistence, and service disruption. This vulnerability is fixed in 16.4.0.	9.1	More Details
CVE-2026-39353	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. Prior to 1.7.2-rc-1, InvoicePlane builds its permitted template list by scanning a PHP template directory that can be written through an administrator-controlled file-write capability. A malicious PHP file placed in the directory is automatically trusted by Mdl_templates and can be selected as public_invoice_template. When a public invoice is rendered, the guest View controller includes the trusted file and executes it with web-server privileges. This issue is fixed in version 1.7.2-rc-1.	9.1	More Details
CVE-2026-75884	A flaw was found in AWX. The container group pod_spec_override field uses an incomplete blocklist that only restricts automountServiceAccountToken, allowing injection of initContainers, serviceAccountName overrides, and projected service account token volumes. An AAP platform administrator can exploit this to escalate privileges to OpenShift namespace-level access and exfiltrate namespace secrets.	9.1	More Details
CVE-2026-92289	Lemonldap::NG::Portal versions from 2.23.0 before 2.23.4 for Perl allow a PKCE bypass for public Relying Parties in "PKCE or secret" mode because checkEndPointAuthenticationCredentials does not verify the client secret. With oidcRPMetaDataOptionsRequirePKCE set to 2, the authorization endpoint issues a code even when the request carries no code_challenge, and token() admits the exchange as long as a challenge was stored or an authentication method was returned for the caller. checkEndPointAuthenticationCredentials() skips the secret comparison for a Relying Party marked public and still returns the method deduced from the request, so any Basic or form credential satisfies the secret branch. validatePKCEChallenge() then passes, because neither a challenge nor a verifier is present. An attacker who intercepts an authorization code issued to a public Relying Party can exchange it for the user's access, ID and refresh tokens by replaying the client_id with an arbitrary secret, which is the attack PKCE prevents. Dynamic client registration creates every Relying Party in this mode.	9.1	More Details
CVE-2026-51994	mcp-remote versions 0.1.32 through 0.1.38 are vulnerable to Server-Side Request Forgery (SSRF) via the resource_metadata URL extracted from a remote MCP server's WWW-Authenticate header	9.1	More Details
CVE-2026-			

78312	Path Traversal in DIAEnergie. This issue affects DIAEnergie: before 1.11.00.022.	9.1	More Details
CVE-2026-86350	Inconsistent interpretation of HTTP/2 requests ('HTTP Request/Response smuggling') vulnerability in Apache Tomcat caused by a regression in fix for CVE-2026-41293 can trigger request header mix-up. This issue affects Apache Tomcat: from 11.0.22 through 11.0.25, from 10.1.55 through 10.1.59, from 9.0.118 through 9.0.121. Users are recommended to upgrade to version 11.0.26, 10.1.60 or 9.0.122, which fix the issue.	9.1	More Details
CVE-2026-82843	The WP OAuth Server (Login with WordPress) WordPress plugin before 6.4.0 does not bind the OpenID Connect identity assertion it issues to the authorization grant being exchanged, returning instead the assertion belonging to whichever user authenticated most recently, which allows users with the Subscriber role and above to obtain a validly signed identity assertion for another user, including an administrator, and authenticate as them at any application that uses the site for single sign-on.	9.0	More Details
CVE-2026-75799	The YAHMAN Add-ons WordPress plugin before 0.9.31 does not validate the type of the remote files it caches in a publicly accessible directory, allowing unauthenticated attackers to write arbitrary PHP files on the server and achieve RCE when the relevant feature is enabled.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	
CVE-2026-94606	authentik is an open-source identity provider. Prior to 2026.2.7, 2026.5.7, and 2026.8.2, authentik email authenticator enrollment during an authentication or enro
CVE-2026-97957	In the Linux kernel, the following vulnerability has been resolved: net: hinic: fix mailbox segment buffer overflow check_mbox_seq_id_and_seg_len() validates that :
CVE-2026-97555	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix heap overflow in DACL owner/group rewrite When id_mode_to_cifs_acl rewrites an KASAN: slab-out-of-bounds in build_sec_desc+0x1e8a/0x2680 [cifs] Write of size 4 at addr ffff8881a5e25374 by task chown/5298 ... The buggy address is located (
CVE-2026-97442	In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: fix invalid data access in ath11k_dp_rx_h_undecap_nwifi In certain cases, hardware i QCAHSPSWPL_V1_V2_SILICONZ_IOE-1
CVE-2026-81545	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to execute arbitrary commands due to improper neutralization of special
CVE-2026-100639	SiYuan v3.8.3 fails to HTML-escape the data-subtype attribute when generating gutter-button markup (app/src/protyle/gutter/button.ts, assigned via innerHTML in i
CVE-2026-81547	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to execute arbitrary commands due to path traversal.
CVE-2026-80423	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to obtain sensitive information due to the exposure of namespace-wide s
CVE-2026-81548	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to execute arbitrary commands due to improper neutralization of special
CVE-2026-100670	Grav CMS 2.0.14 through 2.0.24 contains a privilege escalation vulnerability in the group and account blueprints. The access map is gated by a `security@: admin.
CVE-2026-81552	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to execute arbitrary commands due to improper neutralization of environor
CVE-2026-82093	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to execute arbitrary code due to unsafe deserialization of untrusted data
CVE-2026-93834	A use-after-free vulnerability was found in QEMU's 9pfs subsystem. A race condition between the main thread and a worker thread when processing concurrent Tlc
CVE-2026-18490	IBM Financial Transaction Manager (FTM) for RedHat OpenShift is vulnerable to unauthenticated remote code execution via Java native deserialization on the PayDi
CVE-2026-93799	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: validate sta_id in BA window status notif BA_WINDOW_STATUS_NOTIFICATION_
CVE-2026-93806	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: validate assoc response length before status and IE access cfg80211_rx_assoc_re:
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Unlink NVMe unsol ctx before freeing on LS reject error qla_nvme_xmt_ls_rsp() obt

CVE-2026-100679	stoatchat before 0.15.5 fails to validate that MFA tickets belong to the authenticated user, allowing attackers to bypass MFA by using their own valid ticket with an
CVE-2026-100520	Laranode versions before 1.2.1 contain a path traversal vulnerability in the POST /filemanager/upload-file endpoint that allows authenticated users to write arbitrary
CVE-2026-80425	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to execute arbitrary commands due to improper neutralization of special
CVE-2026-100682	Budibase Server before 3.45.0 contains an arbitrary file write vulnerability in the PWA icon upload endpoint that extracts user-supplied ZIP archives without proper
CVE-2026-96795	Horilla is an HR and CRM software. Prior to 2.0.0, HorillaListView.export_data in horilla_views/generic/cbv/views.py accepts an authenticated user's columns POST p
CVE-2026-81539	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to execute arbitrary code due to improper neutralization of special elements
CVE-2026-81537	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to execute arbitrary code due to OS command injection.
CVE-2026-97509	In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Keep XDomain reference during the lifetime of a service This is needed because we
CVE-2026-100544	openclaw's @openclaw/voice-call package before 2026.8.1 launches the configured agent for classic inbound voice calls without propagating the caller's identity or
CVE-2026-93349	Frictionless before 5.19.1 contains an OS command injection vulnerability in the explore console command that allows an attacker who supplies a crafted Data Pac
CVE-2026-91803	A local privilege escalation vulnerability exists in the updater of Foxit PDF Editor/Reader due to unsafe loading of dynamic-link libraries from a user-writable directo
CVE-2025-51457	D-Link DAP-2610 up to 2.06B08r099 contains an authenticated command injection vulnerability within the web interface at the /index.xgi endpoint. An attacker wit
CVE-2026-91800	A local privilege escalation vulnerability exists in the installer of Foxit PDF Editor for macOS due to insufficient validation of a user-modifiable configuration value d
CVE-2026-13248	An Authenticated Remote Code Execution via Arbitrary File Write in the Intermec Fingerprint Command Interface vulnerability in the web management interface in
CVE-2026-91798	A local privilege escalation vulnerability exists in the update daemon of Foxit PDF Editor/Reader due to an insecure permission configuration that allows the configu
CVE-2026-91813	A vulnerability in Foxit PDF Editor/Reader's update mechanism allows an update package to be replaced between download and high-privilege extraction due to ins
CVE-2026-100575	OpenClaw Slack versions before 2026.8.1 fail to properly enforce sender allowlists in multi-person direct messages. Disallowed participants can trigger Slack agent
CVE-2026-95985	The file write tool in Amazon Kiro IDE versions before 1.0.242 might allow remote unauthenticated actors to inject crafted instructions into the agent's context. Wh
CVE-2026-100552	OpenClaw (npm package 'openclaw') before 2026.8.1 does not correctly enforce per-chat tool policies for Codex app-server runtime tools. A conversation-level tool
CVE-2026-100580	OpenClaw (npm package 'openclaw') before 2026.7.1 improperly handles case sensitivity in the model-facing cron tool: a mixed-case payload kind can pass the ag
CVE-2026-86583	The Import and export users and customers plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.4.17 via the plugin's ow
CVE-2026-96775	MLflow's dspy flavor, versions >= 2.0, applies the MLFLOW_ALLOW_PICKLE_DESERIALIZATION=False security control only when the model_path ends in .pkl, which

CVE-2026-96804	MLflow's statsmodel flavor, versions 2.1.0 to 3.14.0, omits the MLFLOW_ALLOW_PICKLE_DESERIALIZATION=False security control entirely in _load_model(), which a
CVE-2026-15027	CGServiSign developed by Changing has a OS Command Injection vulnerability. Unauthenticated remote attackers can induce victims to visit a malicious web page
CVE-2026-93793	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: validate TX_CMD response layout TX_CMD parsing uses frame_count to walk st
CVE-2026-93790	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: fix out-of-bounds tid_data access in BA notif mvmsta->tid_data was indexed by
CVE-2026-85542	IBM Guardium Data Protection 12.2 is affected by a command injection vulnerability in the GIM bundle import functionality. An authenticated attacker can provide i
CVE-2026-70125	Microsoft Office Outlook Remote Code Execution Vulnerability
CVE-2026-98115	In the Linux kernel, the following vulnerability has been resolved: ksmbd: safely drain sessions during logoff SMB3 multichannel allows requests for one session to i
CVE-2026-80412	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to execute arbitrary code due to improper escaping of connector properti
CVE-2026-97527	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Serialize NVMe unsol ctx list with a per-fcport lock The fcport->unsol_ctx_head list i
CVE-2026-78309	SQL Injection vulnerability in DIAEnergie. This issue affects DIAEnergie: before 1.11.00.022.
CVE-2026-100623	Capgo (capgo.app) exposes the legacy membership table public.org_users directly through Supabase PostgREST. The table's row-level security policies "Allow org i
CVE-2026-77203	The Groups – Memberships and Access Control plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 4.6.0. This is due to the by the flawed authorization check.
CVE-2026-89426	The Knit Pay – Cashfree, Instamojo, Razorpay, PayPal and more plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 9.6.1.0
CVE-2026-96883	pgcollection is an open source extension to PostgreSQL. A type confusion issue in AWS pgcollection 2.0.0 through 2.1.1 might allow an authenticated remote user t
CVE-2026-19804	The s2Member – Excellent for All Kinds of Memberships, Content Restriction Paywalls & Member Access Subscriptions plugin for WordPress is vulnerable to Remote
CVE-2026-85491	Catalyst::Seal versions before 0.03 for Perl allow one request to disable a path or route a later one past an authorization check via a dispatch memo keyed on the r auto() guarding the deeper controller never running. The memo is cleared only when an action is registered, which happens at setup, so an entry lasts for the life c
CVE-2026-77601	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. From 5.12.0 until 7.3.0, an auth
CVE-2026-96524	The MCP Server for WordPress WordPress plugin before 1.8.2 does not correctly verify the WordPress REST API nonce for cookie-authenticated requests when a cor
CVE-2026-62062	Cross-Site Request Forgery (CSRF) vulnerability in Elementor Website Builder allows Cross Site Request Forgery. This issue affects Elementor Website Builder: from
CVE-2026-100599	OpenClaw versions 2026.5.1 through 2026.7.0 fail to apply the configured exec approval path to Google Meet node commands. The googlemmeet.chrome command
CVE-2026-78311	SQL Injection vulnerability in DIAEnergie. This issue affects DIAEnergie: before 1.11.00.022.
CVE-2026-94609	authentik is an open-source identity provider. Prior to 2026.2.7, 2026.5.7, and 2026.8.2, an account with delegated permission to manage a group, group members

CVE-2026-75825	ZohoCorp ManageEngine OpManager versions 12.8.710 and below with the Application Manager Plugin enabled were vulnerable to an Authentication Bypass vulne
CVE-2026-85682	The YOP Poll plugin for WordPress is vulnerable to Origin Validation Error in all versions up to, and including, 7.0.10. This is due to the plugin transmitting a wp_rest
CVE-2026-93280	In the Linux kernel, the following vulnerability has been resolved: greybus: audio: bound the topology section sizes against the fetched size gb_audio_gb_get_topol
CVE-2026-76978	ZohoCorp ManageEngine OpManager and Firewall Analyzer versions 12.8.709 and below were vulnerable to a Command Injection vulnerability in the Diagnose Set
CVE-2026-86678	ZohoCorp ManageEngine Applications Manager versions 182000 and below allowed a low-privileged user to obtain an administrator’s API key and use it to perform
CVE-2026-86677	ZohoCorp ManageEngine Applications Manager versions 182000 and below allowed a low-privileged user to run unauthorized SQL commands, potentially gaining a
CVE-2026-51997	An issue in geelen mcp-remote 0.1.16 through 0.1.38 allows a remote attacker to execute arbitrary code via the open() functions
CVE-2026-97409	In the Linux kernel, the following vulnerability has been resolved: nvme-fc: Do not cancel requests in io target before it is initialized A new nvme-fc controller in CO nvme_fc_ctrl_ioerr_work+0x172/0x210 [nvme_fc] process_one_work+0x82c/0x1450 worker_thread+0x5ee/0xfd0 kthread+0x3a0/0x750 ret_from_fork+0x439/0x6
CVE-2026-100587	OpenClaw versions before 2026.7.1 fail to properly validate owner authorization in the Codex computer-use installation command. Non-owner channel senders can
CVE-2026-96275	A malicious or compromised Flatpak repository can write attacker-controlled content to arbitrary locations on the host filesystem via extract_extra_data(). On syste
CVE-2026-100615	Cap-go capgo.app before 12.267.1 fails to validate target API key privilege during rotation, allowing an apikey_manager to rotate a higher-privileged org_super_adr
CVE-2026-100614	Capgo before 12.244.1 contains a cross-tenant integrity vulnerability in the metadata-cleaning worker that trusts image object keys from mutable database rows w
CVE-2026-100586	OpenClaw Codex before 2026.7.1 fails to properly enforce owner authorization when creating native conversation bindings. Non-owner channel senders with comm
CVE-2026-100619	Capgo (capgo.app) blocks direct user inserts into the public.manifest table with a RESTRICTIVE row-level security policy, but that restriction can be bypassed indire
CVE-2026-96455	The Reachy Mini daemon exposes an HTTP API for managing the robot. Its app installation endpoint, POST /apps/install in src/reachy_mini/daemon/app/routers/app LAN. On a wireless unit, then, any host on the same network can install and run code on the robot without credentials. One related change has already shipped but
CVE-2026-14913	ZohoCorp ManageEngine OpManager and Firewall Analyzer versions 12.8.669 and below were vulnerable to an SQL Injection vulnerability in Rule Management Sea
CVE-2026-80379	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to execute arbitrary commands due to improper neutralization of special
CVE-2026-100596	OpenClaw versions before 2026.7.1 fail to properly authorize non-owner users executing MCP configuration changes through /mcp set and /mcp unset commands.
CVE-2026-82566	The Botslab G980H dash camera firmware contains a session management vulnerability in which authentication state can remain valid after the associated client c
CVE-2026-84399	The Botslab G980H dash camera firmware contains an authorization vulnerability in its session based command functionality. The product does not sufficiently ass
CVE-2026-85496	The Botslab G980H dash camera firmware generates session identifiers using a small sequential value space rather than a suitably unpredictable source. An unaut
CVE-2026-94445	A malicious txtar could escape the intended execution context and force arbitrary writes to the playground host's trusted filesystem. Disjointly, one of the three po
CVE-	

CVE-2026-93284	In the Linux kernel, the following vulnerability has been resolved: drm/pagemap: dma-unmap pages before handling migration errors drm_pagemap_migrate_unma
CVE-2026-100617	Cap-go capgo.app fails to validate that principals in channel_permission_overrides belong to the organization, allowing authenticated app/org admins to grant char
CVE-2026-63498	Snipe-IT is an IT asset/license management system. Prior to 8.7.0, the uploaded-files API endpoint GET /api/v1/{object_type}/{id}/files/{file_id} allows an authentic
CVE-2026-61825	code16 Sharp is a Laravel-based framework for building content-management and administrative interfaces. Versions before 9.22.5 contain a stored cross-site scri
CVE-2026-84683	A flaw was found in Red Hat Ansible Automation Platform's automation- controller. The HTML view of job, ad hoc command, project update, and inventory update s
CVE-2026-84691	A flaw was found in Red Hat Ansible Automation Platform's automation- controller. The setting that formats the log message emitted for API 4XX errors is an admin
CVE-2026-85057	ZITADEL is an open source identity management platform. From 3.0.0 until 3.4.13 and 4.16.1, ZITADEL Actions V1 enables the goja Node-compatible require() regi
CVE-2026-91122	Discourse is an open-source discussion platform. Prior to 2026.1.8, 2026.6.3, 2026.7.2, and 2026.8.0, the video placeholder component allowed crafted HTML to ca
CVE-2026-55610	InvoiceShelf is an open-source web & mobile app that helps track expenses, payments and create professional invoices and estimates. Prior to version 2.4.1, in Inv
CVE-2026-100720	Froxlor 2.0.0 through 2.3.10 is vulnerable to stored cross-site scripting. When a customer (the lowest-privileged authenticated role) uploads an SSL certificate for o
CVE-2026-81455	Dell ThinOS 10, versions prior to SecurityAddon_2605.10.2766_T10, contain a Missing Authentication for Critical Function vulnerability. An unauthenticated attacke
CVE-2026-86064	Klever-Go is the Go implementation of the Klever blockchain protocol. Prior to 1.7.20, the default-open GET /log WebSocket route configured in config/node/api.yan
CVE-2026-77581	BentoPDF is a client-side PDF toolkit that is self hostable. In 2.8.6 and earlier, the certificate and timestamp CORS proxy in cloudflare/cors-proxy-worker.js uses isPr
CVE-2026-100697	Adminer 6.0.0 through 6.0.1, when the official ClickHouse driver plugin (plugins/drivers/clickhouse.php, rewritten in 6.0.0) is loaded, is vulnerable to pre-authentica
CVE-2026-77874	IBM Enterprise Build of Quarkus 3.27.1 through 3.27.5.SP1, and 3.33.1 through 3.33.3.SP1 is vulnerable to SQL injection. A remote unauthenticated attacker could
CVE-2026-97818	phpIPAM through 1.8.3 has incorrect authorization for id=="admins" and id=="all" in api/controllers/User.php.
CVE-2022-4997	The jet-form-builder-stripe-gateway WordPress plugin before 1.1.0 does not sanitise and escape a payment token before using it in a SQL statement, allowing unau
CVE-2026-93773	Contributor SQL Injection in Mollie Forms <= 2.11.0 versions.
CVE-2026-76086	Formie is a Craft CMS plugin for creating forms. Prior to 2.2.23 and 3.1.31, Formie's formie/integrations/form-settings control panel action in IntegrationsController:
CVE-2026-76648	CopyAPIView (awx/awx/api/generics.py:873) sets permission_classes = (IsAuthenticated,), so DRF's get_object() performs no object-level RBAC. The get() handler (
CVE-2026-100618	Capgo (capgo.app) is affected by an authorization flaw in the app icon update path. The PUT /app/:id endpoint accepts a user-controlled `icon` value, normalizes it,
CVE-2026-97730	In Netgate pfSense Plus before 26.07 and pfSense CE before 2.9.0, a Local File Inclusion (LFI) vulnerability in the Dashboard (index.php) widget sequence data han
CVE-	

CVE-2026-79310	webpy web.py 0.76 is vulnerable to server-side template injection (SSTI). The template engine can be tricked into executing attacker-controlled template code that
CVE-2026-93527	Contributor SQL Injection in Live Copy Paste for Elementor <= 1.5.10 versions.
CVE-2026-94124	Contributor SQL Injection in WP EasyCart <= 5.9.4 versions.
CVE-2026-100693	Hugo versions from v0.162.0 before v0.166.0 contain a case-sensitive validation flaw in the security.http.urls IP-literal deny rule that allows attackers to bypass res
CVE-2026-100368	CliInvoke is a .NET library for invoking command-line programs, and its `CliInvoke.Specializations` packages provide specialized wrappers for shells such as Powershell. It removes double quotes from target paths and arguments, additionally reject shell metacharacters in versions 2.2.0 through 2.9.2 and 3.0.0-alpha.1 through 3.0.0-alpha.4, o
CVE-2026-93827	In the Linux kernel, the following vulnerability has been resolved: virtio-fs: avoid double-free on failed queue setup virtio_fs_setup_vqs() allocates fs->vqs and fs->r
CVE-2026-100369	CliInvoke and its formerly named `AlastairLundy.CliInvoke` package are .NET libraries for invoking command-line programs and wrapping executable processes. `CliInvoke` removes double quotes from targets and arguments, additionally removing shell metacharacters when using shell runners, or bypassing the vulnerable factory
CVE-2026-96749	An integer overflow in the BSON document encoding component of the MongoDB Python Driver's bundled native extension may occur when a single document is b
CVE-2026-97450	In the Linux kernel, the following vulnerability has been resolved: ACPICA: validate handler object type in two places ACPICA: validate handler object type in acpi_e
CVE-2026-97452	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Prevent adding invalid references Prevent adding references for local, argument, and del
CVE-2026-97455	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Fix use-after-free in acpi_ds_terminate_control_method() Fix use-after-free issue in acpi_i
CVE-2026-97451	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Fix integer overflow in acpi_ex_opcode_3A_1T_1R() (mid_op) Add overflow check for Inde
CVE-2026-100608	Flowise through 3.1.4 does not enforce authorization on the BullMQ admin dashboard. When the server runs in queue mode with the dashboard enabled and not in
CVE-2026-100551	OpenClaw for iOS versions >= 2026.7.1 and < 2026.8.11 do not enforce saved Gateway TLS pins in the Control UI. While native connections enforced the saved G
CVE-2026-100557	OpenClaw versions before 2026.8.1 contain an authorization bypass vulnerability in skill tool dispatch that fails to carry the sender's owner status. Non-owner send
CVE-2026-100588	OpenClaw (npm package 'openclaw') before 2026.7.1 does not enforce the administrator scope requirement on browser control when it is reached through the nod
CVE-2026-100568	OpenClaw versions before 2026.8.1 fail to properly restrict access to operator command cron jobs, allowing model-visible agent callers to read and execute ownerl
CVE-2026-100589	OpenClaw versions before 2026.7.1 contain a sandbox bypass vulnerability in the browser tool that allows sandboxed sessions to access paired node browser actio
CVE-2026-82157	Dell ThinOS 10, versions prior to SecurityAddOn_2605.10.2766_T10, contains an Improper Certificate Validation vulnerability. An unauthenticated attacker with ad
CVE-2026-95626	Tauri's Content Security Policy hardening, which injects a random nonce to restrict script execution, provides zero protection when an application includes data: or
CVE-2026-86608	The WP Recipe Maker WordPress plugin before 10.8.2 does not have any authorisation check in one of its REST routes, nor does it bound what that route stores, all
CVE-2026-96454	Pake turns a website into a desktop application built on Tauri. Every application it generates inherits two settings from the upstream template, and together they h
CVE-	invoke the application's native commands. That includes third-party script the wrapped site loads on its own, such as analytics, advertising, or a compromised CDN

CVE-2026-19179	IBM Financial Transaction Manager (FTM) for RedHat OpenShift could allow a remote attacker to manipulate database queries due to improper neutralization of spe
CVE-2026-14321	The divi-dash WordPress plugin before 1.0.7 does not validate the source of the client IP address it uses for rate limiting and banning, allowing unauthenticated att
CVE-2026-100391	MediaFlow Proxy through 2.4.9 contains a server-side request forgery vulnerability in the /proxy routes due to missing and incomplete destination validation in the
CVE-2026-100676	January, the media proxy/embed service of stoatchat (stoatchat/stoatchat), before version 0.15.5 improperly resolves SVG <image href> values as local filesystem
CVE-2026-91160	OpenWA is a free, open source, self-hosted WhatsApp API gateway. Prior to 0.23.5, the /events WebSocket gateway delivers the session.qr event to a VIEWER API k
CVE-2026-100567	OpenClaw is an agent gateway distributed as the npm package 'openclaw'. In versions >= 2026.4.5 and < 2026.8.1, the Gateway validated a single DNS resolution
CVE-2026-100673	The Grav Data Manager plugin (getgrav/grav-plugin-datamanager) versions 1.0.1 through 1.4.4 render stored data entries in the item-detail view (admin/templates
CVE-2026-76087	Formie is a Craft CMS plugin for creating forms. Prior to 2.2.23 and 3.1.31, Formie's anonymous formie/submissions/submit action in SubmissionsController::action\$
CVE-2026-56736	phpMyFAQ is an open source FAQ web application. A stored cross-site scripting (XSS) vulnerability in versions prior to 4.2.0-alpha allows any unauthenticated user
CVE-2026-97433	In the Linux kernel, the following vulnerability has been resolved: nvme: validate FDP configuration descriptor sizes Validate descriptor sizes while walking the FDP
CVE-2026-97059	DCMTK through 3.7.0 contains a heap over-read vulnerability in ConcatenationLoader that copies pixel data frames without validating the PixelData buffer length a
CVE-2026-85056	ZITADEL is an open source identity management platform. From 4.0.0 until 4.16.1, ZITADEL Login V2 creates a browser session after password verification and can
CVE-2026-84486	A flaw was found in Red Hat Ansible Automation Platform's automation- controller. Four debug views that trigger the internal task, dependency, and workflow sche
CVE-2026-97525	In the Linux kernel, the following vulnerability has been resolved: x86/mm/pat: Allocate split page tables as kernel page tables A PTE is allocated directly without g
CVE-2026-77294	TREK is a collaborative travel planner. Prior to 3.3.0, TREK allows an authenticated user to store an attacker-controlled llm_base_url through the settings API when t
CVE-2026-51773	An issue in the VMware datastore driver of OpenStack glance_store. When an authenticated attacker provides a maliciously crafted image location URI pointing to i
CVE-2026-58007	Untrusted pointer dereference vulnerability in Altera Trusted Firmware on HPS allows Exploitation of Improperly Configured or Implemented Memory Protections. TI
CVE-2026-58006	Untrusted pointer dereference vulnerability in Altera Trusted Firmware on HPS allows Exploitation of Improperly Configured or Implemented Memory Protections. TI
CVE-2026-100389	GestSup versions before 3.2.61 contain a remote code execution vulnerability in the basic IMAP connector's attachment handling that fails to skip blocked file exte
CVE-2026-100387	pgPointcloud through 1.2.5 contains a heap out-of-bounds read vulnerability in dimensional patch WKB deserialization that allows authenticated database users to
CVE-2026-86683	ZohoCorp ManageEngine Applications Manager versions 182000 and below allowed a low-privileged user to change the proxy settings.
CVE-2026-100532	@openclaw/whatsapp (npm) before 2026.8.1 exposes the WhatsApp login tool through the generic channel-tool path without preserving the originating sender's ov
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: svcrdma: Fix unmatched rn_unregister on failed accept When svc_rdma_accept() takes the errout

93224	place, the accept errout drops the kref_init() birth reference via svc_xprt_put(), which dispatches svc_rdma_free(). Teardown of sc_qp, sc_sq_cq, sc_rq_cq, and sc_p
CVE-2026-58004	Out-of-bounds read vulnerability in Altera Trusted Firmware on HPS allows Privilege Escalation and Overflow Buffers. This issue affects Trusted Firmware: through s
CVE-2026-96756	orval versions before 8.30.0 contain a code injection vulnerability in the @orval/core factory generator that fails to escape date default values in new Date() calls. #
CVE-2026-93221	In the Linux kernel, the following vulnerability has been resolved: nfsd: convert nfsd_net boolean flags to unsigned long flags word nfsd_net contains several boole; reclaim_str_hashtbl with no lock and calls nfs4_remove_reclaim_record() (list_del + kfree) on each entry. Two concurrent walkers corrupt the list and double-free ev
CVE-2026-58005	Out-of-bounds read vulnerability in Altera Trusted Firmware on HPS allows Privilege Escalation and Overflow Buffers. This issue affects Trusted Firmware: through s
CVE-2026-94487	Unauthenticated Cross Site Request Forgery (CSRF) in PublishPress Capabilities <= 2.50.1 versions.
CVE-2026-58008	Stack-based buffer overflow vulnerability in Altera Trusted Firmware on HPS allows Exploitation of Improperly Configured or Implemented Memory Protections. This
CVE-2026-56737	phpMyFAQ is an open source FAQ web application. Versions 3.2.0 through 4.1.5 contain an authentication bypass in its public two-factor authentication verification
CVE-2026-44642	Piwigo is a full featured open source photo gallery application for the web. Prior to 16.4.0, check_upgrade_access_rights() in admin/include/functions_upgrade.php c
CVE-2026-18181	IBM Financial Transaction Manager (FTM) for RedHat OpenShift could allow a remote attacker to bypass authentication and access sensitive information due to a hi
CVE-2026-98069	In the Linux kernel, the following vulnerability has been resolved: net/rds: acquire the fastpath locks in rds_conn_shutdown() rds_conn_shutdown() quiesces the tra BUG_ON()s in rds_ib_sub_signaled(), unexpected op-codes and NULL dereferences in rds_ib_send_cqe_handler() during failover testing - by making the teardown pa so, so its wait now spans the teardown instead of at most one send batch. That waiter runs from rds_tcp_accept_one() on the single-threaded krdsd workqueue and parked accept worker for that time. It cannot deadlock, although the waits do point at each other: the teardown blocks until the bit's holder releases it, and the hol
CVE-2026-90959	A path traversal vulnerability was found in pulpcore. The content upload API accepts a 'file_url' parameter that allows users with file repository privileges to specify
CVE-2026-98070	In the Linux kernel, the following vulnerability has been resolved: net/rds: acquire RDS_IN_XMIT in rds_tcp_reset_callbacks() rds_tcp_reset_callbacks() quiesces the above the wait still holds: the lock is acquired before lock_sock(), so a sender inside tcp_sendmsg() can never be waited on while we hold the socket lock. Two deta new socket, or it has been torn down meanwhile and is dropped. The in-function comment describing the old wait-based quiesce is rewritten to describe the lock-bi
CVE-2026-98130	In the Linux kernel, the following vulnerability has been resolved: sctp: fix a TOCTOU race in SCTP_CMD_TIMER_START The SCTP_CMD_TIMER_START handler check
CVE-2026-13465	Stack-based buffer overflow vulnerability in Altera Trusted Firmware on HPS allows Exploitation of Improperly Configured or Implemented Memory Protections. This
CVE-2026-97573	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Handle buffer allocation failure in bnxt_rx_ring_reset() bnxt_rx_ring_reset() frees the ring
CVE-2026-81630	The Botslab G980H dash camera firmware does not adequately verify the authenticity of firmware updates. The update process retrieves firmware through an unpri
CVE-2026-97055	SigNoz from v0.8.0 before v0.143.0 defaults the JWT tokenizer signing secret (tokenizer::jwt::secret, set via SIGNOZ_TOKENIZER_JWT_SECRET or the deprecated SI
CVE-2026-81473	Dell Rugged Control Center (RCC), versions prior to 5.2.206, contain an Improper Authorization vulnerability. A low privileged attacker with local access could poter
CVE-2026-93508	The WC Fields Factory WordPress plugin before 4.1.11 does not properly restrict access to its field-management AJAX action, allowing authenticated users with Sub
CVE-2026-100646	SiYuan is a self-hosted personal knowledge management system. In versions up to and including 3.8.3, the kernel's authentication guards (CheckAuth in kernel/mc
CVE-2026-77762	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in Apache Tomcat allows an attacker to inject trailer fie
CVE-	

CVE-2026-100627	Capgo (Cap-go/capgo.app) server backend Supabase functions contain an incorrect authorization flaw in the API-key bundle promotion path. The PUT /bundle endpoint is vulnerable to a Denial of Service (DoS) attack. An attacker can trigger a DoS by sending a large number of requests to the endpoint, causing the server to become unresponsive.
CVE-2026-19125	The EthPress – Web3 Login plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 2.3.5. This is due to the verify_login() function not properly validating the user's credentials.
CVE-2026-77967	The Botslab G980H dash camera firmware accepts a reusable authentication value without adequately verifying its freshness or association with the requesting client. This allows an attacker to reuse a valid authentication token to gain unauthorized access to the camera's functionality.
CVE-2026-93787	In the Linux kernel, the following vulnerability has been resolved: smb: client: bound dirent name against end of SMB response in cifs_filldir cifs_filldir() copies the dirent name into the buffer, but it does not check if the name is null-terminated. This can lead to a buffer overflow if the name is longer than the buffer size.
CVE-2026-97875	Rojo's "rojo serve" HTTP API (default port 34872) has no Host/Origin header validation, making it vulnerable to DNS rebinding. A malicious webpage can read all protected data by exploiting this vulnerability.
CVE-2026-92713	The Modula Image Gallery – Photo Grid & Video Gallery plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the upload handler.
CVE-2026-93354	Taskview Community before 1.56.0 contains a missing authentication vulnerability that allows unauthenticated attackers to register arbitrary OAuth clients and take over the application.
CVE-2026-100684	Budibase versions 3.41.0 before 3.45.0 contain an authentication bypass in the OIDC/SSO login path of @budibase/server. In sso.authenticate, when no existing user is found, the system incorrectly grants access.
CVE-2026-84787	ZohoCorp ManageEngine OpManager and Firewall Analyzer versions 12.8.710 and below were vulnerable to a Privilege Escalation vulnerability that allowed an authenticated user to gain root access.
CVE-2026-100680	Budibase versions before 3.45.0 fail to disable external JSON reference resolution in the OpenAPI/Swagger import validator, allowing authenticated builders to read sensitive data from external sources.
CVE-2026-57590	A missing authorization vulnerability exists in the Task Group APIs of Apache DolphinScheduler. The affected APIs do not properly verify whether the authenticated user has the necessary permissions to perform the requested action.
CVE-2026-62368	Snipe-IT is an IT asset/license management system. Prior to 8.7.0, a user with the customfields.create permission can store markup in CustomField.name, and applications can be affected by this vulnerability.
CVE-2026-63493	Snipe-IT is an IT asset/license management system. Prior to 8.7.0, a password-authenticated session for an account with self.api permission can reach the personal data of other users.
CVE-2026-93282	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix maximum allowed access checks The DACL permission check looks for an ACE matching the requested security privilege that ksmbd does not grant. For regular files, include FILE_EXECUTE in maximal access when the client requested GENERIC_EXECUTE and the DACL does not contain FILE_EXECUTE.
CVE-2026-94611	authentik is an open-source identity provider. Prior to 2026.2.7, 2026.5.7, and 2026.8.2, authentik API serializers return stored credentials when an account has view permissions, which is a security flaw.
CVE-2026-13467	Out-of-bounds write vulnerability in Altera Trusted Firmware on HPS allows Exploitation of Improperly Configured or Implemented Memory Protections. This issue affects Altera HPS devices running Trusted Firmware.
CVE-2026-97570	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Bound SW TPA IDs to prevent crashes FW supports up to 1024 concurrent TPAs, so the firmware can crash if the user-space driver does not properly manage the TPA IDs. The invalid write mentioned above is silent in this particular crash. Fix this by allocating rx_tpa with bp->max_tpa rounded up to the next power of 2.
CVE-2026-13466	Incorrect calculation of buffer size vulnerability in Altera Trusted Firmware on HPS allows Overflow Buffers. This issue affects Trusted Firmware: through socfpga_v20.0.0 and socfpga_v20.0.1.
CVE-2026-93786	In the Linux kernel, the following vulnerability has been resolved: ksmbd: preserve VFS inherited POSIX ACL mask The VFS initializes a child's POSIX ACL from the parent's ACL, but it does not preserve the inherited mask, which can lead to incorrect ACL permissions.
CVE-2026-100686	Budibase versions before 3.45.0 fail to validate per-app authorization in the POST /api/global/groups/:groupId/apps endpoint, allowing builders to assign application permissions to unauthorized users.
CVE-2026-100671	Grav is a flat-file CMS. In versions 2.0.19 through 2.0.24 — and in 2.0.0 through 2.0.18 and 1.7.x only where content Twig has been explicitly enabled — page content is not properly sanitized, leading to a Denial of Service (DoS) attack.
CVE-2026-100683	Budibase (@budibase/server) before 3.45.0 builds MySQL and MSSQL column-rename DDL in packages/backend-core/src/sql/sqlTable.ts by interpolating identifiers directly into the SQL query, which is a security flaw.
CVE-	

CVE-2026-100645	SiYuan versions 3.7.0 before 3.8.4 contain a stored cross-site scripting vulnerability in gallery and kanban database renderers where field descriptions are not esca
CVE-2026-100643	SiYuan versions before v3.8.4 fail to properly escape four stored Attribute View values in textarea elements, allowing authenticated attackers to inject JavaScript b
CVE-2026-100641	SiYuan before v3.8.4 does not HTML-escape stored flashcard block content before interpolating it into the card-manager list markup. Block content returned by /ap
CVE-2026-100561	OpenClaw (npm package 'openclaw') versions >= 2026.3.22 and < 2026.8.1 contain an approval-bypass flaw in the exec approval policy: the policy could trust a c
CVE-2026-100585	OpenClaw (npm package `openclaw`) before 2026.7.1 fails to enforce the owner-only authorization requirement for Claude Code permission prompts delivered thr
CVE-2026-100559	OpenClaw versions before 2026.8.1 contain a command parser vulnerability where escaped newlines confuse exec allowlist parsing, allowing hidden commands to
CVE-2026-84095	The wp-review-slider-pro WordPress plugin before 12.7.12 does not perform a capability check on one of its AJAX handlers, and the nonce protecting it is generate
CVE-2026-97735	ITFlow before 26.08 allows SVG attachments in the ticket email parser (cron/ticket_email_parser.php) for email messages that may arrive over SMTP from arbitrary
CVE-2026-84096	The wp-review-slider-pro WordPress plugin before 12.7.12 does not perform a capability check on the AJAX handler that saves its review submission forms, and the
CVE-2026-91812	A vulnerability in Foxit PDF Editor/Reader’s update mechanism allows man-in-the-middle attackers to bypass certificate validation and package integrity checks, pc
CVE-2026-86926	A heap buffer overflow vulnerability in the FileMaker Server database engine block parsing routine allowed a maliciously crafted .fmp12 database file to cause men
CVE-2026-97579	In the Linux kernel, the following vulnerability has been resolved: media: mediatek: vcodec: bound AV1 tile-start copy to the array capacity vdec_av1_slice_setup_t
CVE-2026-97577	In the Linux kernel, the following vulnerability has been resolved: media: verisilicon: rockchip: reject AV1 frames exceeding the tile capacity rockchip_vpu981_av1_
CVE-2026-97576	In the Linux kernel, the following vulnerability has been resolved: media: v4l2-ctrls: validate HEVC tile counts The stateless HEVC decoders read num_tile_columns_
CVE-2026-91789	Foxit PDF Editor/Reader’s U3D/GIF texture decoding path contained insufficient validation of image dimensions and related size information. Under certain conditio
CVE-2026-91790	When rendering the page image, Foxit PDF Editor/Reader fails to perform validation on image objects whose optional content attributes are malformed. As a result,
CVE-2026-91791	When processing a specially crafted PDF file, Foxit PDF Editor/Reader may encounter a reentrant execution condition involving JavaScript triggered by page-visibilit
CVE-2026-97575	In the Linux kernel, the following vulnerability has been resolved: media: v4l2-ctrls: validate AV1 tile counts The stateless AV1 decoders use tile_info.tile_cols and ti
CVE-2026-93782	In the Linux kernel, the following vulnerability has been resolved: vhost-scsi: flush backend after device ioctls vhost-scsi translates guest response descriptors into
CVE-2026-91792	When processing a specially crafted PDF, Foxit PDF Editor/Reader may perform reentrant zoom and layout operations through page- and annotation-related JavaSc
CVE-2026-91793	When opening a specially crafted PDF, Foxit PDF Editor/Reader executes scripts that modify annotation rich-text attributes containing malformed font data. During
CVE-2026-97578	In the Linux kernel, the following vulnerability has been resolved: media: verisilicon: rockchip: guard VPU981 AV1 divisor and tile buffer rockchip_vpu981_av1_dec_
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: mm/slab: take n->list_lock in __slab_try_return_freelist() to avoid race Commit ba7425312607 ("n

97941	0010: __list_add_valid_or_report+0x80/0xd0 ... Call Trace: alloc_from_new_slab+0x183/0x300 __slab_alloc+0x31c/0x890 __kmalloc_noprof+0x3d4/0x800 lsm_blob
CVE-2026-97548	In the Linux kernel, the following vulnerability has been resolved: xfs: fix the rtrmap and rtrefcount _maxlevels_ondisk functions The _maxlevels_ondisk functions a
CVE-2026-93262	In the Linux kernel, the following vulnerability has been resolved: md/raid5-ppl: fix use-after-free in ppl_do_flush() The loop in ppl_do_flush() continues iterating aft
CVE-2026-93277	In the Linux kernel, the following vulnerability has been resolved: RDMA/bnxt_re: Validate udata before executing commands The destroy callbacks currently zero t
CVE-2026-91841	A flaw was found in NetworkManager-vpnc, a VPN plugin for NetworkManager. A local unprivileged user can exploit this vulnerability by injecting a newline charact
CVE-2026-91840	A flaw was found in NetworkManager-vpnc. This vulnerability allows a local unprivileged user to escalate privileges to root. By injecting a newline character into the
CVE-2026-91839	A flaw was found in NetworkManager-fortisslvpn, the FortiSSLVPN plugin for NetworkManager. The nm-fortisslvpn-service improperly handles carriage-return/line-fe
CVE-2026-91838	A flaw was found in NetworkManager-sstp, the SSTP VPN plugin for NetworkManager. A local unprivileged user can exploit this vulnerability by embedding special c
CVE-2026-100713	Froxlor 2.3.10 and earlier contain a time-of-check time-of-use (TOCTOU) race condition in the SSH key synchronization cron (lib/Froxlor/Cron/System/SshKeys.php, ... introduced for GHSA-mq5v-.... . The issue is fixed in Froxlor 2.3.12.
CVE-2026-91837	A flaw was found in NetworkManager-iodine, the iodine VPN plugin for NetworkManager. A local unprivileged user can exploit a vulnerability in how the 'nameserve
CVE-2026-95519	A flaw was found in rpm. An attacker can supply a crafted manifest file that, when processed by a user or automation using `rpm -q -p` or similar manifest-process
CVE-2026-95521	A command injection flaw was found in rpm. Installing or rebuilding a source RPM whose source or spec file basenames contain a %() macro construct causes rpm t
CVE-2026-75131	NetworkManager-l2tp through 1.52.4, fixed in 1.52.6, contains a privilege escalation vulnerability that allows local users with permission to create VPN connections
CVE-2026-89325	An uncontrolled search path element in InsightVM assessment content in Rapid7 Insight Agent on Windows allows a local, low-privileged user to execute arbitrary c managed. This issue was resolved in assessment content version 0.0.269.0, which was made generally available on September 15, 2026. Remediation was deploye
CVE-2026-97513	In the Linux kernel, the following vulnerability has been resolved: media: chips-media: wave5: Release m2m_ctx after Instance Removed from List Possible use aft
CVE-2026-93287	In the Linux kernel, the following vulnerability has been resolved: i2c: smbus: reject oversized block transfers in the common path The SMBus block transfer length (include/trace/events/smbus.h) trace_smbus_write() fires before any validation and copies data->block[0]+1 bytes into a 34-byte event buffer. With block[0]=0xfe Trace: <TASK> __ubsan_handle_out_of_bounds+0xd7/0x120 stub_xfer+0x1971/0x198f [i2c_stub] __i2c_smbus_xfer+0x306/0xa40 i2c_smbus_xfer+0x19e/0x340 i2
CVE-2026-91795	Foxit PDF Editor/Reader's FileOpen plugin did not adequately validate certain encryption metadata in specially crafted PDF files. This could leave an internal pointe
CVE-2026-97497	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Check bounds for allocate_sdma_queue restore_sdma_id allocate_sdma_queue has
CVE-2026-97478	In the Linux kernel, the following vulnerability has been resolved: virt: acrn: Fix irqfd use-after-free during eventfd shutdown acrn_irqfd_deassign() and the eventfd ensures the cleanup work is queued at most once, no matter how many of {EPOLLHUP, deassign, deinit} fire concurrently. This is safe to call from the waitqueue c
CVE-2026-93288	In the Linux kernel, the following vulnerability has been resolved: netfilter: nfnetlink_log: wait for rcu grace period before freeing pernet state sashiko reports: "nfnl
CVE-2026-91794	An out-of-bounds write vulnerability exists in the PDF rendering process of Foxit PDF Editor/Reader due to insufficient consistency and boundary validation when pr
CVE-2026-98122	In the Linux kernel, the following vulnerability has been resolved: vxlan: mdb: Fix use-after-free in vxlan_mdb_remote_src_del() vxlan_mdb_is_valid_source(), which entry, and frees 'ent'. The second call then runs on the freed entry, and its hlist_del() reads ->pprev and ->next out of it and writes through them. Adding the (*, G is expressed by omitting the source, so nothing legitimate is refused. Discovered by XBOW, triaged by Baul Lee <baul.lee@xbow.com>
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix reloc root cleanup in merge_reloc_roots() If the root we got has zero root refs in its root i

93798	
CVE-2026-97903	In the Linux kernel, the following vulnerability has been resolved: exit: hold a reference to thread_pid across proc_flush_pid Commit 0a36bad01731 ("release_task: proc_invalidate_siblings_dcache+0x3e2/0x3f0 Read of size 8 by task h7_pid_reaper/1921 Call Trace: proc_invalidate_siblings_dcache release_task wait_consider_ta
CVE-2026-96442	A code execution flaw was found in Emacs, affecting versions prior to 31.2. The Flymake mode using language backends other than Lisp would execute arbitrary co
CVE-2026-6935	IBM Concert 1.0.0 through 3.0.0 invokes operating system commands without fully qualifying executable paths or adequately restricting search path resolution. As
CVE-2026-97594	In the Linux kernel, the following vulnerability has been resolved: landlock: Fix use-after-free of the source's parent directory current_check_refer_path() reads old_collect_domain_accesses+0x278/0x290 Read of size 4 at addr ffff888160bd53f4 by task llrepro2/549 collect_domain_accesses+0x278/0x290 current_check_refer_j
CVE-2026-6794	IBM Concert 1.0.0 through 3.0.0 has a double free vulnerability that exists due to incorrect memory management. A local attacker can exploit this flaw to corrupt h
CVE-2026-97602	In the Linux kernel, the following vulnerability has been resolved: inet: frags: invalidate queues before flushing them fqdir_pre_exit() flushes the skbs from incompl already owned by another destroy path and must be left alone. Releasing a timer reference removed by inet_frag_kill() is deferred to inet_frag_putn(), after the que packet_sendmsg (net/packet/af_packet.c:3110 net/packet/af_packet.c:3142) __x64_sys_sendmmsg (net/socket.c:2883 net/socket.c:2880 net/socket.c:2880) The bu (net/socket.c:2883 net/socket.c:2880 net/socket.c:2880) packet_sendmsg (net/packet/af_packet.c:2959 net/packet/af_packet.c:3053 net/packet/af_packet.c:3142)
CVE-2026-97429	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: fix UAF race in destroy_queue_cpsch wait_on_destroy_queue() drops locks to wait fo
CVE-2026-100597	OpenClaw (npm package 'openclaw') before 2026.7.1 is vulnerable to a time-of-check time-of-use race condition in OpenShell local mirror filesystem mutation open
CVE-2026-98052	In the Linux kernel, the following vulnerability has been resolved: net: bcmasp: clear txcb->last before writing each descriptor bcmasp_xmit() only wrote txcb->last
CVE-2026-97611	In the Linux kernel, the following vulnerability has been resolved: net: openvswitch: fix use-after-free of the flow table mask array tbl_mask_array_realloc() retires t internal_dev_xmit+0x81/0x170 Freed by task 728: kfree+0x16a/0x4e0 rcu_core+0x853/0x1030 Publish the new array before retiring the old one. The kfree_rcu() t
CVE-2026-96889	A flaw was found in librsvg. When processing an SVG document containing nested XML inclusions (Xincludes) with duplicate entity declarations, a use-after-free err
CVE-2026-97612	In the Linux kernel, the following vulnerability has been resolved: net: mpls: clear inner_protocol when the last label is popped skb_mpls_push() records the pre-enc ffff8ffffc16000 #PF: supervisor write access in kernel mode Oops: 0002 [#1] SMP KASAN NOPTI RIP: 0010:memcpy+0x8/0x20 RDX: 00000000ffffff8 RSI: ffff88810
CVE-2026-97421	In the Linux kernel, the following vulnerability has been resolved: RDMA/umem: Be careful about boundary conditions in ib_umem_find_best_pgsz() Several corner
CVE-2026-79153	Seclore FileSecure Desktop Client before 3.25.1.0 contains improper access control vulnerability in the kernel-mode driver component that allows an authenticated
CVE-2026-98023	In the Linux kernel, the following vulnerability has been resolved: vxlan: reject dynamic fdb entries that reference a nexthop id The commit cited in the Fixes tag al __list_del_entry_valid_or_report+0x1aa/0x210 ... vxlan_fdb_destroy+0x5b8/0xad0 vxlan_cleanup+0x328/0x450 call_timer_fn+0x2a/0x1c0 run_timer_softirq+0x18c
CVE-2026-97415	In the Linux kernel, the following vulnerability has been resolved: btrfs: tree-checker: validate names in ROOT_REF and ROOT_BACKREF ROOT_REF and ROOT_BACK
CVE-2026-97910	In the Linux kernel, the following vulnerability has been resolved: ASoC: sprd: validate compress buffer sizes against fixed allocations sprd_platform_compr_open() the fixed buffers in set_params(), and fix the advertised max fragment size: 128K never fitted into the 32K IRAM buffer. The caps values may have been carried ov
CVE-2026-97911	In the Linux kernel, the following vulnerability has been resolved: accel: ethosu: Ensure SRAM region size matches job It is possible for userspace to set the job SRA
CVE-2026-93237	In the Linux kernel, the following vulnerability has been resolved: LoongArch: Add DIRECT_MAP_PHYSMEM_END definition get_free_mem_region() and mhp_get_plur maximal folio size") keeps that region in bounds on current Loongson-3C6000 configs, but CPUs with smaller cpu_pabits (e.g. the Loongson-2K series) are still affe
CVE-2026-96512	A flaw was found in sudo. When sudoers rules use NOTBEFORE or NOTAFTER time-based access restrictions with timestamps that omit the trailing 'Z' timezone ind
CVE-2026-98017	In the Linux kernel, the following vulnerability has been resolved: net/sched: defer qdisc freeing after failed creation An RTM_NEWQDISC request can make clsmct b
CVE-	

CVE-2026-97580	In the Linux kernel, the following vulnerability has been resolved: media: rkvddec: bound HEVC tile loops and PPS id to the array capacity compute_tiles_uniform() at
CVE-2026-100570	OpenClaw (npm package 'openclaw') versions >= 2026.3.28 and < 2026.8.1 allow an untrusted workspace .env file to set the CLOUDSDK_PYTHON_ARGS environnr
CVE-2026-91815	Foxit PDF Editor/Reader does not perform sufficient verification of the JPEG2000 image metadata in the PDF file, which leads to out-of-bounds write in the heap buf
CVE-2026-98073	In the Linux kernel, the following vulnerability has been resolved: net: Remove conflicting altnames for dying netns in __dev_change_net_namespace(). syzbot repc kworker/u8:9 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 07/24/2026 Workque net/core/net_namespace.c:200 [inline] ops_undo_list+0x43d/0x8d0 net/core/net_namespace.c:253 cleanup_net+0x572/0x810 net/core/net_namespace.c:706 proc
CVE-2026-91816	A use-after-free vulnerability exists in Foxit PDF Editor/Reader’s handling of PDF annotations. Reentrant annotation deletion triggered by embedded JavaScript can
CVE-2026-91818	A use-after-free vulnerability exists in Foxit PDF Editor/Reader’s JavaScript handling of PDF annotations. Reentrant page-event processing during annotation enum
CVE-2026-97185	A flaw was found in GIMP. When processing a specially crafted GIMPressionist preset file, the plug-in does not properly validate vector indices before writing into fi
CVE-2026-81208	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow an authenticated user to access sensitive information due to improper handling of encrypted credentials. .
CVE-2026-92470	GitLab has remediated an issue in GitLab EE affecting all versions from 18.7 before 19.2.7, 19.3 before 19.3.3, and 19.4 before 19.4.1 that under certain conditions
CVE-2026-89032	BerriAI LiteLLM before 1.101.0-rc.1 contains a tenant isolation bypass vulnerability in the semantic cache layer that allows authenticated users to read other tenan
CVE-2026-81536	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to obtain sensitive information due to an XML external entity (XXE) inject
CVE-2026-97454	In the Linux kernel, the following vulnerability has been resolved: ACPICA: add boundary checks in acpi_ps_get_next_field() Add boundary checks in acpi_ps_get_ne
CVE-2026-76089	Formie is a Craft CMS plugin for creating forms. Prior to 2.2.23 and 3.1.31, Formie's formie/sent-notifications/get-resend-modal-content control panel action in Sent
CVE-2026-76979	ZohoCorp ManageEngine OpManager and Firewall Analyzer versions 12.8.709 and below were vulnerable to an XML Injection vulnerability in the Rule Tracking Corr
CVE-2026-100704	Kyverno is a policy engine for Kubernetes. In versions 1.14.0 through 1.19.0, the ImageValidatingPolicy (policies.kyverno.io/v1beta1) evaluator never reads the spe
CVE-2026-100607	Flowise through 3.1.4 resolves SSO and local-password users solely by email without storing provider or subject identifier bindings, allowing attackers to authentic
CVE-2026-100703	Kyverno 1.16.0 through 1.19.0 registers the globalcontext.Lib CEL library in its policy environment without confining it to the policy's namespace, unlike the sibling
CVE-2026-100606	Flowise through 3.1.4 (Enterprise/platform mode with SSO enabled) contains an authentication bypass in the SSO login path. When an SSO callback arrives with an
CVE-2026-97445	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Enhance buffer validation in acpi_ut_walk_aml_resources() Enhance buffer validation in a
CVE-2026-88390	An out-of-bounds write vulnerability in jsGetTokenValueAsString() in Espruino 2v29 (commit bffc6d0) allows crafted JavaScript input containing an overlong token t
CVE-2026-100685	Budibase before 3.45.0 fails to properly scope the GET /api/chat-links endpoint by workspace, allowing builders to enumerate chat identity link records across all w
CVE-2026-97444	In the Linux kernel, the following vulnerability has been resolved: ACPICA: add boundary checks in two places Add boundary checks in acpi_ps_get_next_namestrin
CVE-	

CVE-2026-100707	Kyverno before 1.19.1 contains a namespace isolation bypass in the apiCall context entry of namespaced Policy resources due to inconsistent path interpretation b
CVE-2026-93265	In the Linux kernel, the following vulnerability has been resolved: PCI/pwrctrl: tc9563: Fix parsing the integrated Ethernet MAC Endpoint node DSP3 has an integrat
CVE-2026-95627	When a Tauri application uses the dialog plugin's file or folder picker, an attacker with JavaScript execution (XSS) can force the scope expansion to be recursive, gr
CVE-2026-84499	A flaw was found in Red Hat Ansible Automation Platform's automation- controller. Survey questions of type password are write-only and stored encrypted, display
CVE-2026-97428	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: harden FRU PIA parsing with bounded helpers Replace the open-coded TLV walk wi
CVE-2026-97448	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Add validation for node in acpi_ns_build_normalized_path() Add validation for node in acp
CVE-2026-79764	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. From 2.5.0 until 2.5.1, the /homepage/proxy endpoi
CVE-2026-100636	SiYuan versions before v3.8.4 contain a path traversal vulnerability in the exportBrowserHTML endpoint that allows authenticated administrators to write arbitrary
CVE-2026-100637	SiYuan versions before v3.8.4 contain a path traversal vulnerability in the checkoutRepo endpoint that allows authenticated administrators to write JSON files outsi
CVE-2026-95522	Shop manager SQL Injection in Easy Digital Downloads <= 3.7.0 versions.
CVE-2026-100638	SiYuan versions before v3.8.4 contain a path traversal vulnerability in the setNotebookIcon endpoint that allows authenticated administrators to create arbitrary di
CVE-2026-95593	Editor SQL Injection in Ultimeter <= 3.0.8 versions.
CVE-2026-12370	ZohoCorp ManageEngine OpManager, NetFlow Analyzer, and Network Configuration Manager versions 12.8.667 and below were vulnerable to a Server-Side Templ
CVE-2026-100642	SiYuan versions from v2.1.0 before v3.8.4 contain a cross-site request forgery vulnerability in the CheckAuth lock-screen pass-through branch that grants administ
CVE-2026-84706	A flaw was found in Ansible Automation Platform's automation-controller. The custom Credential Type environment-variable injector validates variable names again
CVE-2026-100705	Kyverno before 1.19.1 is vulnerable to server-side request forgery. The default egress blocklist (169.254.169.254, 169.254.169.253, metadata.google.internal, 127
CVE-2026-84893	IBM Guardium Data Protection 12.2 is vulnerable to SQL injection in the PESI service. An authenticated attacker could exploit this vulnerability to access sensitive in
CVE-2026-100579	OpenClaw (npm package 'openclaw') before 2026.7.1 incorrectly trusts requester provenance in message.action. In identity-bearing Gateway deployments (auth
CVE-2026-63203	Logto is the modern, open-source auth infrastructure for SaaS and AI apps. From 1.31.0 until 1.42.0, the Account API handlers in packages/core/src/routes/account
CVE-2026-96826	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Shazzad Hossain Khan W4 Post List allows Blind SQL Injectio
CVE-2026-94174	Administrator SQL Injection in Email Log <= 2.63 versions.
CVE-2026-77394	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. From 5.0.6 until 7.3.0, an auth
CVE-	

CVE-2026-86681	ZohoCorp ManageEngine Applications Manager versions 182200 and below were vulnerable to a permissions validation issue that allowed low-privileged users to e
CVE-2026-100578	OpenClaw (npm package `openclaw`) before 2026.7.1 fails to restrict owner-only infrastructure tools exposed through the chat.send endpoint. In Gateway deployn
CVE-2026-100631	Parse Server is an open source backend server. In versions prior to 8.6.90 and in versions from 9.0.0 prior to 9.10.1-alpha.9, the device token deduplication logic fo
CVE-2026-97583	In the Linux kernel, the following vulnerability has been resolved: afs: Clear stale peer app data after address list changes afs_fs_probe_fileserver() fetches the curr
CVE-2026-97417	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_contrack: use get_unaligned_be32() in tcp_sack() The timestamp-only fast path dere
CVE-2026-31377	An Improper Authentication vulnerability in the Apache Doris Frontend (FE) meta service allows an unauthenticated remote attacker to access internal metadata se
CVE-2026-93368	The Rename wp-login.php to anything you want plugin for WordPress is vulnerable to time-based SQL Injection via 'log' (Username) Parameter in all versions up to,
CVE-2026-94613	authentik is an open-source identity provider. Prior to 2026.2.7, 2026.5.7, and 2026.8.2, an unauthenticated attacker can submit a malformed SAML message to ar
CVE-2026-75887	A flaw was found in the OpenShift console. An unauthenticated attacker can exploit a path traversal vulnerability by manipulating the `Ing` and `ns` query param
CVE-2026-97990	In the Linux kernel, the following vulnerability has been resolved: vdpa_sim_net: check TX pull result before RX copy vringh_iov_pull_iotlb() returns a signed byte cc
CVE-2026-88357	nDPI 5.1.0 contains a memory access issue in the DNS dissector and serializer deserialization code. Specially crafted network input can cause byte-buffer addresse
CVE-2026-78383	Allocation of resources without limits or throttling vulnerability in Apache Tomcat allows an unauthenticated AJP request to pin an AJP processing thread leading to
CVE-2026-86243	Buffer over-read vulnerability in Apache Tomcat Native during the TLS handshake permits a malicious user to trigger a DoS via a JVM crash. This issue affects Apac
CVE-2026-87022	Improper handling of length parameter inconsistency vulnerability in Apache Tomcat allows WebSocket message smuggling when per-message-deflate is used. Thi
CVE-2026-100644	SiYuan before v3.8.4 contains a SQL injection vulnerability in the graph query endpoint where the dailyNoteSavePath parameter is concatenated into SQL without e
CVE-2026-100622	capgo.app through 12.129.0 fails to verify deletion status when serving cached bundle artifacts from the public file read endpoint. Unauthenticated attackers can c
CVE-2026-93826	In the Linux kernel, the following vulnerability has been resolved: HID: hidpp: fix potential UAF in hidpp_connect_event() If input_register_device() fails, we call input
CVE-2026-100610	Flowise through 3.1.4 exposes GET /api/v1/upsert-history/:id and PATCH /api/v1/upsert-history without route-level permission checks, and the backing service perfo
CVE-2026-93830	In the Linux kernel, the following vulnerability has been resolved: net: stmmac: xgmac2: disable RBUE in default RX interrupt mask Enabling the RX Buffer Unavaila
CVE-2026-15358	ZohoCorp ManageEngine OpManager and Network Configuration Manager versions before 12.8.671 were vulnerable to an unauthorized Path Traversal vulnerability
CVE-2026-97595	In the Linux kernel, the following vulnerability has been resolved: mac802154: fix use-after-free of sdata via queued RX frames The RX softirq producer ieee802154
CVE-2026-77791	Uncontrolled Resource Consumption vulnerability in Apache Tomcat during sending of WebSocket close message enabled a DoS attack. This issue affects Apache T
CVE-	

CVE-2026-79677	Missing release of resource after effective lifetime, Comparison using wrong factors vulnerability in Apache Tomcat allows a denial of service as a result of lost time
CVE-2026-88361	SumatraPDF 3.6.1 contains an integer overflow vulnerability in EngineMupdf::BuildPageLabelRec() when parsing PDF PageLabels /Nums entries.
CVE-2026-100669	Grav before 2.0.25 ships web server configuration samples whose access-control deny rules are matched case-sensitively. In webserver-configs/web.config (IIS), ev webserver-configs/lighttpd.conf, whose user/(config env), directory, script-extension, root-file and dotfile rules lack the (?)i modifier, though it is lower risk because
CVE-2026-100660	Netty's HTTP/3 codec (io.netty:netty-codec-http3) from 4.2.0.Final through 4.2.17.Final retains unbounded per-stream QPACK encoder state. QpackEncoder stores i
CVE-2026-100661	Netty's HTTP/3 codec (io.netty:netty-codec-http3) versions 4.2.0.Final through 4.2.17.Final contain a denial-of-service vulnerability in the QPACK prefixed-integer d
CVE-2026-19438	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ABB Mint Workbench I. This issue affects Mint Workbench I: through 5
CVE-2026-100711	froxlor versions before 2.3.12 fail to invalidate existing panel sessions, API keys, and 2FA trust cookies when a user password is changed. Attackers holding hijacke
CVE-2026-80513	The wpForo Forum WordPress plugin before 3.1.6 does not restrict which classes may be instantiated when it deserializes a user-supplied profile field value, allowin
CVE-2026-93289	The affected products are vulnerable to command injection attack that could allow an unauthenticated attacker to execute system commands during the pairing p
CVE-2026-88382	hiredis commit 29ea279 (post-v1.5.0) contains an uncontrolled memory allocation vulnerability in its RESP aggregate parser.
CVE-2026-92608	Improper handling of property-encoding exceptions in AMQP 1.0-to-AMQP 0-10 message conversion allows authenticated message producers to disrupt delivery to
CVE-2026-89406	The Modula Image Gallery - Photo Grid & Video Gallery plugin for WordPress is vulnerable to unauthorized disclosure of private gallery contents in versions up to, a
CVE-2026-91777	Forward-reference completion for @JsonIdentityInfo object IDs in FasterXML jackson-databind performs a linear scan of the pending-reference accumulator for ever the repeated linear lookup with a keyed pending-reference structure.
CVE-2026-91776	TypeDeserializerBase._findDeserializer() in FasterXML jackson-databind caches the resolved deserializer under the raw, attacker-supplied type ID. When name-bas bounds both the number of cached entries and the length of a cacheable type ID.
CVE-2026-13456	The WP Maps - Google Maps,OpenStreetMap,Mapbox,Store Locator,Listing,Directory & Filters plugin for WordPress is vulnerable to Local File Inclusion in all version
CVE-2026-89425	UTF8DataInputJsonParser._reportInvalidToken() in FasterXML jackson-core builds the offending-token text for its error message by appending Java identifier charac OutOfMemoryError for the whole JVM. UTF8DataInputJsonParser was introduced in 2.8.0 together with createParser(DataInput); releases before 2.8.0 do not contain
CVE-2026-88388	Espruino 2v29 (commit bffc6d0) contains a stack-based buffer overflow vulnerability in the JavaScript error stack-trace handling path on 64-bit builds. A remote att
CVE-2026-88376	Bento4 1.6.0.0 contains an integer underflow vulnerability in AP4_AvccAtom::Create() and AP4_HvccAtom::Create(). A specially crafted MP4 file containing an avcC
CVE-2026-88373	libde265 commit 4d45a6b contains a NULL pointer dereference vulnerability in the NAL parsing path. When de265_push_NAL() is called with a zero-length NAL unit
CVE-2026-77193	The eesy_ID2WP - Publish InDesign HTML5 plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.0.3 via the `id2wp_path` para
CVE-2026-96272	ClipBucket v5 before 5.5.3-#182 contains a blind SQL injection vulnerability in the photo search endpoint where the query parameter is passed unsanitized into SQ
CVE-2026-88372	libsndfile 1.2.2 contains an integer overflow vulnerability in mat4_read_header() when parsing crafted MAT4 (MATLAB v4) files.
CVE-2026-	Froxlor through 2.3.10 stores only a numeric user ID in remembered-2FA tokens (panel_2fa_tokens) without recording the account namespace, and the remembere

100709	
CVE-2026-97057	redis-parser through 3.0.0 fails to validate the multi-bulk length value in RESP protocol parsing, allowing attackers to trigger an uncaught RangeError by supplying
CVE-2026-92550	A pre-authentication attacker could leverage type size/count handling to cause excessive allocation leading to potential denial of service. This issue affects Apache
CVE-2026-100672	The Comments plugin (getgrav/grav-plugin-comments) for Grav CMS through version 1.2.10 registers an admin handler that returns comment data as JSON withou
CVE-2026-100662	Netty's HTTP/3 codec (io.netty:netty-codec-http3) versions 4.2.0.Final through 4.2.17.Final contain an uncontrolled resource consumption vulnerability in the QPAC growth and OutOfMemoryError, resulting in denial of service. Fixed in 4.2.18.Final.
CVE-2026-100663	Netty's HTTP/3 codec (io.netty:netty-codec-http3) from 4.2.2.Final through 4.2.17.Final does not special-case HTTP/1 CONNECT authority-form request-targets whe
CVE-2026-100664	Netty's HTTP/3 codec (io.netty:netty-codec-http3) versions 4.2.2.Final through 4.2.17.Final builds the HTTP/3 :authority pseudo-header from the HTTP/1 Host heade impact only (no code execution, memory corruption, or availability impact). Fixed in 4.2.18.Final.
CVE-2026-100665	Netty versions from 4.2.11.Final before 4.2.18.Final contain an incomplete hostname verification fix in the QUIC certificate verification path when using a plain X50
CVE-2026-85081	The File Manager WordPress plugin before 8.0.5, FileOrganizer WordPress plugin before 1.2.1, File Manager Pro WordPress plugin before 2.1.3 do not correctly valid
CVE-2026-97562	In the Linux kernel, the following vulnerability has been resolved: smb: client: pin DFS superblock in iterator callback tcon_super_cb() stores a raw superblock point
CVE-2026-97557	In the Linux kernel, the following vulnerability has been resolved: smb: client: avoid leaking refcount in cifs_queue_oplock_break() cifs_queue_oplock_break() uncor reference before it has been taken.
CVE-2026-97536	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Fix use-after-free of qpair work on queue teardown The response queue MSI-X han >qpair and ha->wq to match the INIT_WORK() condition and avoid operating on an uninitialized work_struct.
CVE-2026-92560	A pre-authentication attacker could leverage type size/count handling to cause excessive allocation leading to potential denial of service. This issue affects Apache
CVE-2026-97531	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Skip vport under deletion in report ID acquisition qla24xx_report_id_acquisition() fo the existing guard in qla2x00_alert_all_vps().
CVE-2026-100690	Hugo versions from v0.161.0 through v0.165.0 run Node.js tools (css.PostCSS, css.TailwindCSS, js.Babel) under the Node.js permission model to restrict file system
CVE-2026-97524	In the Linux kernel, the following vulnerability has been resolved: mptcp: avoid unneeded actions on subflow reset Once in a blue moon, the mptcp receive path ca
CVE-2026-97523	In the Linux kernel, the following vulnerability has been resolved: mptcp: close race between scheduler and state change The mptcp scheduler may race with subfl
CVE-2026-100692	Hugo is a static site generator. In versions after v0.123.0 and before v0.166.0, Hugo's symlink confinement checks stopped at the mount root itself, so a theme or i
CVE-2026-100700	nodemailer before 10.0.6 contains a denial of service vulnerability in the addressparser free-text fallback regex pattern that exhibits quadratic backtracking behav
CVE-2026-92564	A pre-authentication attacker could leverage type nesting to cause a StackOverflowError potentially leading to denial of service. This issue affects Apache Qpid Bro
CVE-2026-51995	An issue in geelen mcp-remote 0.1.32 through 0.1.38 allows a remote attacker to obtain sensitive information via the src/lib/authorization-server-metadata.ts, src/l
CVE-2026-96532	The Testimonials Widget WordPress plugin through 4.0.4 does not perform a capability or ownership check when handling its front-end testimonial submission form
CVE-2026-	Moquette is a lightweight Java MQTT broker. Prior to 0.18.1, the broker does not enforce a maximum length for pending per-session message queues. When a fast

95845	
CVE-2026-61816	zbateson/mail-mime-parser is a mail mime parser alternative to PHP's imap* functions and Pear libraries for reading messages in Internet Message Format RFC 822 receive patches; users on those lines should upgrade to a fixed release. (Versions prior to 2.0 used a different parser and are not affected by all three paths.) These
CVE-2026-57443	SCBE-AETHERMOORE is a geometric AI governance and evaluation framework. Starting in version 4.0.2 and prior to version 4.2.1, the AetherBrowser API server (`s
CVE-2026-91765	cleanup_xml_node() in the SOAP XML parser recurses once per XML nesting level with no depth limit. An unauthenticated attacker can post a SOAP request contain
CVE-2026-95846	Moquette is a lightweight Java MQTT broker. Prior to 0.18.1, PostOffice.publishWill publishes a client's Last-Will message without applying the canWrite authorizati
CVE-2026-95847	Moquette is a lightweight Java MQTT broker. Prior to 0.18.1, H2PersistentQueue derives a session's message-map name as queue_ plus the client ID and its metadata
CVE-2026-88368	NanoSVG commit 239e102ec contains an incorrect numeric conversion vulnerability in the rasterizer's nsvg__addActive() function. A specially crafted SVG docume
CVE-2026-63645	OpenObserve is a cloud-native observability platform. Prior to 0.90.3, OpenObserve registers the /config/runtime endpoint without authentication and serializes the
CVE-2026-52622	An issue in Wellav Technologies Co., Ltd Wellav WES Emergency Broadcast Terminal WES100, WES270, WES280, and WES290 before 08-08-2023 allows a remote att
CVE-2026-71540	Wazuh is an open-source security platform providing unified XDR and SIEM protection for endpoints and cloud workloads. From 3.9.0 until 4.14.7, wazuh-clusterd in
CVE-2026-100558	OpenClaw versions before 2026.8.1 contain a resource exhaustion vulnerability in the Gateway listener that allows unauthenticated clients to retain response socke
CVE-2026-88421	Incorrect access control in the BlogPage.get_entries() component of APSL puput v1.2.1 through v2.2.0 allows unauthenticated attackers to view restricted blog entri
CVE-2026-50547	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. Prior to 1.7.2, InvoicePlane's Invoices::generate_xml() method c
CVE-2026-49850	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. Prior to 1.7.2, InvoicePlane exposes Invoices::delete() and Invoi
CVE-2026-97362	HFS2 version 2.4.0 and earlier contains a denial of service vulnerability that allows unauthenticated attackers to cause a complete and persistent loss of availability
CVE-2026-95513	Unauthenticated Broken Access Control in Online Booking & Scheduling Calendar for WordPress by vcita <= 4.6.0 versions.
CVE-2026-84884	IBM Guardium Data Protection 12.2 stores internal REST service-account passwords in a reversible plaintext-equivalent format. An authenticated attacker who gain
CVE-2026-85029	IBM Guardium Data Protection 12.2 could allow a remote attacker to obtain sensitive information, delete arbitrary files, or execute arbitrary code due to improper l
CVE-2026-96541	A denial-of-service flaw was found in gnome-remote-desktop. An unauthenticated remote attacker can open RDP connections without completing the handshake an
CVE-2026-95604	Unauthenticated Broken Access Control in Loops & Logic <= 4.2.4 versions.
CVE-2026-97508	In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Set tb->root_switch to NULL when domain is stopped Similarly what we do with the f
CVE-2026-100543	OpenClaw (npm package openclaw) before 2026.8.1 could include deterministic hashes computed over the original, unredacted configuration in redacted configur
CVE-2026-61814	Jawn is an open source JSON parser. Prior to 1.7.0, Jawn's AsyncParser can perform quadratic work when a single JSON token is delivered across many small chunks

CVE-2026-100541	OpenClaw's Matrix integration (npm package @openclaw/matrix) versions >= 2026.2.2 and < 2026.8.1 lowercase complete Matrix user IDs — including historical I
CVE-2026-61695	Wire provides gRPC and protocol buffers for Android, Kotlin, Swift, and Java. Prior to 6.4.1 and 7.0.0-alpha04, Wire's Swift runtime ProtoReader.skipGroup(expected
CVE-2026-59990	Jawn is an open source JSON parser. Prior to 1.7.0, Jawn parse methods accept arbitrarily deep JSON array and object nesting without a depth limit, allowing a remc
CVE-2026-84882	IBM Guardium Data Protection 12.2 is vulnerable to path traversal in the Universal Connector Oracle Wallet upload component. An authenticated remote attacker c
CVE-2026-57440	The EmbedVideo Extension is a MediaWiki extension which adds a parser function called #ev and various parser tags for embedding video clips from various video
CVE-2026-100535	OpenClaw (npm package 'openclaw') versions >= 2026.4.5 and < 2026.8.1 can lose the originating requester's restrictions and untrusted provenance when sessio
CVE-2026-86065	Klever-Go is the Go implementation of the Klever blockchain protocol. Prior to 1.7.20, the default-open GET /subscribe endpoint in network/api/websocket/routes.gc
CVE-2026-77422	JLine is a Java library for handling console input. From 3.0.0 until 3.30.15 and 4.3.1, the JLine built-in grep command in builtins/src/main/java/org/jline/builtins/Posix
CVE-2026-61782	Rsdactor is a build analyzer tailored for projects built with Rspack. Prior to version 1.5.16, the default Rsdactor report HTTP server started by `@rsdoctor/rspack-pl
CVE-2026-5267	Ciena Navigator Network Control Suite (NCS) contains an information exposure vulnerability in an event-streaming API that does not properly enforce authenticatio
CVE-2026-88362	MuJS e892c9fdb contains an incorrect numeric conversion vulnerability in jsR_isindex() in jsrun.c. A specially crafted JavaScript input containing an excessively larg
CVE-2026-100208	Integer overflow or wraparound in Microsoft Office Outlook allows an unauthorized attacker to execute code over a network.
CVE-2026-73591	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Inclusion of Sensitive Information in Source Code vulnerability. An un
CVE-2026-98050	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_ptp: Fix napi_gro_receive() call from GC workqueue context Currently mlxsw_sp stale. It states that mlxsw_sp1_ptp_unmatched_finish() invokes netif_receive_skb(). This has not been accurate since the referenced commit; this patch makes that tainted 6.18.48 #1-NixOS PREEMPT(lazy) Hardware name: Mellanox Technologies Ltd. MSN2410/VMOD0001, BIOS 4.6.5 09/13/2018 RIP: 0010: __list_add_valid_or_n kthread+0xfb/0x260 ret_from_fork+0x22d/0x260 ret_from_fork_asm+0x1a/0x30 </TASK> Kernel panic - not syncing: Fatal exception in interrupt The machinery tl
CVE-2026-82356	Imprivata EAM <=26.2.6 lacks the ability to rotate its RSA key pair after deployment when generating an X.509 certificate. Using an RSA key pair indefinitely for ce
CVE-2026-95844	Moquette is a lightweight Java MQTT broker. Prior to 0.18.1, Moquette does not limit the depth of topic names and topic filters before processing them through recu
CVE-2026-77423	JLine is a Java library for handling console input. From 3.0.0 until 3.30.15 and 4.3.1, the JLine built-in less viewer passes user-controlled search and display-filter pa
CVE-2026-98108	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: fix chan mode for LE_CONN_REQ + EXT_FLOWCTL pchan l2cap_new_connectio
CVE-2026-96673	Photoview through 2.4.0 contains an SQL injection vulnerability in the album download route that allows unauthenticated attackers to inject SQL by manipulating tl
CVE-2026-75907	The door access control on a Norwegian Cruise Line asset grants entry based only on the credential's static 7-byte UID stored on an NTAG212 NFC chip. A UID is a i
CVE-2026-100560	OpenClaw versions before 2026.8.1 contain an authorization bypass vulnerability where Allow Always approvals for exact commands persist as path-only grants on
CVE-2026-19888	Missing validation of a mandatory attribute in the SCRAM client-final-message parser in PgBouncer through 1.25.2 allows an unauthenticated remote attacker to cr

CVE-2026-6668	Integer overflow in the packet buffer growth logic in PgBouncer through 1.25.2 allows an unauthenticated remote attacker to cause a denial of service. Sufficiently
CVE-2026-10758	Esri LERC is an open-source image or raster format which supports rapid encoding and decoding for any pixel type. A Heap based Out-of-Bounds Write via Integer (C
CVE-2026-88830	A unit confusion in BusyBox TLS Montgomery reduction buffer allocation causes a pre-authentication heap buffer overflow when processing a crafted ClientKeyExch
CVE-2026-95842	Moquette is a lightweight Java MQTT broker. Prior to 0.18.1, SessionEventLoop.run catches only InterruptedException, and SessionEventLoopGroup does not restart
CVE-2026-95843	Moquette is a lightweight Java MQTT broker. Prior to 0.18.1, PostOffice.subscribe parses a shared-subscription filter through SharedSubscriptionUtils.extractShareN
CVE-2026-98056	In the Linux kernel, the following vulnerability has been resolved: nvme: remove stale namespaces by NSID range during scan nvme_scan_ns_list() drops the stale that stops once end is reached. This bounds the work by the namespaces that are present instead of by the size of the gap.
CVE-2026-57178	Python Social Auth is a social authentication/registration mechanism. Prior to version 5.0.0, the `vk-app` backend accepted VK application callback data without ve
CVE-2026-97474	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mld: purge async notifications upon nic error This fixes a kernel panic in reconfig failt ieee80211_handle_reconfig_failure in (6), it is also not a good idea to carry and maybe handle notifications from a dead FW. We do purge the notifications when we
CVE-2026-93543	An out-of-bounds read in libXi's Xi2 class parser in libXi before 1.8.4 could be used by malicious X servers to crash an attached X client.
CVE-2026-88907	Incorrect Authorization vulnerability in TÜBİTAK ULAKBİM UlakPDF allows Authentication Bypass. This issue affects UlakPDF: through 09092026.
CVE-2026-100390	Zoraxy versions 3.2.3 through 3.3.4 fail to properly parse IPv6 addresses in the RemoteAddr field when setting forwarded headers. Unauthenticated attackers contr
CVE-2026-61788	DBHub is a database MCP server for Postgres, MySQL, SQL Server, Oracle, MariaDB, SQLite. Prior to version 0.22.6, setting `readonly = true` on the `execute_sql` f
CVE-2026-94181	An address bar spoofing issue in affected versions of Arc could allow an attacker to spoof the browser address bar via a <select> element that triggers requestFull
CVE-2026-93225	In the Linux kernel, the following vulnerability has been resolved: phy: fsl-imx8mq-usb: fix typec switch leak on probe error path If probe fails after imx95_usb_phy_
CVE-2026-97737	In Wakapi before 2.17.6, the user caching service allows a lookup to be resolved in an unintended lookup context, leading to account takeover.
CVE-2026-96808	In Flatpak before 1.18.1, the revokefs writer, used by the flatpak-system-helper to receive repository data from unprivileged callers, validated file paths by rejectin
CVE-2026-94183	Arc Search for Android before version 1.12.10 does not display a fullscreen notification when a page enters fullscreen mode while the app is running in the backgro
CVE-2026-18184	IBM Financial Transaction Manager (FTM) for RedHat OpenShift could allow a remote attacker to obtain sensitive information due to an XML external entity (XXE) in
CVE-2026-42801	NULL pointer dereference vulnerability in ASR Crane , Falcon on Linux (as_rrc module) allows Pointer Manipulation. This vulnerability is associated with program file
CVE-2026-76980	ZohoCorp ManageEngine OpManager and Firewall Analyzer versions 12.8.709 and below were vulnerable to a Data Exposure vulnerability in the Firewall Analyzer s
CVE-2026-94612	authentik is an open-source identity provider. Prior to 2026.2.7, 2026.5.7, and 2026.8.2, an authentik SAML Source verifies an assertion's signature and validity per
CVE-2026-86247	Race condition within a thread vulnerability in Apache Tomcat Native allowed client certificate verification requirements to be down-graded for some configurations

CVE-2026-93260	In the Linux kernel, the following vulnerability has been resolved: powerpc/xive: propagate IPI init errors to prevent use-after-free When xive_init_ipis() fails (e.g. irc
CVE-2026-98096	In the Linux kernel, the following vulnerability has been resolved: ipv6: sr: restore network header before routing and forwarding ipv6_srh_rcv() runs with skb->dat dissection as well as downstream forwarding. On the loopback path, pull skb_transport_offset(skb) to restore skb->data to the SRH before looping back.
CVE-2026-73588	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains a Missing Authentication for Critical Function vulnerability. An unauthent
CVE-2026-18875	IBM Financial Transaction Manager (FTM) for RedHat OpenShift is vulnerable to RAG poisoning via unauthenticated runbook upsert (CWE-74) in the FTM AI agent se
CVE-2026-97882	A weakness has been identified in mathurvishal CloudClassroom-PHP-Project up to 5dadec098bfbbf3300d60c3494db3fb95b66e7be. The impacted element is an ur
CVE-2026-72668	Unintended Proxy or Intermediary ('Confused Deputy') (CWE-441) in Kibana Agent Builder can lead to privilege escalation. A non-administrative user able to edit a
CVE-2026-97182	A security vulnerability has been detected in halo-dev Halo up to 2.25.4/2.26.1. Affected is an unknown function of the file application/src/main/java/run/halo/app/c
CVE-2026-97324	A vulnerability was identified in YunaiV/zhijiantianya ruoyi-vue-pro up to 2026.08. Affected is the function updateDemoOrderPaid of the file yudao-module-pay/src/r
CVE-2026-100315	A vulnerability was detected in mathurvishal CloudClassroom-PHP-Project up to 5dadec098bfbbf3300d60c3494db3fb95b66e7be. Affected is an unknown function c
CVE-2026-18185	IBM Financial Transaction Manager (FTM) for RedHat OpenShift could allow a remote attacker to access sensitive information and modify system configurations due
CVE-2026-96751	A vulnerability has been found in pmTicket Project-Management-Software up to 078fa56a782490c5059a0814f84df27984f4d7e2. This affects the function setSync c
CVE-2026-97646	A weakness has been identified in ningzichun student-management-system up to 98760f5711cf6dc8b4adca53a9e207ca49b02ebf. This affects an unknown functio
CVE-2026-100314	A security vulnerability has been detected in mathurvishal CloudClassroom-PHP-Project up to 5dadec098bfbbf3300d60c3494db3fb95b66e7be. This impacts an unk
CVE-2026-97878	A vulnerability was identified in zhistaredu StarTraining up to 3.8.1. Impacted is the function anonymous of the file /druid/index.html of the component Druid Consc
CVE-2026-95927	A vulnerability was identified in SourceCodester Online Reviewer Management System 1.0. This affects an unknown function of the file /reviewer_0/admins/assessn
CVE-2026-95926	A vulnerability was determined in SourceCodester Online Reviewer Management System 1.0. The impacted element is an unknown function of the file /reviewer_0/
CVE-2026-97883	A security vulnerability has been detected in mathurvishal CloudClassroom-PHP-Project up to 5dadec098bfbbf3300d60c3494db3fb95b66e7be. This affects an unkn
CVE-2026-97885	A flaw has been found in mathurvishal CloudClassroom-PHP-Project up to 5dadec098bfbbf3300d60c3494db3fb95b66e7be. Affected is an unknown function of the f
CVE-2026-95925	A vulnerability was found in SourceCodester Online Reviewer Management System 1.0. The affected element is an unknown function of the file /reviewer_0/admins
CVE-2026-95924	A vulnerability has been found in SourceCodester Online Reviewer Management System 1.0. Impacted is an unknown function of the file /reviewer_0/admins/asses:
CVE-2026-97231	A vulnerability was found in volotat Anagnorisis up to 0.3.1/0.4.0. Affected is an unknown function of the file app.py of the component Socket.IO Connect Interface.
CVE-2026-78437	Incomplete cleanup vulnerability in Apache Tomcat allows a malformed request to potentially (depends on timing) cause one request from another user to fail. This

CVE-2026-93901	The Optima Express IDX plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 8.7.5. This is due to the `provisionBlogCreder username before the plugin has had the opportunity to provision that login for its own integration account.
CVE-2026-97877	A vulnerability was determined in zhistaredu StarTraining up to 3.8.1. This issue affects the function UserLoginService.createToken of the file application.yml of the
CVE-2026-96762	A vulnerability was determined in kvcache-ai mooncake up to 0.3.12/0.3.13.post1. This affects the function UnmountSegment of the component RPC Path Handler.
CVE-2026-97865	A security flaw has been discovered in Open-Web-Analytics up to 1.8.1. Affected is the function Event::loadFromArray of the file queue.php of the component Remo
CVE-2026-100530	OpenClaw versions before 2026.8.1 fail to bind working directory context to reusable exec approvals, allowing approved commands to execute in different director
CVE-2026-100666	Netty's HttpServerCodec (io.netty:netty-codec-http) in versions 4.2.0.Final through 4.2.16.Final and in versions up to and including 4.1.136.Final pairs each outboun
CVE-2026-86938	A DLL hijacking vulnerability in the FileMaker Pro installer for Windows allowed a local user to execute arbitrary code with elevated administrator privileges by plac
CVE-2026-96803	A vulnerability was identified in java110 MicroCommunity up to 2.0. Affected is the function QueryServiceSMOImpl.fallBack of the file BusinessApi.java of the comp
CVE-2026-96604	A vulnerability was identified in SoftNews Media Group DataLife Engine 18.0. This affects the function strip_data of the file engine/modules/search.php of the comp
CVE-2026-96603	A vulnerability has been found in Abdurrab5 online-makeup-store. Affected is the function confirm_logged_in/confirm_user of the file functions.php of the compone
CVE-2026-88369	zserge jsmn commit 25647e6 is vulnerable to Buffer Overflow in example/jsondump.c dump().
CVE-2026-96602	A flaw has been found in Abdurrab5 online-makeup-store. This impacts an unknown function of the file customerSignin.php of the component Customer Login Hanc
CVE-2026-96601	A vulnerability was detected in Abdurrab5 online-makeup-store. This affects an unknown function of the file index.php of the component Admin Login Handler. The
CVE-2026-96514	A weakness has been identified in Neethuharii CafeManagement. Impacted is an unknown function of the file CafePortalLogin.php of the component Login Handler.
CVE-2026-96513	A security flaw has been discovered in Neethuharii CafeManagement. This issue affects some unknown processing of the file AddProductCode.php. The manipulatio
CVE-2026-96898	A vulnerability was detected in yhx070424 ShopXO up to 2.2.7. Affected by this vulnerability is an unknown functionality of the file config/ueditor.php of the compo
CVE-2026-96556	A flaw has been found in Neethuharii CafeManagement. Affected by this vulnerability is the function addcashier of the file AddCashierCode.php. Executing a manip
CVE-2026-94243	A vulnerability in Apache Sling Security Bundle: the ReferrerFilter accepts weaker-than-orgen evidence. This issue affects Apache Sling Security Bundle: before 1.3.:
CVE-2026-61823	code16 Sharp is a Laravel-based framework for building content-management and administrative interfaces. Versions before 9.22.5 contain a stored cross-site scri
CVE-2026-88832	BusyBox romfs volume ID parsing uses unbounded strlen on attacker-controlled metadata, causing a heap buffer overflow when processing crafted filesystem ima
CVE-2026-75973	Improper Authentication vulnerability in Apache Tomcat. When Jakarta Authentication was configured with SimpleAuthConfigProvider as the default provider and m
CVE-2026-97871	A vulnerability has been found in Zhonglun CloudPos up to 3.0.1.76. This issue affects the function OpenLocalBrowser of the file ZIPos/ZIPos/Bizlogic/JSBridge.cs of
CVE-	

CVE-2026-97326	A weakness has been identified in songxinjianqwe Chat up to ac63d25297079eed5e4ba7e88d3b7a032637150d. Affected by this issue is some unknown functional
CVE-2026-61815	zbateson/mail-mime-parser is a mail mime parser alternative to PHP's imap* functions and Pear libraries for reading messages in Internet Message Format RFC 822 any filename before passing it to attachment APIs, and from the result of getFilename() before reusing it in a constructed message — e.g. preg_replace('/[\r\n]+/', ' ')
CVE-2026-91123	Discourse is an open-source discussion platform. Prior to 2026.1.8, 2026.6.3, 2026.7.2, and 2026.8.0, the iframe src traversal guard did not treat literal backslashes
CVE-2026-84862	IBM Guardium Data Protection 12.2 is vulnerable to insecure deserialization in the Quartz JDBC job store. An authenticated attacker could exploit this vulnerability to
CVE-2026-83591	The AMP for WP – Accelerated Mobile Pages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content via Regex Transformation in all
CVE-2026-88843	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.50 does not validate one of its display-style settings before using it to build a template path, a
CVE-2026-94573	The Repeater Fields for Elementor Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Repeater Field Value in all versions up to, and includi
CVE-2026-16591	The WP Directory Kit WordPress plugin before 1.5.8 does not sanitize and escape some of its category and location fields before outputting them in page attributes
CVE-2026-95864	The Themify Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'css[fonts]' Parameter in all versions up to, and including, 7.8.1 due to insu
CVE-2026-95866	The User Profile Builder – Beautiful User Registration Forms, User Profiles & User Role Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Av
CVE-2026-95603	Shop manager PHP Object Injection in Reycob Product Import Export <= 2.3.0 versions.
CVE-2026-96568	The Restaurant Menu and Food Ordering plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'phone_number' parameter in all versions up to, a
CVE-2026-96752	The Zero Spam for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Nested POST Array Keys via Contact Form 7 Integration in all ver
CVE-2026-96656	Plex Media Server before 1.43.3.10861 allows an admin user to write arbitrary files that may be executed on load. The preference TranscoderH264Options is apper
CVE-2026-75886	A flaw was found in openshift/console. An unauthenticated remote attacker can exploit a misconfiguration in the CatalogdHandler, which lacks proper authenticati
CVE-2026-100372	ClipBucket v5 before 5.5.3-#197 contains a path traversal vulnerability in the admin template editor that allows authenticated administrators to overwrite PHP files
CVE-2026-97060	X-SpringBoot through 6.0 lacks object-level authorization in user management endpoints, allowing sub-administrators to modify or delete users without ownership
CVE-2026-42324	Piwigo is a full featured open source photo gallery application for the web. Prior to 16.4.0, admin/element_set_ranks.php stores administrator-controlled image_ord
CVE-2026-42323	Piwigo is a full featured open source photo gallery application for the web. Prior to 16.4.0, admin/batch_manager.php accepts administrator-controlled dimension w
CVE-2026-85475	A flaw was found in the Ansible Automation Platform automation controller. The external logging (rsyslog) configuration is generated by interpolating user-controlle
CVE-2026-33639	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. Prior to 1.7.2, InvoicePlane interpolates the administrator-contr
CVE-2026-93654	The Premium Packages – Sell Digital Products Securely plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'cart_items[][product_name]' Paramete
CVE-	

CVE-2026-85750	Piwigo before v16.4.0 is vulnerable to arbitrary file read and remote code execution in image upload handling when using the Imagick library due to insufficient val
CVE-2026-84281	The Fancy Product Designer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'productTitle' in ' '_fpd_data' Order Item Meta in all versions up to, a
CVE-2026-84280	The Fancy Product Designer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Order 'elements[]'.title' Parameter in all versions up to, ,
CVE-2026-84279	The Fancy Product Designer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'output_format' parameter in all versions up to, and including,
CVE-2026-100612	Capgo (capgo.app) through version 12.261.0 contains an incomplete access-control fix for the public.sso_providers table. Migration 20260826100000_sso_provider existing owner account, nulls its password, and deletes its other identities and sessions. This results in vertical privilege escalation from org_admin to org owner/su
CVE-2026-93303	The HT Contact Form - Drag & Drop Form Builder for WordPress plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via 'form_data' Rich T
CVE-2026-94367	OpenEye Apex Network Video Recorder (NVR) firmware 3.2.9.376 contains an OS command injection vulnerability in recbackup. An authenticated administrator can
CVE-2026-96039	The BA Book Everything plugin for WordPress is vulnerable to Stored Cross-Site Scripting via first_name Parameter in all versions up to, and including, 1.8.27 due to
CVE-2026-96744	Improper neutralization of special elements in data query logic in the cache lock implementation of the MongoDB integration for Laravel can cause a caller-supplied
CVE-2026-93622	Unauthenticated Cross Site Scripting (XSS) in WPS Limit Login <= 1.5.9.3 versions.
CVE-2026-93774	Unauthenticated Cross Site Scripting (XSS) in WP Photo Album Plus <= 9.3.02.002 versions.
CVE-2026-94176	Unauthenticated Cross Site Scripting (XSS) in Mang Board WP <= 2.4.1 versions.
CVE-2026-94179	Unauthenticated Cross Site Scripting (XSS) in Razorpay Payment Button <= 2.4.9 versions.
CVE-2026-18177	IBM Financial Transaction Manager (FTM) for RedHat OpenShift could allow a remote attacker to execute unauthorized payment actions due to missing authorizati
CVE-2026-95515	Unauthenticated Cross Site Scripting (XSS) in Ninja Forms <= 3.15.3 versions.
CVE-2026-82094	IBM DataStage on Cloud Pak for Data 5.4.0.0 could allow a remote authenticated attacker to traverse directories on the system due to improper limitation of a path
CVE-2026-93306	IBM Server Firmware FW1120.00 through FW1120.01, FW1110.00 through FW1110.31, FW1060.00 through FW1060.81, and FW950.00 through FW950.H3 is affect
CVE-2026-95528	Unauthenticated Cross Site Scripting (XSS) in Core Web Vitals & PageSpeed Booster <= 1.0.31 versions.
CVE-2026-95529	Unauthenticated Cross Site Scripting (XSS) in Calculated Fields Form <= 5.5.1.1 versions.
CVE-2026-95590	Subscriber SQL Injection in Tainacan <= 1.2.0 versions.
CVE-2026-93526	Unauthenticated Cross Site Scripting (XSS) in Event Tickets <= 5.29.4 versions.
CVE-2026-96271	Photoview through 2.4.0 contains an authorization bypass vulnerability in the shareAlbum GraphQL mutation that allows authenticated users to create share links f
CVE-	

CVE-2026-97520	In the Linux kernel, the following vulnerability has been resolved: gfs2: move quota_init qc iterator increment Move qc++ from the loop body into the for-loop incre
CVE-2026-97731	MinIO through 7aac2a2 does not verify that every x-amz-* header present on a request also appears in the client-supplied X-Amz-SignedHeaders list. extractSigned
CVE-2026-100718	Froxlor through 2.3.10 does not enforce the mail.allow_external_domains policy in the EmailSender.add API command. When an administrator has enabled the allo
CVE-2026-97496	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Fix OOB memory exposure in get_wave_state() The get_wave_state() function for v5
CVE-2026-100708	Froxlor before 2.3.13 returns the ssl_key_file column — which stores the raw PEM TLS private-key content — verbatim in the JSON responses of the Certificates.get
CVE-2026-100555	OpenClaw is an npm-distributed gateway application. In versions >= 2026.7.1 and < 2026.8.1, Synology Chat attachment delivery could lose DNS pinning: the Gat
CVE-2026-100625	Capgo (capgo.app) exposes a native build TUS upload proxy (supabase/functions/_backend/public/build/upload.ts) that authorizes a caller against a single build job
CVE-2026-97438	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: validate index entry key bounds [BUG] A malformed NTFS directory index entry can adv dir_search_u+0x2c0/0x460 fs/ntfs3/dir.c:254 ntfs_lookup+0x1cc/0x2a0 fs/ntfs3/namei.c:85 __lookup_slow+0x241/0x450 fs/namei.c:1816 lookup_slow fs/namei.c:1 indx_find+0x447/0x900 fs/ntfs3/index.c:1179 dir_search_u+0x2c0/0x460 fs/ntfs3/dir.c:254 ntfs_lookup+0x1cc/0x2a0 fs/ntfs3/namei.c:85 __lookup_slow+0x241/0x
CVE-2026-93816	In the Linux kernel, the following vulnerability has been resolved: f2fs: validate inline dentry name lengths before conversion Inline dentry conversion copies name
CVE-2026-84789	ZohoCorp ManageEngine OpManager and Firewall Analyzer versions 12.8.710 and below were vulnerable to a Broken Access Control vulnerability that allowed an a
CVE-2026-100598	OpenClaw (npm package openclaw) before 2026.7.1 incorrectly binds Signal approval reactions. In affected versions, a reaction intended to resolve a structured ap
CVE-2026-84791	ZohoCorp ManageEngine OpManager and Firewall Analyzer versions 12.8.710 and below were vulnerable to a Broken Access Control vulnerability that allowed an a
CVE-2026-93229	In the Linux kernel, the following vulnerability has been resolved: nfsd: add missing read barrier to rpc_status_get dumpit seqcount retry The hand-rolled seqcount- read_seqcount_retry() does. [cel: Use READ_ONCE instead of smp_load_acquire()]
CVE-2026-100605	Flowise through 3.1.4 contains missing route-level RBAC checks on chat message endpoints that allow low-privileged API keys to read and delete chat history. Atta
CVE-2026-86679	ZohoCorp ManageEngine Applications Manager versions 182000 and below were vulnerable to a permissions validation issue that allowed a low-privileged user to i
CVE-2026-97437	In the Linux kernel, the following vulnerability has been resolved: ntfs3: fix out-of-bounds read in ntfs_dir_emit() and hdr_find_e() The bounds check in ntfs_dir_emit hdr_find_e() to ensure the declared key_size does not exceed the available entry data, preventing comparison functions from reading past entry boundaries on the
CVE-2026-96750	MongoDB Compass can interpolate a database name without escaping into the initial input of its embedded MongoDB shell when a user opens the shell from that c
CVE-2026-82164	Dell Trusted Device Client, versions prior to 8.1.359.0, contain an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with
CVE-2026-84714	A flaw was found in the automation-controller input-validation guard sanitize_jinja(). The function uses two regular expressions to reject user-supplied Jinja, but the
CVE-2026-48070	Docmost is open-source collaborative wiki and documentation software. Prior to 0.80.1, authenticated users can store attacker-controlled avatarUrl values that are
CVE-2026-77293	TREK is a collaborative travel planner. Prior to 3.3.0, the DELETE /api/trips/:tripld/collab/notes/:noteld/files/:fileld endpoint authorizes an authenticated user against
CVE-2026-93796	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: pcie: null RX pointers after free When iwl_pcie_tx_init() fails after RX init, nic init unwi
CVE-	

CVE-2026-100419	gitoxide gix-fs before 0.23.0 contains a path validation bypass vulnerability in the worktree checkout mechanism that allows attackers to escape the worktree direc
CVE-2026-97608	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_log: unregister loggers before per-net teardown nf_log_syslog and nfnetlink_log unreg period after the pre-exit callback clears the per-net selection, while nf_log_unregister() continues to cover readers of the global logger table. Apply this ordering fix
CVE-2026-97609	In the Linux kernel, the following vulnerability has been resolved: netfilter: cttimeout: prevent UAF during module unload nf_ct_set_timeout() protects the timeout f unregister_pernet_operations+0x232/0x490 unregister_pernet_subsys+0x1c/0x30 cttimeout_exit+0x52/0x970 [nfnetlink_cttimeout] Clear the hook and wait for ex
CVE-2026-97926	In the Linux kernel, the following vulnerability has been resolved: ufs: validate cylinder group metadata before caching it ufs_read_cylinder() copies the cylinder gr group being read, or whose rotors fall outside the group, before the metadata is cached. Valid filesystems keep cg_cgx equal to the group number and the rotors w
CVE-2026-100310	GNU libextractor before 1.16 loads plugins from an untrusted search path specified by the LIBEXTRACTOR_PREFIX environment variable without proper privilege ch
CVE-2026-97589	In the Linux kernel, the following vulnerability has been resolved: s390/crypto: Fix wrong return code to engine in asynch callbacks When crypto_finalize_hash_req
CVE-2026-100504	Ghidra versions through 12.1.4 contain a stack-based out-of-bounds write vulnerability in the decompiler's leftshift128 function when processing negative shift am
CVE-2026-97931	In the Linux kernel, the following vulnerability has been resolved: ALSA: us122l: Prevent write upgrades for read mappings The hwdep mmap callback rejects read-
CVE-2026-97953	In the Linux kernel, the following vulnerability has been resolved: net: stmmac: fix TX descriptor availability check for TSO traffic stmmac_tso_xmit() estimates the availability check.
CVE-2026-98027	In the Linux kernel, the following vulnerability has been resolved: net: dsa: mv88e6xxx: bound the policy rule dump by the caller's buffer size mv88e6xxx_get_rxnf
CVE-2026-98029	In the Linux kernel, the following vulnerability has been resolved: eth: nfp: bound the ntuple rule dump by the caller's buffer size nfp_net_get_fs_loc() dumps every
CVE-2026-93810	In the Linux kernel, the following vulnerability has been resolved: cachefiles: Fix double fput Fix a double fput() in error handling in cachefiles_create_tmpfile()).
CVE-2026-93801	In the Linux kernel, the following vulnerability has been resolved: smb/client: zero-initialize stack-allocated cifs_open_info_data Stack-allocated cifs_open_info_data
CVE-2026-98154	In the Linux kernel, the following vulnerability has been resolved: nvme-rdma: fix -EIO cleanup order in queue_rq On -EIO, the RDMA queue_rq path reports a host p
CVE-2026-98150	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix BPF_F_CPU validation for sparse CPU IDs BPF_F_CPU stores the target CPU ID in the upper valid range and CPUs absent from the possible mask, while allowing valid sparse CPU IDs.
CVE-2026-98030	In the Linux kernel, the following vulnerability has been resolved: net: dsa: bcm_sf2: bound the CFP rule dump by the caller's buffer size bcm_sf2_cfp_rule_get_all()
CVE-2026-98041	In the Linux kernel, the following vulnerability has been resolved: bpf: Don't predict JMP32 pointer vs zero comparisons Consider the following program: r1 = map_\
CVE-2026-98083	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix transaction use-after-free in raid stripe insertion If allocation of a RAID stripe extent fails
CVE-2026-96611	FFmpeg before 9.0 has a signed integer overflow in libavformat/mov.c. In mov_read_ispe(), uint32_t width/height values from a crafted HEIF ispe box are stored int
CVE-2026-74991	The WPForms WordPress plugin before 2.0.2 does not verify that a Stripe payment object supplied during a public form submission belongs to it before acting on it.
CVE-2025-15696	The Real3D Flipbook WordPress plugin before 5.4 does not sanitize or escape several flipbook editor fields before rendering them back in the admin editor, allowing
CVE-2026-86842	The Real3D Flipbook WordPress plugin before 5.4 does not perform capability checks on several of its authenticated flipbook management actions, allowing users v
CVE-	

CVE-2026-85006	The HappyAddons for Elementor WordPress plugin before 3.50.0 does not escape an icon value on one of its button widgets before outputting it inside an HTML att
CVE-2026-92411	The WP Delicious WordPress plugin before 1.10.8 does not validate or escape the HTML tag name taken from user-supplied recipe block data before rendering it or
CVE-2026-73587	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Improper Certificate Validation vulnerability. An unauthenticated atta
CVE-2026-97056	SigNoz versions from v0.98.0 up to (but not including) v0.143.0, when configured to use the opaque session tokenizer (which was not the default before v0.143.0),
CVE-2026-100540	OpenClaw Feishu before 2026.8.1 fails to validate whether a configured default account is disabled before selecting it for model tool operations. Attackers can expl
CVE-2026-88997	The JSM Show Post Metadata WordPress plugin before 4.9.1 does not properly escape a post meta key before outputting it into an inline event-handler attribute in
CVE-2026-80338	The CMB2 WordPress plugin before 2.13.0 does not perform any capability check on one of its AJAX actions, allowing users with a role as low as Subscriber to creat
CVE-2026-89237	The Bluff Post WordPress plugin through 1.1.1 does not sanitise and escape parameters before using them as identifiers in a SQL query, allowing unauthenticated s
CVE-2026-61413	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Improper Privilege Management vulnerability. A low privileged attack
CVE-2026-88956	The Botslab G980H dash camera firmware contains an authentication vulnerability in the root account exposed through the device's UART interface. The affected a
CVE-2026-96531	The Optimole WordPress plugin before 4.2.13 does not escape unrecognized attributes of its video-player block before rendering them onto the block's wrapper ele
CVE-2026-89002	The WPeMatico RSS Feed Fetcher WordPress plugin before 2.8.26 does not sanitize and escape content it retrieves from a user-supplied source before rendering it,
CVE-2026-91024	The Booking Manager WordPress plugin before 2.1.21 does not sanitize and escape values taken from a fetched external iCalendar feed before using them in a SQL
CVE-2026-89005	The WPeMatico RSS Feed Fetcher WordPress plugin before 2.8.26 does not sanitise and escape one of its campaign configuration fields when a certain feature is en
CVE-2026-96445	A flaw was found in the Conditional OTP authenticator of Keycloak, an identity and access management solution. The issue occurs when the system evaluates spec
CVE-2026-94416	An authorization bypass was found in the Ansible Automation Platform (AAP) gateway. The gateway API allows an authenticated administrator to create a new serv
CVE-2026-88916	Incorrect Authorization vulnerability in TÜBİTAK ULAKBİM UlakPDF allows Privilege Escalation. This issue affects UlakPDF: through 09092026.
CVE-2026-100609	Flowise (npm packages `flowise` and `flowise-components`) through 3.1.4 looks up credentials by ID without filtering on the requesting user's workspace (findOne
CVE-2026-97846	Keycloak provides a feature called mTLS holder-of-key binding which ensures that a token can only be used by the client that originally requested it by binding it to
CVE-2026-79959	The Botslab G980H dash camera firmware contains a hard-coded root account password that cannot be changed by the user. An attacker who obtains the firmware
CVE-2026-91073	The Subscribe Forms WordPress plugin before 1.6.3 does not sanitise and escape one of its form settings before outputting it in a page, allowing authenticated use
CVE-2026-57176	Python Social Auth is a social authentication/registration mechanism. Prior to version 5.0.0, the Vend OAuth2 backend used only the numeric Vend user_id as the s
CVE-2026-	BusyBox passwd/group tokenize() references a stale endpoint pointer after trimming, causing an out-of-bounds write of heap pointers.

88839	
CVE-2026-100584	OpenClaw is an npm-distributed agent runtime. In versions >= 2026.2.26 and < 2026.7.1, PowerShell command analysis on Windows hosts running in exec allowli
CVE-2026-97177	A flaw was found in the user update mechanism of the Keycloak Admin REST API. When Fine-Grained Admin Permissions are enabled, the system fails to check for
CVE-2026-84724	An argument-injection flaw was found in the Ansible Automation Platform automation-controller system-job subsystem. The system-job template launch endpoint s
CVE-2026-96448	A flaw was found in the Fine-Grained Admin Permissions (FGAP v2) feature of Keycloak, an identity and access management solution. The issue occurs when the sy
CVE-2026-79761	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. From 1.7.0 until 2.5.1, the Termix SSH key deployme
CVE-2026-84716	A flaw was found in the automation-controller instance install-bundle endpoint. When a System Administrator downloads an execution/hop node's install bundle, th because receptor work submission is gated by a separate signing key not included in the bundle.
CVE-2026-94398	Uncontrolled Resource Consumption (CWE-400) in Elasticsearch can lead denial of service via Excessive Allocation (CAPEC-130)
CVE-2026-94399	Uncontrolled Resource Consumption (CWE-400) in Elasticsearch can lead denial of service via Excessive Allocation (CAPEC-130)
CVE-2026-93545	An out-of-bounds read in libXi's XListInputDevices() in libXi before 1.8.4 could be used by malicious X servers to crash an attached X client.
CVE-2026-97636	Apache Airflow HashiCorp provider: the HashiCorp Vault secrets backend's team-scope guard can be bypassed with a user-controlled key. In a multi-team deploym
CVE-2026-100678	stoatchat before 0.15.5 fails to enforce account-level attempt limits on MFA login challenges, allowing attackers who know a password to guess TOTP codes with or
CVE-2026-94397	Uncontrolled Resource Consumption (CWE-400) in Elasticsearch can lead denial of service via Excessive Allocation (CAPEC-130)
CVE-2026-100668	Grav 2.0.0 through 2.0.24 contain a Twig content sandbox escape. The `array` filter (and its identical function form) is on the sandbox allowlist but is registered wi
CVE-2026-94400	Uncontrolled Resource Consumption (CWE-400) in Kibana can lead denial of service via Excessive Allocation (CAPEC-130)
CVE-2026-95811	Lemonldap::NG::Handler versions from 2.0.0 before 2.16.10, from 2.17.0 before 2.21.6, from 2.22.0 before 2.23.4 for Perl allow an equivalent spelling of a path to l
CVE-2026-100659	Netty's HTTP/3 codec (io.netty:netty-codec-http3) in versions 4.2.0.Final through 4.2.17.Final does not enforce the RFC 9114 requirement that the :authority pseud
CVE-2026-100654	vLLM before 0.29.0 accepts user-controlled stop_token_ids on the OpenAI-compatible POST /v1/completions and POST /v1/chat/completions endpoints but validates
CVE-2026-93544	An out-of-bounds read in libXi's XI2 XIQueryDevice reply parsing in libXi before 1.8.4 can be used by a malicious X server to crash an attached X client.
CVE-2026-88367	NanoSVG 239e102ec contains an incorrect numeric conversion vulnerability in nsvg__curveDivs() during SVG stroke rasterization. A specially crafted SVG documen
CVE-2026-94396	Uncontrolled Resource Consumption (CWE-400) in Elasticsearch can lead denial of service via Excessive Allocation (CAPEC-130)
CVE-2026-82300	Uncontrolled Resource Consumption (CWE-400) in Elasticsearch can lead to denial of service via Excessive Allocation (CAPEC-130).
CVE-2026-	The Better Messages – Chat Rooms, Group Chat, Private Messages & AI Chat Bots plugin for WordPress is vulnerable to generic SQL Injection via 'group_id' Messag

93899	
CVE-2026-82294	Uncontrolled Resource Consumption (CWE-400) in Elasticsearch can lead to denial of service via Excessive Allocation (CAPEC-130).
CVE-2026-78582	Missing Authorization (CWE-862) in Kibana can lead to unauthorized deletion of data via Exploiting Incorrectly Configured Access Control Security Levels (CAPEC-18)
CVE-2026-100719	Froxlор versions before 2.3.12 contain a credential disclosure vulnerability in the DirProtections.listing API command that returns htpasswd password hashes. Authen
CVE-2026-100712	froxlор through 2.3.10 disables a user's two-factor authentication immediately upon an unauthenticated-triggerable GET request to the 2FA management page (e.g
CVE-2026-91133	Discourse is an open-source discussion platform. Prior to 2026.1.8, 2026.6.3, 2026.7.2, and 2026.8.0, authenticated users could supply unescaped SQL LIKE metac
CVE-2026-82708	The Botslab G980H dash camera firmware contains a path traversal vulnerability in its HTTP server. An attacker with access to the device's WiFi network could sub
CVE-2026-100688	Budibase server before 3.45.0 contains a cross-tenant information disclosure vulnerability in the GET /api/applications/:appld/appPackage endpoint that allows aut
CVE-2026-100675	stoatchat versions before 0.15.5 contain a denial of service vulnerability in the acknowledgement worker that processes mass mention messages. Authenticated u
CVE-2026-93542	An out-of-bounds read in libXi's XI2 class parsing via size_classes() and copy_classes() in libXi before 1.8.4 could be used by malicious servers to crash the X client.
CVE-2026-100653	vLLM is an inference and serving engine for large language models. In versions from 0.22.1 through 0.28.0, the operator-supplied model revision pin (--revision / --c trust_remote_code=False bypass. The issue is fixed in version 0.28.0.
CVE-2026-51772	A Server-Side Request Forgery (SSRF) vulnerability exists in the Image API (v2) of OpenStack Glance. When the show_multiple_locations configuration option is ena
CVE-2026-100651	vLLM before 0.29.0 fails to enforce decoder prompt-length validation on the disaggregated serving endpoint /inference/v1/generate. When the request contains a 't
CVE-2026-61811	Wazuh is an open-source security platform providing unified XDR and SIEM protection for endpoints and cloud workloads. From 3.8.0 until 4.14.7, the _getattribute:
CVE-2026-63432	Horilla is an HR and CRM software. From 1.0.0 until 1.6.0 and 2.0.0, the get_mail_preview handlers in recruitment/views/actions.py and employee/not_in_out_dashb
CVE-2026-63431	Horilla is an HR and CRM software. In 1.5.0-85 and earlier, payroll/views/component_views.py does not consistently authorize access in allowances_deductions_tab
CVE-2026-100501	Flame through 2.4.0 contains an improper restriction of excessive authentication attempts vulnerability in the POST /api/auth login endpoint that allows unauthenti
CVE-2026-91767	php_openssl_matches_wildcard_name() in ext/openssl/xp_ssl.c underflows the length argument passed to memchr() when a TLS server certificate presents a wildca
CVE-2026-54461	Habitica is a habit tracker application that treats goals like a role-playing game. From 4.172.1 until 5.48.2, a query parameter on Habitica's /api/v3/groups/:groupId
CVE-2026-100192	X-SpringBoot through 6.0 exposes appKey and appSecret credentials in the GET /application/manager/select endpoint without authentication or field filtering. Unau
CVE-2026-65827	Docmost is open-source collaborative wiki and documentation software. From 0.21.0 until 0.95.0, any authenticated workspace member with edit rights to a space
CVE-2026-100650	vLLM through 0.29.0 fetches and fully materializes remote or inline media before enforcing its documented media controls (the VLLM_MAX_AUDIO_CLIP_FILESIZE_M unauthenticated by design. There is no code execution or data disclosure impact.
CVE-2026-	Bludit CMS through 3.22.0 contains a missing authorization vulnerability that allows authenticated users holding the Author or Editor role to read the full content of

93365	
CVE-2026-85291	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. Prior to 1.7.2, InvoicePlane's Users::change_password() method
CVE-2026-85289	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. Prior to 1.7.2, InvoicePlane omits ensure_valid_post_request() f
CVE-2026-85274	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. Prior to 1.7.2, InvoicePlane exposes Recurring::stop() as a state
CVE-2026-93030	FTM 4.x ALL could allow a remote authenticated attacker to obtain sensitive information due to an XML external entity injection flaw.
CVE-2026-96746	An out-of-bounds write in the connection-monitoring logic of the MongoDB C Driver may allow an unauthenticated party who controls name resolution and the resp
CVE-2026-91768	The IPv6 branch of the FastCGI client access check compares only the first 12 bytes of a 16-byte IPv6 address, so listen.allowed_clients matches on a /96 prefix ins
CVE-2026-100531	The @openclaw/slack npm package before 2026.8.1 contains an authorization flaw in its Slack download-file handler: when a file lacks the share metadata used to
CVE-2026-100536	OpenClaw versions before 2026.8.1 fail to validate all source fields in structured message attachments, allowing attackers to hide unvalidated host paths behind al
CVE-2026-100538	OpenClaw (npm package 'openclaw') before 2026.8.1 does not apply the originating sender's global or per-agent toolsBySender policy when handling outbound att
CVE-2026-92573	Improper handling of compressed data in the shared GZIP decompressor used for AMQP 0-8/0-9/0-9-1 and AMQP 0-10 message delivery, message conversion and t
CVE-2026-100566	OpenClaw LINE versions before 2026.8.1 contain an access control vulnerability where group allowlist mode silently inherits DM allowFrom values when groupAllow
CVE-2026-100582	OpenClaw channel plugins (@openclaw/msteams, @openclaw/feishu, @openclaw/matrix, and @openclaw/googlechat) before 2026.8.1 do not enforce the configure
CVE-2026-96748	PyMongo's connection string parsing decodes percent-encoded characters in the host portion before the host list is separated on its delimiters. When an application
CVE-2026-100594	OpenClaw versions before 2026.7.1 contain an authorization bypass vulnerability in the /export-trajectory endpoint that allows non-owner senders to request and r
CVE-2026-100595	OpenClaw versions before 2026.7.1 contain an authorization bypass vulnerability in the diagnostics export command that allows non-owner channel senders to acc
CVE-2026-84097	The wp-review-slider-pro WordPress plugin before 12.7.12 does not sanitize a value stored through one of its AJAX handlers, which lacks a capability check, before
CVE-2026-100602	ClawHub (openclaw/clawhub application/backend) contains a missing authorization check in the changelog preview feature. A signed-in caller can invoke the public
CVE-2026-94281	An out-of-bounds read in libXi's XListInputDevices() class parsing in libXi before 1.8.4 could be used by malicious X servers to crash an attached X client.
CVE-2026-100611	Capgo (capgo.app backend, versions ≤ 12.261.0) improperly restricts which roles the apikey_manager organization role may bind to newly created API keys. When organization's apps. As of the advisory publication no patched version was available.
CVE-2026-82585	The Botslab G980H dash camera firmware transmits sensitive information over unencrypted HTTP and RTSP connections. An attacker capable of intercepting commn
CVE-2026-100632	Parse Server is an open-source backend server. In versions >= 9.0.0 and < 9.10.1-alpha.8, and in versions < 8.6.89, LiveQuery evaluates the protectedFields class or per-user protectedFields groups.
CVE-2026-	SiYuan is a self-hosted personal knowledge management system. In versions 3.8.0 through 3.8.3, the MCP file tool's sensitive-path guard (util.IsForbiddenAbsPath() version 3.8.4. Suggested title: SiYuan 3.8.0 through 3.8.3 Sensitive-Path Guard Bypass in Recursive MCP File Operations.

100633	
CVE-2025-14181	The SOAP HTTP client guards its response buffer growth with a check that relies on signed integer overflow, which is undefined behaviour and is not guaranteed to
CVE-2026-92928	OpenEye Apex Network Video Recorder (NVR) firmware 3.2.9.376 contains a hardcoded, undocumented recovery account with a shared credential that cannot be c
CVE-2026-95525	Subscriber Arbitrary File Deletion in WP User Frontend <= 4.3.11 versions.
CVE-2026-94118	Contributor Cross Site Scripting (XSS) in Premium Blocks - Gutenberg Blocks for WordPress <= 2.3.17 versions.
CVE-2026-84720	A flaw was found in the Ansible Automation Platform automation-controller. The WorkflowJobNode.ancestor_artifacts database column, which stores the raw merge
CVE-2026-94168	Contributor Cross Site Scripting (XSS) in Premium Addons for Elementor <= 4.11.105 versions.
CVE-2026-94391	Contributor Cross Site Scripting (XSS) in Ultimate FAQ <= 2.4.14 versions.
CVE-2026-88837	BusyBox httpd treats yescrypt (\$y\$) password hashes as plaintext during Basic Authentication, inverting the authentication check.
CVE-2026-94461	Contributor Cross Site Scripting (XSS) in Ditty <= 3.1.69 versions.
CVE-2026-96443	Insufficient validation of the JDBC driver URL in Apache Doris allows a privileged user to achieve remote code execution on the FE.
CVE-2026-84098	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.9.5 does not properly verify a listing's ownership before deletin
CVE-2026-86867	Cinnamon's Kotaemon (all versions up to and including v0.12.0) multi-user chat interface contains multiple vulnerabilities due to incorrect authorization and improv
CVE-2026-4806	The Custom Thank You Page for WooCommerce plugin for WordPress is vulnerable to unauthorized access and loss of data due to a missing capability check on the
CVE-2026-94498	Unauthenticated Broken Access Control in AppMySite <= 3.15.4 versions.
CVE-2026-94251	A vulnerability in Apache Sling Security Bundle: ContentDispositionFilter mediates only one address/API shape of a resource This issue affects Apache Sling Security
CVE-2026-94684	Contributor Cross Site Scripting (XSS) in Ocean Extra <= 2.6.1 versions.
CVE-2026-82195	The 10Web Booster WordPress plugin before 2.34.0 does not restrict access to the routine which issues the shared secret that authenticates its cloud connection, c
CVE-2026-97155	Fabasoft Folio Client before 2026, a locally installed component that communicates with the Fabasoft browser extension via web messaging, does not restrict which
CVE-2026-94682	Contributor Cross Site Scripting (XSS) in Podcast Importer SecondLine <= 1.5.6 versions.
CVE-2026-77798	Velociraptor contains a deadlock condition that may be triggered by authenticated users. The issue stems from a lock management bug in the user management n
CVE-2026-88359	libfyaml 0.9.6 contains a stack exhaustion vulnerability in fy_atom_iter_format(). When processing a specially crafted YAML document containing a very large litera
CVE-2026-	simdjson 4.6.1 contains a one-byte out-of-bounds read vulnerability in dom::parser::parse_unpadded(). A specially crafted truncated JSON document whose final st

88358	
CVE-2026-79304	CyberPanel 1.9.1 contains a path traversal vulnerability in the readFileContents method of the /filemanager/controller endpoint. An authenticated remote attacker can exploit this vulnerability to read arbitrary files on the system.
CVE-2026-76907	LaSuite Doc is a collaborative note taking, wiki and documentation platform. From 4.8.2 until 5.4.0, GET /api/v1.0/documents/search/ accepts sequential seven-digit IDs, allowing an attacker to bypass authentication and access sensitive data.
CVE-2026-94680	Contributor Cross Site Scripting (XSS) in The Post Grid <= 7.9.5 versions.
CVE-2026-79306	CyberPanel v1.9.1 contains a path traversal vulnerability in the compress method exposed through the /filemanager/controller endpoint. An authenticated remote attacker can exploit this vulnerability to read arbitrary files on the system.
CVE-2026-6831	The Advanced Contact form 7 DB plugin for WordPress is vulnerable to missing authorization in all versions up to, and including, 2.0.9. This is due to the plugin not properly checking the user's capabilities before allowing access to the database.
CVE-2026-96654	Plex Media Server before 1.43.3.10861 does not correctly neutralize URL values included in 'searchOne,' allowing an attacker to call other plugins' functions and potentially execute arbitrary code.
CVE-2026-96651	Plex Media Server before 1.43.3.10861 builds a file path from the url parameter without checking it for ../ sequences, allowing path traversal via '/system/agents/metadata/...' and potentially accessing sensitive files.
CVE-2026-94500	Contributor Cross Site Scripting (XSS) in ElementsKit Elementor addons Lite <= 4.0.5 versions.
CVE-2026-86601	The WP Recipe Maker WordPress plugin before 10.8.2 does not remove shortcodes from comment content before expanding it while building a page's structured metadata, allowing an attacker to inject malicious code.
CVE-2026-84713	A flaw was found in the automation-controller notification subsystem. Although NotificationTemplate.notification_ configuration is protected from API filtering, its read operation is not, allowing an attacker to access sensitive information.
CVE-2026-95602	Authorization Bypass Through User-Controlled Key vulnerability in YITH YITH WooCommerce Request A Quote allows Exploiting Incorrectly Configured Access Control to access restricted features.
CVE-2026-92164	Streamlink is a CLI utility which pipes video streams from various services into a video player. Prior to 8.6.0, HTTPSession mounts a FileAdapter for the file scheme, allowing an attacker to access local files.
CVE-2026-95527	Unauthenticated Broken Access Control in Conekta Payment Gateway <= 6.2.4 versions.
CVE-2026-18179	IBM Financial Transaction Manager (FTM) for RedHat OpenShift could allow a remote attacker to clear active chat sessions due to improper authorization.
CVE-2026-93541	An out-of-bounds read in libXi's XQueryDeviceState() in libXi before 1.8.4 could be used by a malicious user to read arbitrary memory.
CVE-2026-95530	Subscriber Cross Site Scripting (XSS) in PixelYourSite - Your smart PIXEL (TAG) Manager <= 11.4.1 versions.
CVE-2026-95586	Contributor Cross Site Scripting (XSS) in Ultimate Addons for Contact Form 7 <= 3.5.50 versions.
CVE-2026-78313	Improper Access Control in DIAEnergie. This issue affects DIAEnergie: before 1.11.00.022.
CVE-2026-77112	Server-Side request forgery (SSRF) vulnerability in Global IT Informatics Technology Services Inc. Weoll allows Server Side Request Forgery. This issue affects Weoll: before 1.0.0.
CVE-2026-96276	If a malicious SDK container declares an extension point with a crafted `directory` path, and a developer runs `flatpak build-init --writable-sdk --sdk-extension` with the malicious SDK, an attacker can potentially execute arbitrary code.
CVE-2026-93772	Subscriber Cross Site Scripting (XSS) in wpForo Forum <= 3.1.5 versions.
CVE-2026-96653	Contributor Broken Access Control in WSP MCP – AI Agents Connector <= 2.7.0 versions.

93529	
CVE-2026-77421	JLine is a Java library for handling console input. From 3.0.0 until 3.30.15 and 4.3.1, the JLine built-in nano editor's regex search mode passes a user-controlled search
CVE-2026-95523	Subscriber Bypass Vulnerability in WP User Frontend <= 4.3.11 versions.
CVE-2026-93620	Unauthenticated Broken Access Control in PayPlus Payment Gateway <= 8.2.5 versions.
CVE-2026-65422	A flaw in the authorization mechanism for Media Gateway API in Genetec Security Center may allow a user with no playback privileges to generate video thumbnails
CVE-2026-80342	The Payment Plugins for PayPal WooCommerce WordPress plugin before 2.0.27 does not verify that a PayPal order supplied in a payment request belongs to the WordPress
CVE-2026-73581	Improper Check for Certificate Revocation vulnerability in Apache Tomcat. Both the OpenSSL and OpenSSL-FFM TLS implementations ignore CRLs when certificate
CVE-2026-94671	Contributor Cross Site Scripting (XSS) in The Post Grid <= 7.9.5 versions.
CVE-2026-16264	The Newsletters WordPress plugin before 4.18.1 does not perform an ownership check on some of its subscriber management actions, and issues a management success
CVE-2026-93618	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock. Jetimpex Inc. JetTricks allows Stored XSS. This issue
CVE-2026-18180	IBM Financial Transaction Manager (FTM) for RedHat OpenShift could allow a remote authenticated attacker to obtain sensitive information due to SQL injection.
CVE-2026-79760	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. From 2.5.0 until 2.5.1, Termix allows authenticated users to
CVE-2026-91119	Discourse is an open-source discussion platform. Prior to 2026.1.8, 2026.6.3, 2026.7.2, and 2026.8.0, the topic small-action and nested-activity-log components introduced
CVE-2026-63000	REDAXO is a PHP-based content management system. Prior to 5.21.2, rex_api_install_package_update in redaxo/src/addons/install/lib/api/api_package_update.php
CVE-2026-84721	A server-side request forgery flaw was found in the Ansible Automation Platform automation-controller email notification backend. The email backend passes the user
CVE-2026-15273	The Automatic.css plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REQUEST_URI in all version 4.0.0 due to insufficient input sanitization and on
CVE-2026-96672	Frappe ERPNext versions before 16.34.1 fail to validate that Financial Report Template calculation_formula values reference whitelisted methods before passing the
CVE-2026-73586	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Insufficient Session Expiration vulnerability. A low privileged attacker
CVE-2026-57175	Python Social Auth is a social authentication/registration mechanism. Prior to version 5.0.0, the SAML backend accepted SAML responses on the Assertion Consumer
CVE-2025-14814	The CSS & JavaScript Toolbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's cjtoolbox shortcode in all versions up to, and including
CVE-2026-93897	The GeoDirectory - WP Business Directory Plugin and Classified Listings Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Text-type Custom
CVE-2026-93747	The wpForo Forum plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'telegram' profile field in versions up to, and including, 3.1.6. This is due
CVE-2026-94376	The Better Messages - Chat Rooms, Group Chat, Private Messages & AI Chat Bots plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the

CVE-2026-96766	The GeoDirectory – WP Business Directory Plugin and Classified Listings Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'business
CVE-2026-100529	OpenClaw versions before 2026.8.1 contain an authorization scope widening vulnerability in file-transfer allow-always approvals that allows attackers to reuse stan
CVE-2026-91161	OpenWA is a free, open source, self-hosted WhatsApp API gateway. Prior to 0.23.5, the GET /api/sessions/{sessionId}/groups/{groupId}/invite-code endpoint and tl
CVE-2026-13179	The WP Maps – Google Maps,OpenStreetMap,Mapbox,Store Locator,Listing,Directory & Filters plugin for WordPress is vulnerable to Stored Cross-Site Scripting via s
CVE-2026-93656	The User Profile Builder – Beautiful User Registration Forms, User Profiles & User Role Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Av
CVE-2026-100546	OpenClaw (npm package `openclaw`) versions >= 2026.7.2 and < 2026.9.2 contain a race condition in the Discord realtime voice transcript path. Concurrent cont
CVE-2026-92746	The Gutenverse – WordPress Blocks, Page Builder & Site Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Post Comment Block 'suffixMair
CVE-2026-15731	The WP Multilang – Translation and Multilingual Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the post content in all versions up to, an
CVE-2026-5924	The Getwid – Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Google Maps block's 'customStyle' attribute in all versions i
CVE-2026-97225	A flaw has been found in DbGate up to 7.2.5-beta.5. This affects an unknown function of the file packages/api/src/controllers/runners.js of the component JSON Run
CVE-2026-97884	A vulnerability was detected in mathurvishal CloudClassroom-PHP-Project up to 5dadec098bfbbf3300d60c3494db3fb95b66e7be. This impacts an unknown funcionr
CVE-2026-97886	A vulnerability has been found in mathurvishal CloudClassroom-PHP-Project up to 5dadec098bfbbf3300d60c3494db3fb95b66e7be. Affected by this vulnerability is
CVE-2026-95868	A weakness has been identified in AdithyaYelloju Restaurant-Management-System up to 7f0e7e84255e8fcfd488e83f8f91451bbbff6b9c. Affected by this issue is the
CVE-2026-73589	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, Versions prior to 5.36, contains a Weak Encoding for Password vulnerability. A lov
CVE-2026-95833	A weakness has been identified in itsourcecode Leave Management System 1.0. Impacted is an unknown function of the file /module/leavetype/index.php. This ma
CVE-2026-95829	A vulnerability was identified in TDuckCloud tduck-platform up to 5.3. This vulnerability affects the function PaginationInnerInterceptor.concatOrderBy of the file td
CVE-2026-100312	A security flaw has been discovered in mathurvishal CloudClassroom-PHP-Project up to 5dadec098bfbbf3300d60c3494db3fb95b66e7be. The impacted element is a
CVE-2026-95830	A security flaw has been discovered in theRealSain Pixtream up to 866afd4f0cea812b918780fb74b67dccf8c4d6a0. This issue affects some unknown processing of
CVE-2026-97226	A vulnerability has been found in DbGate up to 7.2.5/7.3.1-premium-beta.1. This impacts the function fs.readFile of the file packages/api/src/controllers/files.js of th
CVE-2026-97895	A vulnerability was determined in krayin laravel-crm up to 2.2.5. This affects an unknown part of the file packages/Webkul/Admin/src/Http/Controllers/Settings/User
CVE-2026-97232	A vulnerability was determined in volotat Anagnorisis up to 0.4.2. Affected by this vulnerability is the function get_file_content/save_file_content/move_files/start_st
CVE-2026-100592	OpenClaw is an agent gateway distributed via npm. In versions >= 2026.4.10 and < 2026.7.1, persistent memory dreaming mutations omit owner permission chec

CVE-2026-100591	OpenClaw is an npm-distributed agent gateway. In versions before 2026.7.1, the global Active Memory toggle mutations could omit owner checks. An authorized n
CVE-2026-85738	TREK is a collaborative travel planner. Prior to 3.4.0, the checkSsrf logic in server/src/utls/ssrfGuard.ts does not recognize NAT64, 6to4, or Teredo IPv6 transition ac
CVE-2026-95929	A weakness has been identified in iFlytek astron-agent up to 1.0.7. Affected is an unknown function of the file console/backend/commons/src/main/resources/mapp
CVE-2026-97365	A vulnerability was determined in chonkie-inc littrs 0.6.1/0.6.2. Impacted is the function Sandbox::mount of the file crates/littrs/src/lib.rs. Executing a manipulation
CVE-2026-96676	A vulnerability was identified in Fast FAC1900R 20190827_2.0.2. The impacted element is the function get_alias_name of the component uhttpd. Such manipulation
CVE-2026-100556	OpenClaw (npm package openclaw) versions >= 2026.5.2 and < 2026.8.1 contain an incorrect authorization vulnerability in WhatsApp group handling. A group ser
CVE-2026-96777	A vulnerability was determined in Forma LMS up to 4.1.43. This impacts the function UserselectorAdmController::getDataTask of the file /appCore/ajax.adm_server
CVE-2026-97321	A vulnerability has been found in YunaiV/zhijiantianya ruoyi-vue-pro up to 2026.08. The impacted element is the function GoViewDataServiceImpl.getDataBySQL of
CVE-2026-97323	A vulnerability was determined in YunaiV/zhijiantianya ruoyi-vue-pro up to 2026.08. This impacts the function getOriginalFilename of the file yudao-module-mp/src,
CVE-2026-96884	A security flaw has been discovered in MantisZip up to 0.4.5. Affected by this issue is the function Path.Combine of the file MainWindow.UI.cs of the component Pre
CVE-2026-100577	OpenClaw versions before 2026.8.1 fail to validate video asset URLs returned by providers, allowing server-side requests to private destinations. A malicious or cor
CVE-2026-72662	Authorization Bypass Through User-Controlled Key (CWE-639) in Kibana can lead to unauthorized disclosure, modification, and deletion of data via Accessing Funct
CVE-2026-97366	A security flaw has been discovered in jhen0409 react-native-debugger up to 0.14.0. The impacted element is the function openDevTools of the file electron/windo
CVE-2026-97368	A weakness has been identified in chillzhuang SpringBlade up to 5.0.2. This affects the function UserServiceImpl.userInfo of the file blade-service/blade-system/src,
CVE-2026-96678	A security vulnerability has been detected in weiqingwen spring-boot-forum up to 538eecc3c6b85fdf0768ab4e8354b48c0c17d94f. Affected is the function validate
CVE-2026-95930	A security vulnerability has been detected in iFlytek astron-agent up to 1.0.6. Affected by this vulnerability is the function UrlCheckTool.checkUrl of the component
CVE-2026-96456	The Reachy Mini Bluetooth service asks a connecting device for a PIN before it will accept commands. The check protects the session but not the caller, so an attac media sounds API, tracked as CVE-2026-55419, which places an attacker-controlled script on the filesystem. This issue then provides command access over Blueto
CVE-2026-97320	A flaw has been found in YunaiV/zhijiantianya ruoyi-vue-pro up to 2026.08. The affected element is the function AiKnowledgeDocumentServiceImpl.readUrl of the fi
CVE-2026-19267	IBM Financial Transaction Manager (FTM) for RedHat OpenShift is vulnerable to missing authentication on the Business Rules Manager commands REST endpoint (`
CVE-2026-6544	IBM Concert 1.0.0 through 3.0.0 allows recursive copying of directories without proper controls which can lead to unintentional inclusion of sensitive or unnecessar
CVE-2026-88389	Espruino 2v29 (commit bffc6d0) contains a NULL pointer dereference vulnerability in jslGetRawString() in src/jslex.c. Crafted raw/binary string input can cause the
CVE-2026-6718	IBM Concert 1.0.0 through 3.0.0 is vulnerable to improper access control which allows unauthorized modification of application files.

CVE-2026-84403	The Botslab G980H dash camera firmware does not require authenticated pairing or client binding before permitting access to Bluetooth Low Energy communicati
CVE-2026-88377	Bento4 1.6.0.0 contains an integer underflow vulnerability in the avcC and hvcC configuration atom parsers. A specially crafted MP4 file containing an atom with a
CVE-2026-92930	OpenEye Apex Network Video Recorder (NVR) firmware 3.2.9.376 uses an administrator password-reset unlock-code design that lacks a per-device secret or other
CVE-2026-93405	Mailspring is a fast, cross-platform, open-source email client. Prior to 1.17.0, attachment quick preview converts Markdown, DOCX, and XLSX attachments with Sna
CVE-2026-78393	The Link Library WordPress plugin before 7.9.6 does not properly escape some parameters before outputting them in the addresses of links it generates on its fron
CVE-2026-88835	BusyBox dpkg read_package_field() steps past a NUL terminator on malformed .deb packages, causing an out-of-bounds heap read.
CVE-2026-100694	Hugo is a static site generator. In versions from v0.56.0 through v0.165.x, content files mapped to the text/org media type are rendered without escaping raw HTM
CVE-2026-17577	The SSL Zen plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'uri' (and 'host') parameters in versions up to, and including, 4.7.42. The ss
CVE-2026-18320	Readwise Reader for Android uses a sanitize-html configuration that permits all attributes on SVG and PATH elements due to a wildcard attribute rule. This configur
CVE-2026-18312	Readwise Reader for Android constructs URLs in its WebView using attacker-controlled metadata without proper encoding or escaping. The application interpolates
CVE-2026-18311	Readwise Reader for Android contains a cross-site scripting vulnerability due to missing HTML sanitization in its processing of imported document metadata. Attack
CVE-2026-100237	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in The Wikimedia Foundation Mediawiki - Thanks Extension allows !
CVE-2026-88996	The WPForms – AI Form Builder for WordPress – Contact Forms, Payment Forms, Survey Form, Quiz & More plugin for WordPress is vulnerable to Reflected Cross-Si
CVE-2026-61784	xhtml-purifier is a Node.js library to take in raw/unknown/untrusted HTML and output cleaned, purified, trusted HTML. Versions prior to 0.4.3 do not HTML-entity-en
CVE-2026-91796	The interface of Foxit PDF Editor/Reader lacks the permission verification for secure reading mode, which allows specially crafted PDFs to trigger external SMB auth
CVE-2026-91807	A heap-based out-of-bounds read vulnerability exists in Foxit PDF Editor/Reader’s handling of malformed image soft-mask data. Insufficient validation of the soft-m
CVE-2026-91808	A heap-based out-of-bounds read vulnerability exists in Foxit PDF Editor Reader’s handling of PDF image objects with inconsistent compression metadata. Insufficie
CVE-2026-91810	A heap-based out-of-bounds read vulnerability exists in Foxit PDF Editor/Reader’s handling of malformed PDF image masks. Inconsistent image metadata may caus
CVE-2026-100695	Adminer before 6.0.2 contains a cross-site scripting vulnerability where the CONNECTION_ID() database result is interpolated into JavaScript without proper escapir
CVE-2026-91817	A heap-based out-of-bounds read vulnerability exists in Foxit PDF Editor/Reader's handling of wide strings in embedded PDF JavaScript. Insufficient validation of str
CVE-2026-100522	Cotonti through 1.0.0 contains a reflected cross-site scripting vulnerability in message.php where the lng parameter is not properly escaped before output in the cc
CVE-2026-92212	The JetFormBuilder — Dynamic Blocks Form Builder plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via 'jfb_xss' (URL Query Variable) Paramete

CVE-2026-100521	Cotonti through 1.0.0 contains a reflected cross-site scripting vulnerability in the search plugin highlight parameter that performs no HTML or JavaScript escaping. CVE-2026-100521
CVE-2026-78902	Cross Site Scripting vulnerability in Netgate pfSense 26.03.1-RELEASE allows an attacker to execute arbitrary code via the pfBlockerNG package CVE-2026-78902
CVE-2026-92001	Improper restriction of recursive entity references in DTDs ('XML entity expansion') vulnerability in Apache Sling XSS. This issue affects Apache Sling XSS: before 2.12.0 CVE-2026-92001
CVE-2026-91999	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Apache Sling XSS. This issue affects Apache Sling XSS: before 2.12.0 CVE-2026-91999
CVE-2026-100523	Cotonti through 1.0.0 contains an open redirect vulnerability in message.php that base64-decodes the redirect parameter without domain validation. Unauthenticated users can redirect other users to arbitrary domains. CVE-2026-100523
CVE-2026-91928	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Apache Sling XSS. This issue affects Apache Sling XSS: before 2.12.0 CVE-2026-91928
CVE-2026-91852	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Apache Sling XSS. This issue affects Apache Sling XSS: before 2.12.0 CVE-2026-91852
CVE-2026-73192	An improper neutralization of input during web page generation ('Cross-site Scripting') [CWE-79] vulnerability when using the XSSAPI.getValidHref() in Apache Sling CVE-2026-73192
CVE-2026-54790	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. Prior to 1.7.2, InvoicePlane stores an administrator-controlled cookie in the browser. CVE-2026-54790
CVE-2026-91766	When the http:// stream wrapper follows a redirect it forwards the user-supplied Authorization, Cookie and Proxy-Authorization headers unchanged, even when the user-agent is not configured to follow redirects. CVE-2026-91766
CVE-2026-100701	Nodemailer versions 5.0.0 through 10.0.1 use a process-global DNS cache that is keyed only by the DNS host, while each cache entry also stores the caller-specific IP address. CVE-2026-100701
CVE-2026-100702	Nodemailer before 10.0.2 fails to properly flatten deeply nested arrays in recipient fields such as to, cc, and bcc, allowing attackers to cause stack exhaustion. CVE-2026-100702
CVE-2026-81645	Out-of-bounds read vulnerability in the graphics module. Successful exploitation of this vulnerability may affect availability. CVE-2026-81645
CVE-2026-92842	The convert.base64-encode, convert.quoted-printable-encode and convert.quoted-printable-decode stream filters accept a line-break-chars option whose length is not validated. CVE-2026-92842
CVE-2026-100652	vLLM versions 0.22.0 through 0.23.0 fail to validate stop_token_ids against vocabulary bounds in Rust HTTP and gRPC frontends, allowing out-of-vocabulary token IDs to be used. CVE-2026-100652
CVE-2026-100689	GitPython before 3.1.62 does not validate the `path` field read from an untrusted .gitmodules file when updating submodules. While a prior fix (GHSA-hmq2-w58f-7242) addressed the issue for the case where the path is a relative path, it did not address the case where the path is an absolute path. CVE-2026-100689
CVE-2026-6669	Missing upper bound on the key derivation iteration count accepted during SCRAM authentication to a backend server in PgBouncer through 1.25.2 allows a malicious user to perform a denial of service attack. CVE-2026-6669
CVE-2026-95625	The Tauri updater plugin verifies update binaries using minisign signatures, but the signature covers only the raw binary bytes. The update manifest -- which contains the signature -- is not verified. CVE-2026-95625
CVE-2026-100635	SiYuan before v3.8.4 contains an authentication bypass vulnerability in the publish service where session cookies are issued without Secure or SameSite attributes. CVE-2026-100635
CVE-2026-100574	OpenClaw (npm package 'openclaw') before 2026.8.1 contains a server-side request forgery vulnerability in its trusted-host DNS checks. For fetches that use the trusted-host header, the host is not validated. CVE-2026-100574
CVE-2026-77703	Key exchange without entity authentication vulnerability in HAVELSAN Inc. Liman Render Engine allows Adversary in the Middle (AiTM). This issue affects Liman Render Engine: before 2026.8.1 CVE-2026-77703
CVE-2026-77707	Improper certificate validation vulnerability in HAVELSAN Inc. Liman Render Engine allows Adversary in the Middle (AiTM). This issue affects Liman Render Engine: before 2026.8.1 CVE-2026-77707
CVE-	

CVE-2026-96599	Isotope eCommerce through 2.9.10 derives order identifiers from uniqid() instead of a cryptographically secure source, allowing unauthenticated attackers to guess order identifiers.
CVE-2026-19708	The File Manager WordPress plugin before 8.0.5 does not prevent unauthenticated users from downloading its database backup archives, and in some cases writes backup archives to the local file system.
CVE-2026-100698	Adminer 5.5.1 through 6.0.1 improperly parses the login 'server' string in the host_port() function in adminer/include/functions.inc.php. The port capture group requires a non-empty string.
CVE-2026-100696	Adminer 4.16.0 through 6.0.1 contain a pre-authentication Server-Side Request Forgery (SSRF) vulnerability in the optional Elasticsearch driver (plugins/drivers/elasticsearch.php or an adminer_object() configuration; it is not loaded in a default build) and that PHP allow_url_fopen be enabled.
CVE-2026-96533	The Testimonials Widget WordPress plugin through 4.0.4 does not validate a user-supplied URL before fetching it server-side and storing the response as a public file in the uploads directory.
CVE-2026-93682	When the HTTP stream wrapper follows a redirect and the response carries a Location header with an empty value, the redirect code reads one byte past the end of the response body.
CVE-2026-87118	The Botslab G980H dash camera firmware contains an out of bounds write vulnerability in its command processing functionality. An authenticated attacker with administrative access can exploit this to write arbitrary data to memory.
CVE-2026-96548	A flaw has been found in sfturing hosp_order up to 627f426331da8086ce8fff2017d65b1ddef384f8. This affects an unknown part of the file ssm_pro/src/main/resources/properties/properties.properties.
CVE-2026-97866	A weakness has been identified in Zhonglun CloudPOS 3.0. Affected by this vulnerability is an unknown functionality of the file Program.cs of the component AutoNPOS.
CVE-2026-96745	Deserialization of untrusted data in the command monitoring support of the MongoDB PHP Driver can cause class names embedded in document content to be horizontally concatenated.
CVE-2026-86612	The Ninja Tables WordPress plugin before 5.2.17 does not restrict shortcode expansion to administrator-authored table rows which, in a non-default configuration, allows an attacker to execute arbitrary PHP code.
CVE-2026-88386	libsndfile 1.2.2 contains a misaligned memory access issue in psf_binheader_readf() while parsing WAV fmt chunks. A specially crafted WAV file can cause the function to read past the end of the file.
CVE-2026-12037	The Asset CleanUp: Page Speed Booster plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.4.0.5 via the 'page_cleaner' endpoint.
CVE-2026-77420	JLine is a Java library for handling console input. From 3.0.0 until 3.30.15 and 4.3.1, DefaultHistory.matchPatterns(String patterns, String line) in reader/src/main/java/org/jline/reader/DefaultHistory.java has a buffer overflow.
CVE-2026-100547	OpenClaw is a coding agent distributed as the npm package `openclaw`. In affected versions (2026.7.1 through 2026.7.2), alternate but valid `file:` URL spellings could be used to bypass security checks.
CVE-2026-100569	OpenClaw is an npm-distributed application. In versions >= 2026.4.25 and < 2026.8.1, the workspace environment-variable filter did not block variables ending in a space character.
CVE-2026-100616	capgo.app is an over-the-air update platform for Capacitor apps. In all versions prior to a fix, the row-level security UPDATE policy on the public.orgs table permits updates to the orgs table.
CVE-2026-93290	Omni C20 uses hard-coded credentials that could allow an attacker to monitor log files to obtain credentials to access information like mapping data.
CVE-2026-100687	Budibase Server before 3.45.0 fails to redact plaintext datasource credentials before broadcasting external table updates to the Builder collaboration websocket room.
CVE-2026-100581	OpenClaw for iOS before 2026.8.11 stores Gateway credentials as cleartext JSON in App Group UserDefaults instead of the device Keychain. Attackers with access to the app group can retrieve the credentials.
CVE-2026-88387	LibRaw 0.22.0 contains an incorrect numeric conversion vulnerability in LibRaw::parse_tiff_ifd() when processing TIFF tag 0x00fe (NewSubfileType). A specially crafted file can cause a buffer overflow.
CVE-2026-100629	Capgo (capgo.app backend) before 12.127.5 contains an authorization flaw in the PATCH /private/role_bindings/:binding_id endpoint. The handler verifies that the role exists but does not verify that the user has permission to update it.
CVE-	

CVE-2026-92680	Araxis Merge for Windows version 2011.4074 through 2026.0 stores user-configured credentials for remote servers in the Windows registry and does not apply suf
CVE-2026-88384	OpenEXR 3.4.14 contains a NULL Pointer Dereference in the C++ attribute parsing path. A specially crafted EXR file containing an unknown-type attribute with dat
CVE-2026-95928	A security flaw has been discovered in recommenders-team recommenders up to 1.2.1. This impacts the function pickle.load of the file recommenders/models/new
CVE-2026-96273	Ghidra before 12.1.4 fails to validate the TYPE_COL byte in OptionsDB.createUnregisteredOption(), causing an ArrayIndexOutOfBoundsException that leaves domai
CVE-2026-95897	A security vulnerability has been detected in Dask up to 2026.8.0. This affects the function from_npy_stack of the file dask/array/core.py of the component Loader.
CVE-2026-79762	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. From 1.7.0 until 2.5.1, Termix derives the keys that
CVE-2026-97222	A heap use-after-free flaw was found in Gnumeric. When a user opens a crafted Gnumeric workbook containing a malformed SheetObjectComponent element, the
CVE-2026-96600	Isotope eCommerce through 2.9.10 contains a blind SQL injection vulnerability in backend callbacks that interpolate request-controlled identifiers and administrato
CVE-2026-100630	AVideo contains a stored cross-site scripting vulnerability in the video trailer1 field rendered unsanitized within an inline onclick JavaScript string. Attackers with vic
CVE-2026-100603	ClawHub (openclaw/clawhub) application/backend contains a flaw in the skill report moderation flow: four distinct ordinary authenticated accounts can report a visi
CVE-2026-100604	ClawHub (openclaw/clawhub) contains an incorrect authorization vulnerability in the ClawHub application/backend: an organization-owned skill retains the ownerUs
CVE-2026-80444	URL redirection to untrusted site ('open redirect') vulnerability in Abis Technology Ltd. Co. AVESİS allows Input Data Manipulation. This issue affects AVESİS: from 2
CVE-2026-88420	A reflected cross-site scripting (XSS) vulnerability in the EntryAbstract.save() component of APSL puput v1.2.1 through v2.2.0 allows authenticated attackers with v
CVE-2026-91120	Discourse is an open-source discussion platform. Prior to 2026.1.8, 2026.6.3, 2026.7.2, and 2026.8.0, provider-controlled video titles in lazy video embeds could be
CVE-2026-71177	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Improper Restriction of Rendered UI Layers or Frames vulnerability. A
CVE-2026-100388	RustDesk versions before 1.5.0 fail to properly validate file transfer permissions on incoming file clipboard messages in the Clipdr message handler on Linux and r
CVE-2026-48542	Krayin CRM through 2.2.6 contains a stored client-side template injection vulnerability that allows authenticated attackers to execute arbitrary JavaScript in other u
CVE-2026-97062	Aureus ERP through 1.6.0 stores uploaded SVG files on its public disk and serves them from the application origin, allowing authenticated users to upload malicious
CVE-2026-92874	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.3 before 19.2.7, 19.3 before 19.3.3, and 19.4 before 19.4.1 that under certain condi
CVE-2026-96763	A security flaw has been discovered in kvcache-ai mooncake up to 0.3.12/0.3.13.post1/0.3.14-rc1. This issue affects the function ScopedSegmentAccess::MountSeg
CVE-2026-48540	Krayin CRM through 2.2.6 contains a stored client-side template injection vulnerability that allows authenticated attackers to execute arbitrary JavaScript in other u
CVE-2026-48541	Krayin CRM through 2.2.6 contains a stored client-side template injection vulnerability that allows authenticated attackers to execute arbitrary JavaScript in other u
CVE-	

CVE-2026-100593	OpenClaw (npm package `openclaw`) before 2026.7.1 does not enforce the documented owner-only requirement for persistent `/activation` policy changes in gro
CVE-2026-48543	Krayin CRM through 2.2.6 contains a stored client-side template injection vulnerability that allows authenticated attackers to execute arbitrary JavaScript in other u
CVE-2026-100681	Budibase before 3.45.0 contains an unauthenticated server-side request forgery and credential exfiltration vulnerability in the Microsoft Teams webhook endpoint f
CVE-2026-84150	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.9.5 does not verify that the target user of a REST route matches
CVE-2026-100691	Hugo versions 0.75.0 through 0.165.x contain a stored cross-site scripting vulnerability: the syntax highlighter does not escape the `lineAnchors` option before pas
CVE-2026-91134	Discourse is an open-source discussion platform. Prior to 2026.1.8, 2026.6.3, 2026.7.2, and 2026.8.0, the Discourse post sanitizer allowed a stored cross-origin ifra
CVE-2026-47132	phpMyFAQ is an open source FAQ web application. Prior to version 4.2.0-alpha, an authenticated SQL LIKE wildcard injection vulnerability in phpMyFAQ's chat user
CVE-2026-97736	tinyauth before 5.1.3 allows rule bypass by appending an allowed route string. This is caused by an unanchored regular expression.
CVE-2026-18335	The Kirki - Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to Blind Server-Side Request Forgery in all versions up to, and i
CVE-2026-97723	madpsy ka9q_ubersdr before 0.1.58 has a stored cross-site scripting (XSS) vulnerability in the chat message rendering functionality. User-controlled URLs in chat n
CVE-2026-88974	WPGraphQL provides a GraphQL API for WordPress sites. Prior to 2.22.2, the updatePost mutation in src/Mutation/PostObjectUpdate.php checks only the collection-
CVE-2026-100624	Capgo.app before 12.264.5 does not enforce upload expiry or build lifecycle state in the /build/upload/:jobId TUS proxy endpoint. When a native build request is cre
CVE-2026-79758	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. From 1.8.0 until 2.5.1, authenticated Termix users c
CVE-2026-93366	Bludit CMS through 3.22.0 contains an authorization bypass vulnerability that allows authenticated users with the Author role to enumerate and delete media files
CVE-2026-94679	Subscriber Broken Access Control in Fluent Support <= 2.3.2 versions.
CVE-2026-100562	OpenClaw versions before 2026.8.1 contain an authorization bypass vulnerability in the sessions.create endpoint that allows operator.write callers to modify sessio
CVE-2026-100528	OpenClaw (npm package 'openclaw') before 2026.8.1 could send third-party provider credentials to the wrong endpoint. In affected versions, when a third-party pr
CVE-2026-100550	OpenClaw (npm package 'openclaw') before 2026.8.1 contains an access-control bypass in the Microsoft Teams integration. When groupPolicy is set to allowlist, a i
CVE-2026-100549	OpenClaw versions before 2026.8.1 contain a path traversal vulnerability in QQBot voice attachment handling where filenames are decoded twice, allowing encode
CVE-2026-100576	OpenClaw versions before 2026.8.1 contain a server-side request forgery vulnerability in browser wait predicates that allows attackers to bypass SSRF protections
CVE-2026-100564	OpenClaw versions before 2026.8.1 fail to neutralize spreadsheet formula characters in participant display names within attendance CSV exports. Attackers can inj
CVE-2026-100524	Cotonti through 1.0.0 contains a cross-site request forgery vulnerability in the extensions manager that allows attackers to perform state-changing actions without
CVE-2026-	OpenClaw (npm package `openclaw`) before 2026.8.1 does not neutralize leading characters that spreadsheet applications interpret as formulas when the Control

100563	
CVE-2026-18505	IBM Financial Transaction Manager (FTM) for RedHat OpenShift is vulnerable to open redirect in the PMP `HostHeaderFilter` (`HostHeaderFilter.java:151`). An unau
CVE-2026-100303	TDuck survey form through 6.0 lacks authorization checks on FormThemeController write endpoints for global form themes and categories. Authenticated non-adm
CVE-2026-80514	The wpForo Forum WordPress plugin from 3.0.0 before 3.1.6 does not verify the source of client-supplied IP address headers before using them to key its per-visito
CVE-2026-100533	OpenClaw versions before 2026.8.1 contain a path traversal vulnerability in the tools.fs.workspaceOnly feature where Unicode filename fallback can normalize vali
CVE-2026-88929	The Product Badge, Label, Countdown Timer for WooCommerce WordPress plugin before 7.5.2 does not check whether a product is published before returning its c
CVE-2026-75558	The Botslab G980H dash camera firmware uses a hard-coded cryptographic key and initialization vector to protect WiFi credentials communicated by the device. A
CVE-2026-87979	The Paymob for WooCommerce WordPress plugin before 4.1.14 does not verify the request signature on the card-token branch of its payment webhook, allowing u
CVE-2026-88846	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.50 does not check whether user registration is enabled on the site before creating an account
CVE-2026-96881	A vulnerability was determined in TaleLin lin-cms-spring-boot up to 0.2.1. Affected is the function getBooks of the file src/main/java/io/github/talelin/latticey/controlle
CVE-2026-84741	The Events Calendar WordPress plugin before 6.17.5 does not check the post status of linked records before embedding their stored details into a public REST API r
CVE-2026-92929	OpenEye Apex Network Video Recorder (NVR) firmware 3.2.9.376 trusts an X-Forwarded-For header supplied by an arbitrary client when determining the request s
CVE-2026-88761	The Botslab G980H dash camera firmware generates the default WiFi password using predictable device information, portions of which are advertised by the produ
CVE-2026-86783	The Post Grid Gutenberg Blocks WordPress plugin before 5.0.41 does not perform an authorization or post-visibility check on a REST API route that returns the cust
CVE-2026-96882	A vulnerability was identified in TaleLin lin-cms-spring-boot up to 0.2.1. Affected by this vulnerability is the function searchBook of the file src/main/java/io/github/t
CVE-2026-100677	stoatchat before 0.15.5 contains an account enumeration vulnerability in the login endpoint that exposes source file locations in error responses. Unauthenticated
CVE-2026-86785	The Social Commerce for WooCommerce WordPress plugin through 2.5.4 does not have authorisation checks on some of its REST API endpoints, allowing unauther
CVE-2026-86837	The Bookly WordPress plugin before 28.3 does not properly verify a customer's identity before updating their stored details, allowing unauthenticated attackers wh
CVE-2026-88840	BusyBox TLS get_client_hello() reads past the end of the input buffer when parsing a truncated ClientHello message.
CVE-2026-94080	Unauthenticated Broken Access Control in MarketKing <= 2.1.70 versions.
CVE-2026-84168	The Easy Hide Login WordPress plugin before 1.7 does not fully enforce its hidden-login protection, allowing an unauthenticated attacker to reach the standard logi
CVE-2026-95524	Unauthenticated Bypass Vulnerability in WP User Frontend <= 4.3.11 versions.
CVE-2026-	Flame through 2.4.0 contains an information exposure vulnerability in the unauthenticated GET /api/config endpoint that returns the entire configuration object wit

100418	
CVE-2026-100306	TDuck survey form through 6.0 fails to validate write passwords on submission endpoints, enforcing the check only on the front end. Remote unauthenticated attac
CVE-2026-100304	TDuck survey form 6.0 contains an information disclosure vulnerability in FormAuthUtils.hasPermission that fails open when a form does not exist, allowing authen
CVE-2026-97647	A security vulnerability has been detected in ningzichun student-management-system up to 98760f5711cf6dc8b4adca53a9e207ca49b02ebf. This impacts an unkn
CVE-2026-79763	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. From 2.4.0 until 2.5.1, the POST /users/totp/disable i
CVE-2026-97181	GPM LIGHT developed by ezGlobal has a Sensitive Data Exposure vulnerability. Unauthenticated remote attackers can directly access system logs.
CVE-2026-92905	ZohoCorp ManageEngine EventLog Analyzer and Log360 before build 13071 were vulnerable to a DoS vulnerability that allowed attackers to crash the log collector
CVE-2026-92799	The Online Scheduling and Appointment Booking System – Bookly plugin for WordPress is vulnerable to Authorization Bypass via PHP Type Juggling in all versions u non-string values such as the JSON boolean `true` untouched; submitting `true` as the `verification_code` satisfies the loose comparison against the session's non
CVE-2026-77765	The Better Payment WordPress plugin before 2.3.4 does not validate the submitted payment amount server-side against the merchant's configured fixed price befo
CVE-2026-100526	OpenClaw's Discord integration (npm package @openclaw/discord) before version 2026.9.3 could lose the sender-scoped media policy in the emoji and sticker uplo
CVE-2026-83555	The Email Subscribers & Newsletters WordPress plugin before 5.9.35 does not verify the per-subscriber management token before changing a subscriber's subscrip
CVE-2026-84026	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.9.5 does not restrict access to a REST endpoint that returns use
CVE-2026-93353	copyparty contains a volume restriction bypass vulnerability in its SFTP front end that allows authenticated SFTP users to create, remove, and truncate arbitrary pa
CVE-2026-19532	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in HAVELSAN Inc. Liman MYS allows Path Traversal. This issue affects Li
CVE-2026-93623	Unauthenticated Insecure Direct Object References (IDOR) in AI Engine <= 3.7.8 versions.
CVE-2026-100527	OpenClaw before 2026.8.2 contains a denial of service vulnerability in the Browser extension relay that allows unauthenticated network sources to exhaust pendin
CVE-2026-97879	A security flaw has been discovered in zhistaredu StarTraining up to 3.8.1. The affected element is an unknown function of the file SecurityConfig.java of the comp
CVE-2026-100699	Nodemailer is a Node.js email-sending library. In versions >= 9.1.0 and < 10.0.9, the address parser (src/addressparser) mishandles addresses whose local-part is
CVE-2026-94079	Unauthenticated Broken Access Control in WP User Manager <= 2.9.19 versions.
CVE-2026-88831	BusyBox httpd IP deny rules with invalid CIDR prefix lengths fail open, leaving a parsed IP with a zeroed mask so the rule matches no clients.
CVE-2026-100545	OpenClaw (npm package `openclaw`) before 2026.8.1 incorrectly enforces sender tool policies during session-memory filename generation. In affected versions, fi
CVE-2026-88370	libconfini 1.16.4 contains a heap out-of-bounds write condition involving the bundled load_ini_buffer.h utility and strip_ini_cache(). The bundled utility allocates exa
CVE-2026-3626	IBM Concert 1.0.0 through 3.0.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. T

CVE-2026-100548	OpenClaw (npm package 'openclaw') versions >= 2026.3.28 and < 2026.8.1 contain a credential exposure issue in memory embedding failover. When remote eml
CVE-2026-87071	The Forminator Forms WordPress plugin before 1.57.2.1 does not restrict which metadata keys a form submission may supply, and does not exclude the keys Worc
CVE-2026-100572	OpenClaw versions >= 2026.3.25 and < 2026.8.1 apply invalid-token rate limiting for Synology Chat webhooks before authentication and key the limit on the raw
CVE-2026-100613	capgo.app is an over-the-air (OTA) update platform for Capacitor apps. In all versions up to and including the current release (no patch available at time of publicat
CVE-2026-48072	Docmost is open-source collaborative wiki and documentation software. Prior to 0.80.1, the public avatar and logo image endpoint accepts attacker-controlled fileh
CVE-2026-87978	The Paymob for WooCommerce WordPress plugin before 4.1.14 does not verify the request signature on one branch of its payment webhook, allowing unauthentic
CVE-2026-90950	The Paid Membership Subscriptions WordPress plugin before 3.1.0 does not verify the reCAPTCHA on its registration handler when a form field is absent from the r
CVE-2026-95600	Unauthenticated Sensitive Data Exposure in TrustedLogin Connector <= 2.0.3 versions.
CVE-2026-95592	Unauthenticated Insecure Direct Object References (IDOR) in Team <= 6.0.0 versions.
CVE-2026-87070	The Forminator Forms WordPress plugin before 1.57.2.1 does not verify that a request came from a trusted proxy before preferring client-supplied forwarding head
CVE-2026-95514	Unauthenticated Bypass Vulnerability in Netgsm <= 2.10.0 versions.
CVE-2026-100601	ClawHub (openclaw/clawhub) application/backend contains a server-side request forgery vulnerability in the public profile preview's image fetching. The preview a
CVE-2026-97864	A vulnerability has been found in GibbonEdu Gibbon up to 30.0.01. The affected element is the function makeBlock of the file modules/Planner/units_add_blockAjax
CVE-2026-100600	ClawHub (the openclaw/clawhub application/backend) does not bind anonymous HTTP API requests to a trusted caller identity, so all direct anonymous API request
CVE-2026-84091	The SUMIT Payment Gateway for WooCommerce WordPress plugin before 4.0.0 does not verify with the payment provider that a payment notification is genuine b
CVE-2026-100230	Input Leap (aka input-leap) through 3.0.3, when the non-default --enable-drag-drop option is used on Windows or macOS, mishandles the / versus \ distinction and
CVE-2026-11871	The Team Members WordPress plugin before 9.3 does not perform any authorization or visibility check in an unauthenticated AJAX action that returns full team me
CVE-2026-73858	Solspace Freeform plugin for Craft CMS 5.x is a super flexible form-building tool. From 5.0.0 through 5.10.13, submitted values from public Freeform forms can be c
CVE-2026-100571	OpenClaw (npm package 'openclaw') versions >= 2026.6.6 and < 2026.8.1 apply the SMS webhook invalid-request rate limit before Twilio signature verification ar
CVE-2026-84712	A flaw was found in the automation-controller API. The unauthenticated health-check endpoint /api/v2/ping/ (ApiV2PingView, AllowAny) over-serializes RBAC-gated
CVE-2026-96880	A vulnerability was found in TaleLin lin-cms-spring-boot up to 0.2.1. This impacts the function getBook of the file src/main/java/io/github/talelin/latticy/controller/v1/
CVE-2026-100648	vllm before 0.29.0 fails to enforce VLLM_MAX_AUDIO_CLIP_FILESIZE_MB limit in multimodal chat audio decoding, allowing unauthenticated clients to bypass file siz

CVE-2026-93511	The Premium Packages WordPress plugin before 7.2.1 does not verify PayPal's webhook signature before processing payment and subscription notifications, allowi
CVE-2026-84717	A flaw was found in the Ansible Automation Platform automation-controller. The unauthenticated Bitbucket Data Center webhook receiver skips HMAC signature ve
CVE-2026-97058	sprintf-js through 1.1.3 passes unbounded precision specifiers to toFixed, toExponential, and toPrecision methods without validation, causing uncaught RangeError
CVE-2026-89331	The FluentBoards WordPress plugin before 2.1.0 does not properly restrict the member data returned by its public, token-shared board feature, allowing unauthent
CVE-2026-100667	grav-plugin-login (the Grav CMS Login plugin) versions >= 3.8.7 and < 3.9.7 allow the two-factor authentication challenge to be bypassed for content gated by the
CVE-2026-96772	A security flaw has been discovered in Intelliant's Subrion CMS up to 4.2.1. This affects an unknown part of the file /actions.json?action=assign-owner. The manipula
CVE-2026-100647	vLLM versions before 0.29.0 contain a denial-of-service vulnerability in the cache_salt parameter accepted on OpenAI-compatible and Anthropic API endpoints, whi
CVE-2026-91814	A signature validation vulnerability exists in Foxit PDF Editor/Reader's handling of incrementally updated PDF documents. Changes to visible document content ma
CVE-2026-96606	A security flaw has been discovered in LB-Link BL-CPE600EU 5.8.13. This vulnerability affects unknown code of the file Mifi_config.bin of the component Configurati
CVE-2026-85290	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. Prior to 1.7.2, InvoicePlane's Cron::recur() method writes an inv
CVE-2026-6925	IBM Concert 1.0.0 through 3.0.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request contain
CVE-2026-90985	The WPC Smart Compare for WooCommerce WordPress plugin before 6.6.1 does not apply WordPress's post-password protection when returning product content t
CVE-2026-77320	TREK is a collaborative travel planner. Prior to 3.3.0, getSharedTripData in server/src/services/shareService.ts returns days, assignments, dayNotes, and places thr
CVE-2026-96774	A vulnerability was found in SPON Communications IP Network Audio Device XC-9603 1.2.3_20181106 Build 107. This affects the function loadCfg of the file /ini/sys
CVE-2026-52853	Docmost is open-source collaborative wiki and documentation software. Prior to 0.90.1, an authenticated workspace ADMIN can use the workspace invitation flow t
CVE-2026-97732	IRONMACE Ironshield 1.0.0.167 has a tvk.sys kernel-mode driver that authenticates client executables by checking for expected publisher and root-certificate strin
CVE-2026-17503	IBM PowerVM Hypervisor FW1120.00 through FW1120.01, FW1110.00 through FW1110.31, FW1060.00 through FW1060.81, and FW950.00 through FW950.H3 is af
CVE-2026-17504	IBM PowerVM Hypervisor FW1120.00 through FW1120.01, FW1110.00 through FW1110.31, FW1060.00 through FW1060.81, and FW950.00 through FW950.H3 is af
CVE-2026-17413	IBM PowerVM Hypervisor FW1120.00 through FW1120.01, FW1110.00 through FW1110.31, FW1060.00 through FW1060.81, and FW950.00 through FW950.H3 is af
CVE-2026-71458	URLModificationMiddleware resolves named-URL lookups against unfiltered Model.objects before RBAC. The 403→404 shim only rewrites 403 responses, leaving th
CVE-2026-96747	The client-side field level encryption support in the MongoDB Python Driver can treat a key management endpoint value ending in ".sock" as a local Unix domain so
CVE-2026-91121	Discourse is an open-source discussion platform. Prior to 2026.1.8, 2026.6.3, 2026.7.2, and 2026.8.0, attacker-controlled upload filenames used in chat message e

CVE-2026-100502	Flame through 2.4.0 contains an insufficient session expiration vulnerability in the login endpoint that allows attackers with former admin access to obtain tokens v
CVE-2026-84046	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.9.5 does not validate a user-supplied URL before fetching it sen
CVE-2026-71459	JobJobEventsChildrenSummary view has no model/parent_model. ModelAccessPermission.check_get_permissions() falls through (returns True) for any authenticate
CVE-2026-17602	The SSL Zen — SSL Certificate Installer & HTTPS Redirects plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 4.7.42 via tl
CVE-2026-39372	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. Prior to 1.7.2, InvoicePlane stores and serves uploaded image a
CVE-2026-100710	Froxlor through 2.3.10 does not filter sensitive columns from API responses: Domains::get(), Domains::listing(), SubDomains::get(), and the admin branch of SubDo
CVE-2026-94408	Uncontrolled Resource Consumption (CWE-400) in Elasticsearch can lead denial of service via Excessive Allocation (CAPEC-130)
CVE-2026-77825	IBM ContextForge MCP Gateway 1.0.0 through 1.0.8 was vulnerable to path traversal in its Admin API log-download endpoint (`GET /v1/admin/logs/file`). The path c
CVE-2026-63002	REDAXO is a PHP-based content management system. Prior to 5.21.2, redaxo/src/addons/mediapool/pages/sync.php inserts filenames held in \$diffFiles from the m
CVE-2026-85292	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. Prior to 1.7.2, InvoicePlane's User_Controller compares the sess
CVE-2026-63001	REDAXO is a PHP-based content management system. Prior to 5.21.2, the mediaIsInUse() handler in redaxo/src/addons/media_manager/lib/media_manager.php ins
CVE-2026-85293	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. In version 1.7.2-beta-1, InvoicePlane stores client_email values
CVE-2026-86604	The GTranslate WordPress plugin before 5.0.1 does not remove shortcodes from the content of outgoing emails before expanding them which, in a non-default con
CVE-2026-94457	Unauthenticated Bypass Vulnerability in Captcha Code <= 3.32 versions.
CVE-2026-87981	The Paymob for WooCommerce WordPress plugin before 4.1.14 does not perform a capability check on several admin AJAX actions that manage its payment-gatew
CVE-2026-100634	SiYuan before v3.8.4 does not validate the sender or restrict recipients in the 'siyuan-send-windows' IPC handler of the Electron main process (app/electron/main.js
CVE-2026-100640	SiYuan before v3.8.4 contains an authorization omission in the siyuan-get IPC handler that allows remote-kernel renderers to access native clipboard formats by in
CVE-2026-91788	When implementing the JavaScript interface, Foxit PDF Editor/Reader did not perform the attribute authorization checks required by the specification. As a result, a
CVE-2026-97649	A flaw has been found in ningzichun student-management-system up to 98760f5711cf6dc8b4adca53a9e207ca49b02ebf. Affected by this vulnerability is an unknow
CVE-2026-81338	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.50 does not properly sanitise and restrict HTML in user-submitted content before storing it and
CVE-2026-82716	The Botslab G980H dash camera firmware includes sensitive configuration information, including WiFi credentials, in diagnostic logs generated during the support
CVE-2026-96545	An out-of-bounds heap read flaw was found in GIMP's TIM image loader. When a user opens a crafted 4bpp TIM image that causes promotion to an RGBA layer, the

CVE-2026-19087	IBM Financial Transaction Manager (FTM) for RedHat OpenShift could allow a local attacker to achieve privilege escalation within the container due to improper priv
CVE-2026-56792	Dell Rugged Control Center (RCC), versions prior to 5.2.206, contain an Improper Authorization vulnerability. A low privileged attacker with local access could poter
CVE-2026-96674	alsa-lib through 1.2.16.1 computes combined topology element size using 32-bit arithmetic in src/topology/ctl.c, allowing integer overflow that defeats bounds che
CVE-2026-100505	Ghidra versions 9.2 through 12.1.4 contain a heap out-of-bounds read vulnerability in StringManager::getCodepoint when decoding multi-byte UTF-8, UTF-16, or UT
CVE-2026-100628	capgo.app before 12.128.12 fails to enforce an organization's API key expiration policy when creating app-scoped API keys. In the POST /apikey endpoint, requests
CVE-2026-62998	REDAXO is a PHP-based content management system. Prior to 5.21.2, rex_list::getSortColumn() in redaxo/src/core/lib/list.php accepts the sort request parameter w
CVE-2026-61834	scim-patch is a library for applying SCIM patch operations. Prior to 0.9.2, navigate() reads inherited properties and assign() uses prototype-chain membership chec
CVE-2026-100313	A weakness has been identified in mathurvishal CloudClassroom-PHP-Project up to 5dadec098bfbf3300d60c3494db3fb95b66e7be. This affects an unknown functi
CVE-2026-96773	A weakness has been identified in Intellian's Subrion CMS up to 4.2.1. This vulnerability affects the function iaUsers::authorize of the file front/login.php of the com
CVE-2026-100621	Capgo (capgo.app) contains an incomplete access-control/content-lock enforcement issue affecting all versions; no patch is available at the time of publication. The upload content immutability hardening added for a previous app_versions metadata-tampering issue.
CVE-2026-100626	capgo through 12.128.2 contains an insecure direct object reference vulnerability in the PUT /app/:appId endpoint that accepts attacker-controlled icon storage pat
CVE-2026-100674	stoatchat before 0.15.5 fails to revalidate usernames after Unicode sanitization, allowing attackers to create usernames with forbidden characters by submitting Ur
CVE-2026-91025	The Booking Manager WordPress plugin before 2.1.21 does not verify that a request to modify a user's Booking Manager WordPress plugin before 2.1.21-specific se
CVE-2026-96764	A weakness has been identified in kvcache-ai mooncake up to 0.3.12/0.3.14-rc1. Impacted is the function MasterService::GetReplicaListByRegex of the component
CVE-2026-86602	The WP Recipe Maker WordPress plugin before 10.8.2 does not perform any capability check in one of its AJAX actions, allowing any authenticated user, such as a s
CVE-2026-97061	Black Candy through 3.2.1 fails to scope playlist search queries to the authenticated session user, allowing any authenticated user to enumerate all playlists on the
CVE-2026-96680	A vulnerability was detected in ByteDance Coze Scraper Extension up to 2.0.2. Affected by this vulnerability is the function chrome.runtime.onMessageExternal.ad
CVE-2026-92529	GitLab has remediated an issue in GitLab EE affecting all versions from 19.1 before 19.2.7, 19.3 before 19.3.3, and 19.4 before 19.4.1 that under certain conditions
CVE-2026-100590	OpenClaw before 2026.7.1 contains an authorization bypass vulnerability in the /voice set command that allows non-owner external-channel senders to persist Gat
CVE-2026-92530	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 19.1 before 19.2.7, 19.3 before 19.3.3, and 19.4 before 19.4.1 that under certain condi
CVE-2026-86603	The WP Recipe Maker WordPress plugin before 10.8.2 does not have any authorisation check in one of its AJAX actions, allowing any authenticated user, such as a
CVE-2026-93510	The Points and Rewards for WooCommerce WordPress plugin before 2.10.4 does not validate the claimed reward amount or restrict who can call its Win Wheel clai
CVE-	

CVE-2026-96739	A flaw has been found in SEMCMS up to 4.2. Affected by this issue is some unknown functionality of the file /Edit/php/upload_json.php of the component KindEditor
CVE-2026-77321	TREK is a collaborative travel planner. Prior to 3.3.0, the get_trip_summary tool in server/src/mcp/tools/trips.ts is registered for scoped OAuth MCP tokens without r
CVE-2026-96652	Plex Media Server before 1.43.3.10861 allows SSRF via '/player/timeline'. An attacker using any X-Plex-Token value can include a full URL in the 'protocol' paramete
CVE-2026-100583	OpenClaw Discord versions before 2026.7.1 contain an authorization bypass vulnerability in guild metadata read actions that allows lower-trust senders to retrieve
CVE-2026-6327	IBM Concert 1.0.0 through 3.0.0 could allow an unauthorized user to inject data into log messages due to improper neutralization of special elements when written
CVE-2026-57177	Python Social Auth is a social authentication/registration mechanism. Prior to version 5.0.0, the LoginRadius backend did not validate OAuth state during the auth
CVE-2026-79759	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. From 1.7.0 until 2.5.1, the POST /credentials/:id/depl
CVE-2026-97469	PostgreSQL Anonymizer contains a vulnerability that allows unprivileged masked users to repeatedly call the anon.hash() function and collects (seed, hash_output)
CVE-2025-32000	HCL Sametime is vulnerable to insufficient input sanitization. The application did not appropriately sanitize user input. When user input is implicitly or explicitly tru
CVE-2026-81508	ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. In 5.5.5, 6.0.1, and 6.1, the BlueDroid A2DP sink function btc_a2dp_sink_handle_inc_med
CVE-2026-97224	A vulnerability was detected in Excalidraw up to 0.18.1. The impacted element is an unknown function of the file packages/excalidraw/data/restore.ts of the compo
CVE-2026-97724	A prototype pollution vulnerability in Software Mansion React Native Worklets before 0.12.2 allows an attacker-controlled object containing a __proto__ property to
CVE-2026-48073	Docmost is open-source collaborative wiki and documentation software. From 0.70.0 until 0.80.1, a low-privileged authenticated user who can edit an exportable p
CVE-2026-52850	Docmost is open-source collaborative wiki and documentation software. Prior to 0.90.1, an authenticated workspace member who does not belong to a private spa
CVE-2026-93363	The @payloadcms/storage-vercel-blob storage adapter for Payload contains an improper access control vulnerability that allows authenticated users to bypass coll
CVE-2026-93364	Bludit CMS through 3.22.0 contains a mass assignment vulnerability that allows authenticated users with the Author role to modify privileged page fields reserved
CVE-2026-93513	Contributor Insecure Direct Object References (IDOR) in SiteSkite <= 2.1.7 versions.
CVE-2026-100305	TDuck survey form through 6.0 fails to enforce form fill-in restrictions on the authenticated submission endpoint POST /user/form/data/create. Authenticated attack
CVE-2026-62286	Dozzle is a realtime log viewer for docker containers. Prior to 10.6.7, streamEvents in internal/web/events.go applies a restricted user's label filter to container lists
CVE-2026-84718	A flaw was found in the Ansible Automation Platform automation-controller. In the shipped production configuration, the Controller trusts the client-supplied X-Forw
CVE-2026-18870	IBM PowerVM Hypervisor FW1120.00 through FW1120.01, FW1110.00 through FW1110.31, FW1060.00 through FW1060.81, and FW950.00 through FW950.H3 coul
CVE-2026-6103	phar_tar_number() parses the octal size field of a TAR header into a uint32_t with no overflow check. The field is 11 octal digits wide and holds values up to 0x1FFF
CVE-	

CVE-2026-96551	A vulnerability was determined in sfturing hosp_order up to 627f426331da8086ce8fff2017d65b1ddef384f8. Impacted is an unknown function of the file ssm_pro/sr
CVE-2026-91769	PHP's OpenSSL stream peer verification checks the certificate's subjectAltName entries first and, whenever no entry matches, falls back to the Common Name. RFC
CVE-2026-71461	HostList.list() catches bare Exception and returns str(e) verbatim. Via host_filter, any authenticated user triggers Django FieldError (leaking complete Host model re
CVE-2026-71460	/api/v2/config/ is protected only by IsAuthenticated. license_info (account_number, subscription_id, pool_id, sku, support_level, instance counts) returned to any au
CVE-2026-100525	The OpenClaw Prometheus diagnostics plugin (@openclaw/diagnostics-prometheus) before version 2026.9.3 does not enforce the operator.read scope on its auth
CVE-2026-55632	GoCD is a continuous deliver server. From 20.2.0 until 26.1.0, the internal pipeline structure API used for autocompletion while editing pipeline, template, environn
CVE-2026-96655	Plex Media Server before 1.43.3.10861 allows an authenticated user to request arbitrary internal or external addresses via the '/video:/transcode/universal' path p
CVE-2026-84027	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.9.5 does not check user capabilities when creating orders throu
CVE-2026-97322	A vulnerability was found in YunaiV/zhijiantianya ruoyi-vue-pro up to 2026.08. This affects an unknown function of the file yudao-module-infra/src/main/java/cn/iocc
CVE-2026-100553	OpenClaw versions >= 2026.6.9 and < 2026.8.1 do not declare the native chatId parameter as a delivery target in the Feishu unpin feature, so unpin requests can
CVE-2026-95957	A vulnerability was found in SourceCodester Smart Attendance System with QR Code Scanner 1.0. This issue affects the function prepend of the file student_signu
CVE-2026-91132	Discourse is an open-source discussion platform. Prior to 2026.1.8, 2026.6.3, 2026.7.2, and 2026.8.0, sites using wildcard patterns in the allowed_iframes setting c
CVE-2026-19775	The OpenStation — Desktop Windows, Dock & Virtual Desktops for WP Admin plugin for WordPress is vulnerable to authorization bypass in all versions up to, and in
CVE-2026-78310	Authorization Bypass Through User-Controlled Key in DIAEnergie. This issue affects DIAEnergie: before 1.11.00.022.
CVE-2026-97179	A security vulnerability has been detected in O2OA up to 9.5.3/10.0.2. This vulnerability affects the function list of the file o2server/x_base_core_project/src/main/ja
CVE-2026-81339	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.50 does not perform a per-object ownership check when returning a quiz attempt result, allow
CVE-2026-77766	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.9.5 does not scope one of its REST collection endpoints to the r
CVE-2026-92829	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 9.1.0. This is du
CVE-2026-97311	A flaw was found in the Admin REST API of Keycloak, an identity and access management solution. The endpoints used to retrieve groups associated with a specific
CVE-2026-88847	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.50 does not verify that a user is enrolled in a course before recording lesson completions agai
CVE-2026-93662	The Events Manager WordPress plugin before 7.4.5 does not force the scope of its logged-in event and location search when a caller supplies their own owner valu
CVE-2026-88845	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.50 does not perform any capability or nonce checks on an administrative maintenance action,
CVE-	

CVE-2026-16302	The Spectra Legacy – Gutenberg Blocks plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.20.0 via the edit
CVE-2026-82850	The Masteriyo LMS WordPress plugin before 3.4.2 does not restrict access to quiz answer keys, allowing any authenticated user, such as a student, to retrieve the c
CVE-2026-96258	A vulnerability has been found in onSite internet GmbH Auktion NG Auktionssoftware up to 20260722. This affects an unknown part of the file /forgotpasswd.html c
CVE-2026-96892	A flaw has been found in Edimax BR-6428nC 1.16. The impacted element is the function websRedirect of the component goform Handler. Executing a manipulation
CVE-2026-3253	The MailerLite – Signup forms (official) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the forms() me
CVE-2026-18364	The zportals WordPress plugin before 6.4.2 does not perform any capability or nonce check on several of its AJAX actions, allowing users with a subscriber-level acc
CVE-2026-97325	A security flaw has been discovered in YunaiV/zhijiantianya ruoyi-vue-pro up to 2026.08. Affected by this vulnerability is the function validOAuthClientFromCache o
CVE-2026-82849	The Masteriyo LMS WordPress plugin before 3.4.2 does not verify that the user making the request owns the course-progress records being returned, allowing any
CVE-2026-97650	A vulnerability has been found in ningzichun student-management-system up to 98760f5711cf6dc8b4adca53a9e207ca49b02ebf. Affected by this issue is the funct
CVE-2026-18365	The zportals WordPress plugin before 6.4.2 does not perform any capability or nonce check on one of its AJAX actions, allowing users with a subscriber-level accou
CVE-2026-97648	A vulnerability was detected in ningzichun student-management-system up to 98760f5711cf6dc8b4adca53a9e207ca49b02ebf. Affected is an unknown function. Po
CVE-2026-96446	A flaw was found in the Pushed Authorization Request PAR implementation of Keycloak. The issue occurs when the silent authentication path prompt=none is used
CVE-2026-100554	OpenClaw (npm package 'openclaw') versions >= 2026.5.12 and < 2026.8.1 do not immediately invalidate Canvas HTTP authorization when a paired node is revol
CVE-2026-97176	A flaw was found in the Level of Authentication enforcement mechanism of Keycloak, an identity and access management solution. The issue occurs when a client
CVE-2026-88848	The MasterStudy LMS WordPress plugin from 1.9 before 3.7.50 does not verify that a course a member asks to enrol in is covered by their membership plan, nor th
CVE-2026-57179	Python Social Auth is a social authentication/registration mechanism. Prior to version 5.0.0, the partial-pipeline resume mechanism accepted `partial_token` as a b
CVE-2026-84302	Discourse is an open-source discussion platform. Prior to 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0, Discourse AI reviewables associated with private messages c
CVE-2026-100373	OpenMetadata through 2.0.2 contains a server-side request forgery vulnerability in the URLValidator.validateURL function that fails to properly resolve DNS hostna
CVE-2026-78394	The Link Library WordPress plugin before 7.9.6 does not sanitize a user-supplied destination folder before writing a generated image to disk, allowing users with th
CVE-2026-97869	A flaw has been found in langchain4j up to 1.5.3-beta10/1.11.10-beta18/1.18.1-beta27. This vulnerability affects the function AgenticScopeSerializer.fromJson of th
CVE-2026-71462	StringListPathField.to_internal_value() calls os.path.exists() on unbounded user-supplied paths. 200 vs 400 response reveals existence of arbitrary absolute paths c
CVE-2026-78397	The Link Library WordPress plugin before 7.9.6 does not validate the destination of a user-supplied URL before falling back to an unprotected fetch when its safe re
CVE-	

CVE-2026-96807	In Flatpak before 1.18.1, a malicious sandboxed app can replace ~/.var/app/\$appid/.ld.so with a symlink, causing regenerate_ld_cache to write files at an arbitrary
CVE-2026-84743	The Events Calendar WordPress plugin before 6.17.5 does not perform a per-object capability check on one family of its REST write routes, allowing users with a lo
CVE-2026-100620	Capgo CLI (npm package @capgo/cli) through 7.98.2 is affected by an over-permissioned service account in its Android onboarding flow. When onboarding via Goo
CVE-2026-100649	vLLM before 0.29.0 contains a resource-limit bypass vulnerability in PyNvVideoCodec decoder allocation where sampler subclass shadowing allows independent co
CVE-2026-71178	Dell Secure Connect Gateway (SCG) Policy Manager, versions prior to 5.34.00.16, contains an Use of Non-Canonical URL Paths for Authorization Decisions vulnerab
CVE-2026-87848	The MPCX Lightbox WordPress plugin 1.2.2 through 1.2.5 does not have any authorisation or authentication on one of its AJAX actions available to unauthenticated
CVE-2026-77756	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') vulnerability in Apache Tomcat caused by processing the transfer-encoding hea
CVE-2026-93528	The NP Quote Request for WooCommerce WordPress plugin before 2.4.16 does not verify order ownership before rendering an order's details, allowing unauthentic
CVE-2026-97764	django-allauth before 65.19.4 does not have the expected limits on failed login attempts because, in some common configurations, an attacker can leverage the h
CVE-2026-96550	A vulnerability was found in sfturing hosp_order up to 627f426331da8086ce8ff2017d65b1ddef384f8. This issue affects the function getProperties of the file ssm_p
CVE-2026-90951	The Paid Membership Subscriptions WordPress plugin before 3.1.0 does not bind one of its unauthenticated payment actions to the requesting user, allowing some
CVE-2026-87074	The Forminator Forms WordPress plugin before 1.57.2.1 does not bind its saved-draft notification to the visitor who created the draft, and takes both the recipient i
CVE-2026-77797	Velociraptor's prefetch library contains an out of bound vulnerability which may cause a crash when parsing certain malformed prefetch files.
CVE-2026-100311	A vulnerability was identified in mathurvishal CloudClassroom-PHP-Project up to 5dadec098bfbf3300d60c3494db3fb95b66e7be. The affected element is an unknc
CVE-2026-97896	A vulnerability was identified in krayin laravel-crm up to 2.2.5. This vulnerability affects the function ConfigurationForm::rules of the file packages/Webkul/Admin/sr
CVE-2026-97897	A security flaw has been discovered in Krayin laravel-crm up to 2.2.5. This issue affects some unknown processing of the file Sanitizer.php of the component TinyM
CVE-2026-97233	A vulnerability was identified in volotat Anagnorisis up to 0.4.11. Affected by this issue is the function html of the file PlaylistManager.js of the component Media Fil
CVE-2026-84151	The Post Grid WordPress plugin before 7.9.5 does not limit an expansion of the WordPress allowed-HTML list to its own markup and applies it site-wide, allowing us
CVE-2026-97868	A security vulnerability has been detected in sheshbabu zen up to 1.5.0. Affected by this issue is the function dangerouslySetInnerHTML of the file features/notes/N
CVE-2026-96810	A vulnerability was identified in huanzi-qch base-admin up to 52816b760cd53244989fd664bbb2b3d4edbfdbf1. This issue affects the function Save of the file base-
CVE-2026-63630	BentoPDF is a client-side PDF toolkit that is self hostable. In 2.8.6 and earlier, deserializeWorkflow() accepts the Timestamp node's tsaUrl control from imported JSC
CVE-2026-18857	IBM OPENBMC FW1120.00 through FW1120.01, FW1110.00 through FW1110.31, and FW1060.00 through FW1060.81 is affected by a vulnerability in the BMC firmv
CVE-2025-	The mysqlnd wire protocol parser reads fields out of server packets before checking that the packet still holds enough bytes for them. A malicious or compromised

1218	
CVE-2026-17511	IBM PowerVM Hypervisor FW1120.00 through FW1120.01, FW1110.00 through FW1110.31, FW1060.00 through FW1060.81, and FW950.00 through FW950.H3 is af
CVE-2026-96549	A vulnerability has been found in sfturing hosp_order up to 627f426331da8086ce8fff2017d65b1ddef384f8. This vulnerability affects unknown code of the file ssm_
CVE-2026-95958	A security flaw has been discovered in JusticeRage Manalyze 1.0.0. Impacted is the function PE::_parse_relocations of the file manape/pe.cpp of the component PE
CVE-2026-100573	OpenClaw versions before 2026.8.1 contain a sandbox policy bypass vulnerability in the MCP loopback component that allows sandboxed coding-agent sessions to
CVE-2026-93507	The WC Fields Factory WordPress plugin before 4.1.11 does not properly restrict access to, or verify a nonce for, a post-cloning action, allowing Contributor-level us
CVE-2026-18104	IBM Db2 Mirror for i 7.6, 7.5, and 7.4 could allow a local attacker to obtain sensitive information due to the use of the AES Electronic Codebook (ECB) mode for encr
CVE-2026-96675	alsa-lib through 1.2.16.1 contains a denial of service vulnerability in the multi PCM plugin that fails to validate sparse binding indices before array access. Attackers
CVE-2026-100503	Ghidra versions through 12.1.4 contain a heap use-after-free vulnerability in the decompiler's Funcdata::opInsertAfter function caused by stale INDIRECT effect-op
CVE-2026-19492	IBM PowerVM Hypervisor FW1120.00 through FW1120.01, FW1110.00 through FW1110.31, and FW1060.00 through FW1060.81 is affected by a vulnerability in a h
CVE-2026-71464	LaunchConfigurationBaseSerializer.scm_branch has no validate_scm_branch() leading-dash check, unlike Project/JobTemplate/JobLaunch serializers. Schedule and V
CVE-2026-100417	RustDesk before 1.5.0 on Windows fails to enforce the one-way file transfer option against peer clipboard file requests, allowing authenticated peers to read files fr
CVE-2026-96552	A vulnerability was identified in sfturing hosp_order up to 627f426331da8086ce8fff2017d65b1ddef384f8. The affected element is the function MD5.getMD5 of the f
CVE-2026-71465	RunAdHocCommand.build_args() appends limit as bare positional (args.append(limit)) instead of using args.extend(['-l', limit]) like RunJob. A limit beginning with -
CVE-2026-92628	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.6 before 19.2.7, 19.3 before 19.3.3, and 19.4 before 19.4.1 that under a race conditio
CVE-2026-87069	The Forminator Forms WordPress plugin before 1.57.2.1 does not perform a nonce, capability or ownership check before running a one-time payment-field migratio
CVE-2026-100534	OpenClaw versions before 2026.8.1 contain an authorization bypass vulnerability in webhook TaskFlow cancellation that allows attackers to cancel unrelated sessio
CVE-2026-100537	OpenClaw (npm package 'openclaw') before 2026.8.1 fails to apply the originating requester's effective tool policy during Active Memory automatic recall. In deplo
CVE-2026-100542	OpenClaw (npm package 'openclaw') versions >= 2026.5.28 and < 2026.8.1 mishandle archive listings in the tar.bz2 skill installer: bounded command-output suffi
CVE-2026-73064	In Mbed TLS 3.2.0 though 3.6.6 and 4.0.0 through 4.1.0, an attacker who can cause an entropy source to fail can remove or inject bytes into the start of the TLS str
CVE-2026-96526	The MCP Server for WordPress WordPress plugin before 1.8.2 does not perform an object-level authorization check on one of its workflow REST routes, allowing use
CVE-2026-97228	Rapid7 Bulk Export MCP versions 0.2.5 through 0.6.1 suffer from a GraphQL query injection issue in the export-status component (`get_export_status` in `src/expo
CVE-2026-	IBM Guardium Data Protection 12.2 could allow an administrative user to obtain sensitive information when a detailed technical error message is returned in the br

4921	
CVE-2026-89004	The WPeMatico RSS Feed Fetcher WordPress plugin before 2.8.26 does not verify ownership or authorization before returning a campaign's stored configuration an
CVE-2026-93661	The Events Manager WordPress plugin before 7.4.5 does not stop a ticket-update request from replacing the identifiers of the ticket it was authorized against, lettir
CVE-2026-96525	The MCP Server for WordPress WordPress plugin before 1.8.2 does not perform an ownership or sufficient capability check on its workflow create, update and delet
CVE-2026-71463	Notification template Jinja AST whitelist only inspects static Getattr nodes. Dynamic subscripts (job['job'+'_env']) and {% if job.id > 100 %} conditional gating bypa
CVE-2026-91077	The Event Booking Manager for WooCommerce WordPress plugin before 5.7.3 does not restrict its event listing query to events the requesting user is permitted to
CVE-2026-97721	A weakness has been identified in Sanluan PublicCMS up to 6.202506.e. This vulnerability affects the function CmsContentAdminController of the file publiccms-pai
CVE-2026-84742	The Events Calendar WordPress plugin before 6.17.5 does not check the capability required to publish content before creating or updating it through its REST API, i
CVE-2026-100539	OpenClaw (npm package 'openclaw') before 2026.8.1 fails to revoke memory tool access when an operator hot-disables memory configuration. Existing memory_s
CVE-2026-96546	A one-byte out-of-bounds heap read flaw was found in GIMP's uncompressed DDS image loader. When a user opens an uncompressed DDS image, the file-dds plug
CVE-2026-97487	In the Linux kernel, the following vulnerability has been resolved: jfs: handle set_blocksize failures jfs uses buffer_heads, which don't handle block size > PAGE_SIZ
CVE-2026-88371	ZBar commit 2ea2ca58 contains an undefined-behavior vulnerability in the Code 128 decode6() function. When processing specially crafted Code 128 input, decod
CVE-2026-90903	Joomla Extension - joomshaper.com - Missing CSRF Token Verification across Administrator AJAX API Endpoints in Easy Store extension 1.0.0-3.0.0 - The administra
CVE-2026-56723	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.2, a customer who can view a ticket cannot see internal ticket articles throug
CVE-2026-57861	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-66071	RabbitMQ is a messaging and streaming broker. From 3.13.0 until 3.13.15 and 4.0.22 and 4.1.11 and 4.2.6 and 4.3.1, Atom exhaustion: OAuth2 JWT tag: scope val
CVE-2026-53990	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-56724	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.2, summary An issue with permission checks in the knowledge base manager
CVE-2026-56729	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.2, when multiple KB categories have different editor roles assigned, a user wi
CVE-2026-96875	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Mediawiki - Cargo extension allows Stored XSS. This issue affect
CVE-2026-90904	Joomla Extension - joomshaper.com - Broken Access Control (ACL Bypass) in ApiController Record Editing in Easy Store extension 1.0.0-3.0.0 - The allowEdit() meth
CVE-2026-61837	RabbitMQ is a messaging and streaming broker. From 4.0.0 until 4.3.3, 4.2.9, 4.1.14, and 4.0.23, AMQP 1.0 management GET /bindings exposes full binding topolo Confidentiality impact: a non-management AMQP 1.0 user can enumerate the complete routing topology of any virtual host it can connect to , every (source excha
CVE-2026-	Joomla Extension - joomshaper.com - Missing CSRF and Access Control on Site Configuration Update in Easy Store extension 1.0.0-3.0.0 - The endpoint administrat

90905	
CVE-2026-92284	Caddy is an extensible server platform that uses TLS by default. In version 2.11.3 and earlier, in modules/caddyhttp/replacer.go, resolving http.request.body reads
CVE-2026-92692	Sulu is an open-source PHP content management system based on the Symfony framework. Prior to 2.6.25 and 3.0.8, the affected Sulu 2.6 and 3.0 release lines ha
CVE-2026-80432	Missing Authorization in the drop handling path of the drag and drop protocol in kitty from 0.47.0 before 0.49.0 allows a program writing to the terminal to obtain t without ever releasing them into it.
CVE-2026-96877	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Mediawiki - Cargo extension allows Reflected XSS. This issue aff
CVE-2026-84460	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, any authenticated user can call the REST endpoint for getting a tag list and
CVE-2026-63207	Zammad is a web based open source helpdesk/customer support system. In 7.0.3 and 7.1.1, an authenticated administrator can obtain stored integration credenti
CVE-2026-63208	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, when a Microsoft Graph request fails, Zammad logs the error including the
CVE-2026-63216	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, unsanitized option labels are rendered in the configuration dialogs of AI Ag
CVE-2026-84458	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, when the "Automatic account link on initial logon" setting is enabled, Zamm
CVE-2026-93283	In the Linux kernel, the following vulnerability has been resolved: i3c: master: Fix device_register() error path When device_register() fails in i3c_master_register_n
CVE-2026-67223	RabbitMQ is a messaging and streaming broker. The advisory establishes affected 3.13, 4.0, 4.1, 4.2, and 4.3 maintenance lines but contains conflicting first-fixed
CVE-2026-56744	`@bsv/wallet-toolbox` provides BRC-100 wallet signing and storage components, while `@bsv/wallet-toolbox-client` and `@bsv/wallet-toolbox-mobile` provide clie storage, or independently verify every transaction output's locking script and value against the original request before signing
CVE-2026-84461	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, the two-factor login step let an attacker try unlimited password guesses fo
CVE-2026-97488	In the Linux kernel, the following vulnerability has been resolved: qnx4: handle set_blocksize failures qnx4 uses buffer_heads, which don't handle block size > PAGI
CVE-2026-84463	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, a user with Knowledge Base editing rights for a category can embed a vide
CVE-2026-84464	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, zammad's External Data Source feature, used to look up records from an e
CVE-2026-84465	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, when Zammad checks the digital signature on an incoming S/MIME-signed
CVE-2026-67222	RabbitMQ is a messaging and streaming broker. From 3.13.0 until 3.13.15, 4.0.20, 4.1.11, and 4.2.6, mechanisms/1 applied list_to_atom/1 to every colon-delimited
CVE-2026-92700	Caddy is an extensible server platform that uses TLS by default. In version 2.11.3 and earlier, in modules/caddyhttp/fileserver/staticfiles.go, fileHidden() uses case-
CVE-2026-66078	RabbitMQ is a messaging and streaming broker. From 3.13.0 until 3.13.15 and 4.0.20 and 4.1.11 and 4.2.6, protected tag bypass via bulk-delete. DELETE /api/users
CVE-2026-66073	RabbitMQ is a messaging and streaming broker. From 3.13.0 until 3.13.15 and 4.0.20 and 4.1.11 and 4.2.6, Atom table exhaustion via management API node field.
CVE-2026-	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Mediawiki - Cargo extension allows Reflected XSS. This issue aff

96876	
CVE-2026-93274	In the Linux kernel, the following vulnerability has been resolved: pinctrl: bcm2835: Don't remove an unregistered GPIO chip If the devm_pinctrl_register() function
CVE-2026-97510	In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Release request if tb_cfg_request() fails in __tb_xdomain_response() If tb_cfg_reques
CVE-2026-88366	NanoSVG commit 239e102ec contains an incorrect numeric conversion vulnerability in nsvg__pathArcTo() when parsing SVG arc commands. A specially crafted SV
CVE-2026-57864	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-97163	Joomla Extension - lomart.fr - Unauthenticated remote code installation in UP plugin extension 5.0.0-5.2.0, 6.0.0-6.0.29
CVE-2026-56738	phpMyFAQ is an open source FAQ web application. The `StopWords::add()` method inversions prior to 4.1.6 builds a SQL `INSERT` statement using `sprintf()` and
CVE-2026-26054	SumatraPDF is a multi-format reader for Windows. Prior to 3.6, the MobiDoc::ParseHeader function in src/MobiDoc.cpp validates a record using kMobiHeaderMinLer
CVE-2026-96874	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in the Mediawiki - Cargo extension allows Stored XSS. This issue af
CVE-2026-97162	Joomla Extension - lomart.fr - Various SQL injection vectors in UP plugin extension 5.0.0-5.2.0, 6.0.0-6.0.29
CVE-2026-97483	In the Linux kernel, the following vulnerability has been resolved: usb: core: hcd: fix possible deadlock in rh control transfers >From within the SCSI error handler n
CVE-2026-97161	Joomla Extension - lomart.fr - Various path traversal / file access vectors in UP plugin extension 5.0.0-5.2.0, 6.0.0-6.0.29
CVE-2026-63205	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, when creating or updating an email signature, Zammad processes inline in
CVE-2026-96879	Improper removal of sensitive information before storage or transfer vulnerability in Wikimedia Foundation's Mediawiki - FlaggedRevs extension through 1.46.0.
CVE-2026-9313	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-100381	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation Mediawiki - UploadWizard Extens
CVE-2026-100382	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Wikimedia Foundation Mediawiki - ExternalData Ext
CVE-2026-100383	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation Mediawiki - WikiLambda Extensio
CVE-2026-97514	In the Linux kernel, the following vulnerability has been resolved: media: chips-media: wave5: Fix Reports from Kernel Lock Validator handle_dynamic_resolution ct
CVE-2026-97482	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: goku_udc: avoid NULL deref of dev->driver in INT_USBRESET log goku_irq() handles
CVE-2026-77285	OpenBao is an open source identity-based secrets management system. Prior to 2.6.0, OpenBao Agent's exec rendering mode could write secrets from env_templ
CVE-2026-17545	On Windows, PHP's filesystem and stream APIs do not reject reserved device names such as CON, PRN, AUX, NUL, COM1 to COM9, LPT1 to LPT9, CONIN\$ and CONC
CVE-2026-97484	In the Linux kernel, the following vulnerability has been resolved: usbip: vhci_hcd: fix NULL deref in status_show_vhci platform_get_drvdata() can return NULL if a V

CVE-2026-97512	In the Linux kernel, the following vulnerability has been resolved: spi: spi-qcom-qspi: Fix incomplete error handling in runtime PM The runtime PM functions had inc
CVE-2026-96878	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Mediawiki - Cargo extension allows Reflected XSS. This issue aff
CVE-2026-90902	Joomla Extension - joomshaper.com - Authenticated, Privileged SQL Injection in Coupon Bulk Update in Easy Store extension 1.0.0-3.0.0 - The coupon bulk update t
CVE-2026-97511	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: avoid out-of-bounds access in monitor In NAN, we don't know on what band the f
CVE-2026-90901	Joomla Extension - joomshaper.com - Authenticated, Privileged SQL Injection in Media Image Deletion in Easy Store extension 1.0.0-3.0.0 - The media deletion endp
CVE-2026-100376	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation Mediawiki - TemplateSandbox Ex
CVE-2026-100377	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wikimedia Foundation Mediawiki - WikiLambda Extension allows Excavation. This issue i
CVE-2026-100378	Missing Authorization vulnerability in Wikimedia Foundation Mediawiki - Translate Extension allows Accessing Functionality Not Properly Constrained by ACLs. This
CVE-2026-100379	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wikimedia Foundation Wikipedia Android App allows Accessing/Intercepting/Modifying I
CVE-2026-100380	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation Mediawiki - Wikibase Extension a
CVE-2026-100248	The Rattadan Cosmowarp smart contract before 56c6147 can have a comparison to an unintended value of current_admin.
CVE-2026-90900	Joomla Extension - joomshaper.com - Missing CSRF Token Verification in Storefront Product Review Submission in Easy Store extension 1.0.0-3.0.0 - The product re
CVE-2026-97486	In the Linux kernel, the following vulnerability has been resolved: hpfs: handle set_blocksize failures hpfs uses buffer_heads, which don't handle block size > PAGE_
CVE-2026-90899	Joomla Extension - joomshaper.com - Unauthenticated PII Exposure via IDOR in Guest Checkout in Easy Store extension 1.0.0-3.0.0 - The checkout.searchGuestUse
CVE-2026-82368	Insecure access controls on internal service ports in Brocade SANnav versions before 3.0.1a allow local, non-administrative host users to communicate directly with
CVE-2026-97485	In the Linux kernel, the following vulnerability has been resolved: omfs: handle set_blocksize failures omfs uses buffer_heads, which don't handle block size > PAGI
CVE-2026-63206	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, zammad's HTML sanitizer, which blocks remote images in ticket articles an
CVE-2026-63204	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, an authenticated user with agent permissions can supply an arbitrary AI ar
CVE-2026-97507	In the Linux kernel, the following vulnerability has been resolved: media: dm1105: fix missing error check for dma_alloc_coherent The return value of dm1105_dma
CVE-2026-56735	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.2 and 7.1.0, zammad's HTML sanitizer (HtmlSanitizer::Strict) blocks external I
CVE-2026-67412	RabbitMQ is a messaging and streaming broker. From 3.13.0 until 4.3.3, 4.2.9 , 4.1.14, 4.0.24, and 3.13.18, Federation upstream in RabbitMQ skips vhost authoriza
CVE-2026-56728	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.2, a broken access control vulnerability exists in Zammad's GraphQL API. An i
CVE-	

CVE-2026-56730	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.2, an authorization bypass vulnerability was found that allows an authenticat
CVE-2026-56731	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.1, a low-privilege authenticated user may inject arbitrary HTML markup, inclu
CVE-2026-56732	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.2, vulnerability in Zammad's HTML sanitization allows injection of specific HTI
CVE-2026-56733	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.2 and 7.1.0, this issue concerns a lack of discursive validation within the auth the target system's functional authorization hierarchy, which allows for iterative escalation of the privileged access context. This issue is fixed in versions 7.0.2 and
CVE-2026-56734	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.2, during federated authentication (OAuth/OIDC/SAML), a profile image URL fi
CVE-2026-67411	RabbitMQ is a messaging and streaming broker. From 3.13.0 until 3.13.18, 4.0.23, 4.1.14, 4.2.9, and 4.3.3, native MQTT and MQTT over WebSocket behind a trustee
CVE-2026-97498	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/userq: pin mqd and fw object bo to avoid eviction mqd and fw objects are queue co
CVE-2026-61525	Zammad is a web based open source helpdesk/customer support system. In 7.0.2 and 7.1.0, zammad's session management for websocket and long-polling conne
CVE-2026-65828	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, the legacy destroy_form action on AttachmentsController deletes UploadC
CVE-2026-67410	RabbitMQ is a messaging and streaming broker. From 4.2.0 until 4.3.3 and 4.2.9, OAuth2 Client Secret Exposed via Unauthenticated JavaScript Endpoint (CWE-200 requests. Any RabbitMQ deployment with: This issue is fixed in versions 4.3.3 and 4.2.9.
CVE-2026-84462	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, a security filter that protects Zammad's AI Agent configuration can be byp
CVE-2026-97500	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: phy: check length before parsing PHY status IE Hardware might report PHY status IE v
CVE-2026-97499	In the Linux kernel, the following vulnerability has been resolved: coresight: perf: Retrieve path and source from event data ETM perf callbacks currently use the pe
CVE-2026-67409	RabbitMQ is a messaging and streaming broker. From 3.13.0 until 4.3.3, 4.2.9, 4.1.14, 4.0.23, and 3.13.18, JWKS Fetch Ignores HTTP Response Status Code - Signir authentication DoS: Once keys are destroyed, ALL OAuth2/JWT authentication fails for all users until a new successful JWKS refresh occurs Amplification: A single at
CVE-2026-56727	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.2, summary In Zammad's inbound PGP email processing, the return value of f
CVE-2026-56726	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.2, this vulnerability breaks normal ticket isolation boundaries between agents
CVE-2026-67413	RabbitMQ is a messaging and streaming broker. From 4.0.0 until 4.0.23, 4.1.14, 4.2.9, and 4.3.3, the optional rabbitmq_jms_topic_exchange plugin's x-jms-topic ex
CVE-2026-56725	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.2, summary An unauthenticated request to POST /api/v1/import/otrs/import_c
CVE-2026-93279	In the Linux kernel, the following vulnerability has been resolved: staging: octeon: add missing tasklet_kill in cvm_oct_tx_shutdown The TX cleanup tasklet can be s
CVE-2026-67421	RabbitMQ is a messaging and streaming broker. From 3.13.0 until 3.13.19, 4.0.24, 4.1.15, 4.2.10, and 4.3.5, RabbitMQ Management rendered an AMQP authorizati
CVE-2026-93278	In the Linux kernel, the following vulnerability has been resolved: staging: octeon: add missing napi_disable in cvm_oct_rx_shutdown cvm_oct_rx_shutdown calls fr
CVE-2026-67420	RabbitMQ is a messaging and streaming broker. From 3.13.0 until 3.13.19, 4.0.24, 4.1.15, 4.2.10, and 4.3.5, RabbitMQ OAuth credential refresh retains revoked run
CVE-	

CVE-2026-93281	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: fix HE extended capability length check rtw89_mac_check_he_obss_narrow_bw_ru_items
CVE-2026-67419	RabbitMQ is a messaging and streaming broker. Prior to 4.3.5, an authenticated user who can bind a queue to a topic exchange and publish to it can use consecutive publishes to cause a denial of service.
CVE-2026-97506	In the Linux kernel, the following vulnerability has been resolved: crypto: ixp4xx - fix buffer chain unwind on allocation failure chainup_buffers() builds a linked list of buffers
CVE-2026-97505	In the Linux kernel, the following vulnerability has been resolved: PCI/sysfs: Add CAP_SYS_ADMIN check to __resource_resize_store() Currently, the __resource_resize_store() function does not check for CAP_SYS_ADMIN
CVE-2026-95834	Use After Free in the drag source path of the drag and drop protocol in kitty from 0.47.0 before 0.49.0 allows a program writing to the terminal to cause the terminal to create that fails because an entry of the same name already exists, because the client may declare two entries with one name and the create operations use O_CREAT
CVE-2026-95835	Missing Authorization in the askpass escape code handler in kitty from 0.25.0 before 0.49.0 allows a local user other than the one running the terminal to obtain the user's password, including a masked password prompt, and read the typed secret back out of the object afterwards. The prompt text is additionally passed to the terminal
CVE-2026-67415	RabbitMQ is a messaging and streaming broker. From 4.2.0 until 4.2.9 and 4.3.3, the Shovel parameter parser converted attacker-controlled runtime parameter values to integers
CVE-2026-97504	In the Linux kernel, the following vulnerability has been resolved: watchdog: lenovo_se10_wdt: Fix use-after-free and resource leak risk Review by sashiko.dev high severity
CVE-2026-97503	In the Linux kernel, the following vulnerability has been resolved: genirq/proc: Size interrupt directory names for 10-digit interrupt numbers /proc/irq/<n>/ directory entries
CVE-2026-97502	In the Linux kernel, the following vulnerability has been resolved: mmc: davinci: avoid NULL deref of host->data in IRQ handler mmc_davinci_irq() returns early on NULL data
CVE-2026-97501	In the Linux kernel, the following vulnerability has been resolved: pinctrl: mediatek: paris: bypass pinctrl GPIO layer in set GPIO direction pinctrl_gpio_direction_input() .gpio_set_direction field in mtk_pmxops to signal we are no longer using the pinctrl GPIO layer for setting the direction.
CVE-2026-67408	RabbitMQ is a messaging and streaming broker. From 4.1.0 until 4.3.3, 4.2.9, and 4.1.11, Stream Management Super-Stream Binding Keys Allocation Allows Low-Priority Streams to be Evicted
CVE-2026-67407	RabbitMQ is a messaging and streaming broker. From 4.0.0 until 4.3.3 and 4.2.9 and 4.1.14 and 4.0.23, Incomplete fix for CVE-2026-44838: escaperegexchar/1 does not escape backslashes
CVE-2026-63006	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, attacker-controlled HTML in inbound emails or tickets could bypass the image alt text sanitization
CVE-2026-67227	RabbitMQ is a messaging and streaming broker. From 4.0.0 until 4.0.22 and 4.1.14 and 4.2.7 and 4.3.1, Atom exhaustion: toatom on global-parameter :name. resource is not limited
CVE-2026-49470	GLPI is a free asset and IT management software package. From 11.0.0 until 11.0.8, the time-based one-time password verification endpoint does not limit failed sign-in attempts
CVE-2026-53610	GLPI is a free asset and IT management software package. From 11.0.0 until 11.0.8, an attacker can craft a URL for a dashboard that reflects attacker-controlled metadata
CVE-2026-67237	RabbitMQ is a messaging and streaming broker. From 4.2.0 until 4.2.8 and 4.3.2, set_token_auth/2 inserted a bearer token from the Authorization header or access token
CVE-2026-53625	GLPI is a free asset and IT management software package. From 0.70 until 10.0.26 and 11.0.8, a technician can manipulate the authtype value through the API to cause a denial of service
CVE-2026-53626	GLPI is a free asset and IT management software package. From 11.0.5 until 11.0.8, under certain conditions, permission logic can grant access to a document with a non-existent file
CVE-2026-67234	RabbitMQ is a messaging and streaming broker. From 4.2.0 until 4.2.8 and 4.3.2, get_auth_mechanism/1 used term_to_binary/1 on the strict_auth_mechanism or password
CVE-2026-67230	RabbitMQ is a messaging and streaming broker. From 3.13.0 until 3.13.15, 4.0.20, 4.1.11, and 4.2.6, the Web STOMP WebSocket handler enforced neither max_frame_size nor max_frame_delivered
CVE-	

CVE-2026-53627	GLPI is a free asset and IT management software package. From 11.0.0 until 11.0.8, a low-privileged authenticated user can use the new API (v2) to perform updat
CVE-2026-67406	RabbitMQ is a messaging and streaming broker. From 4.0.0 until 4.3.3, 4.2.9, 4.1.14, and 4.0.23, Shovel does not format state logged by the crash reporter and can
CVE-2026-53628	GLPI is a free asset and IT management software package. From 0.84 until 10.0.26 and 11.0.8, an administrator holding the Update auth and sync or Update auth,
CVE-2026-67226	RabbitMQ is a messaging and streaming broker. From 4.0.0 until 4.0.22 and 4.1.14 and 4.2.7, Admin-only atom exhaustion: PUT /api/users tags list. settags/2 maps
CVE-2026-53629	GLPI is a free asset and IT management software package. From 9.4.0 until 10.0.26 and 11.0.8, an attacker with the READ right on logs can craft a URL for the histo
CVE-2026-55214	GLPI is a free asset and IT management software package. From 11.0.6 until 11.0.8, an authenticated technician can store active markup in supplier website fields
CVE-2026-67225	RabbitMQ is a messaging and streaming broker. From 3.13.0 until 3.13.15, 4.0.20, 4.1.11, and 4.2.6, the stream protocol stored the FrameMax value negotiated du
CVE-2026-55217	GLPI is a free asset and IT management software package. From 0.85 until 10.0.26 and 11.0.8, a low-privileged authenticated user can create, update, or delete kr
CVE-2026-61855	Zammad is a web based open source helpdesk/customer support system. In 7.0.3 and 7.1.1, under certain conditions, Zammad's verification of inbound PGP-signed
CVE-2026-49469	GLPI is a free asset and IT management software package. From 0.70 until 10.0.26 and 11.0.8, an authenticated hotliner or technician can submit crafted criteria tl
CVE-2026-48482	GLPI is a free asset and IT management software package. From 11.0.0 until 11.0.8, a form administrator can use Form import with a crafted illustration or scene ic
CVE-2026-47679	GLPI is a free asset and IT management software package. From 10.0.0 until 10.0.26 and 11.0.8, any logged-in GLPI user can exploit insufficient path validation in f
CVE-2026-45801	GLPI is a free asset and IT management software package. From 0.72 until 10.0.26 and 11.0.8, an authenticated user without the required permission can enable c
CVE-2026-93205	In the Linux kernel, the following vulnerability has been resolved: iommu/arm-smmu-v3: Manage teardown with devm arm_smmu_device_remove() manually frees
CVE-2026-67242	RabbitMQ is a messaging and streaming broker. From 4.2.0 until 4.2.9 and 4.3.3, OAuth2 isinteger(Exp) guard skips token-expiry checks for float exp. validateToken
CVE-2026-67241	RabbitMQ is a messaging and streaming broker. From 4.2.0 until 4.2.9 and 4.3.3, AMQP 1.0 management exchange.declare skips alternate-exchange permission cl
CVE-2026-97495	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Check bounds on allocate_doorbell allocated_doorbell has an option to set the doort
CVE-2026-97494	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: validate and share PSP fw_pri_buf copies via psp_copy_fw Change psp_copy_fw fron
CVE-2026-67239	RabbitMQ is a messaging and streaming broker. From 3.13.0 until 3.13.18 and 4.0.23 and 4.1.14 and 4.2.9 and 4.3.3, Stored XSS via TLS peer-certificate DN in stre
CVE-2026-93276	In the Linux kernel, the following vulnerability has been resolved: phy: renesas: phy-rcar-gen3-usb2: Fix devm action registration for disabled VBUS regulator devm
CVE-2026-97493	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Bound GPIO I2C table entry count from VBIOS Reject undersized tables and cap the
CVE-2026-93421	Mesop is a Python-based UI framework that allows users to build web applications. Prior to 1.3.4, the unauthenticated /__csp__ endpoint passes attacker-controlled
CVE-	

CVE-2026-97492	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: don't call ieee80211_handle_reconfig_failure when not needed In case reconfigur
CVE-2026-92730	LimeSurvey Community Edition 7.0.14 contains a reflected cross-site scripting vulnerability on the administrative survey-participant CSV import result page.
CVE-2026-97491	In the Linux kernel, the following vulnerability has been resolved: net/rds: Don't sleep inside rds_ib_conn_path_shutdown New rds rdma self tests exposed a hang w
CVE-2026-97490	In the Linux kernel, the following vulnerability has been resolved: affs: handle set_blocksize failures affs uses buffer_heads, which don't handle block size > PAGE_S
CVE-2026-93275	In the Linux kernel, the following vulnerability has been resolved: perf/x86/intel/pt: Fix stop/start with no update If pt_event_stop() is called without PERF_EF_UPDA1 perf_aux_output_end() are balanced. A cleared PERF_HES_UPTODATE bit indicates that an AUX output context is still open. Amend pt_event_start() / pt_event_stop()
CVE-2026-97489	In the Linux kernel, the following vulnerability has been resolved: bfs: handle set_blocksize failures bfs uses buffer_heads, which don't handle block size > PAGE_Sl
CVE-2026-93267	In the Linux kernel, the following vulnerability has been resolved: RDMA/core: Fix potential use after free in uverbs_free_dmah() When accessing a dmah via the ne management consistent and predictable.
CVE-2026-63132	OpenBao is an open source identity-based secrets management system. Prior to 2.6.0, OpenBao's handleLogicalRecovery path in http/logical.go compared the high
CVE-2026-97481	In the Linux kernel, the following vulnerability has been resolved: serial: 8250: fix possible ISR soft lockup There are rare cases in which the host gets stuck in the I
CVE-2026-93821	In the Linux kernel, the following vulnerability has been resolved: PCI: altera: Protect root bus removal with rescan lock Hold the pci_rescan_remove_lock lock while
CVE-2026-93819	In the Linux kernel, the following vulnerability has been resolved: PCI: mediatek: Protect root bus removal with rescan lock Hold the pci_rescan_remove_lock lock w
CVE-2026-93818	In the Linux kernel, the following vulnerability has been resolved: PCI: plda: Protect root bus removal with rescan lock Hold the pci_rescan_remove_lock lock while s
CVE-2026-93243	In the Linux kernel, the following vulnerability has been resolved: mm/secretmem: properly account locked pages secretmem accounts folios by treating memory a user_struct->locked_vm. Since the scope tracked is actually inode lifetime, the RLIMIT_MEMLOCK applies per-user not per-process, so it doesn't make sense to byp
CVE-2026-5696	Reflected Cross-Site Scripting (XSS) in Microweber. The vulnerability lies in the 'group' parameter of the '/admin/settings' endpoint in the administration panel. A st
CVE-2026-93244	In the Linux kernel, the following vulnerability has been resolved: drm/sysfb: simpledrm: Improve stride validation Validate the computed stride against the maxim
CVE-2026-5695	Arbitrary file upload vulnerability due to a lack of proper validation in upload forms. This allows authenticated users to upload files to the server without restrictions
CVE-2026-93815	In the Linux kernel, the following vulnerability has been resolved: net: au1000: move free_irq out of the close-time spinlocked section au1000_close() calls free_irq()
CVE-2026-93273	In the Linux kernel, the following vulnerability has been resolved: regulator: tps6594: Fix device node reference leaks in multiphase loop In tps6594_regulator_prob
CVE-2026-93814	In the Linux kernel, the following vulnerability has been resolved: spi: core: Abort active target transfer on controller suspend When an SPI controller operating in tr
CVE-2026-93245	In the Linux kernel, the following vulnerability has been resolved: apparmor: policy_int make sure list heads are initialized before fail path If profile create fails befo ffff88803f734800 RCX: ffff88801af2a580 RDX: 0000000000000000 RSI: ffffffff8e38eba4 RDI: ffffffff90634320 RBP: 0000000000000000 R08: 00000000000000cc0 R arch/x86/entry/syscall_64.c:61 [inline] do_syscall_64+0x166/0x520 arch/x86/entry/syscall_64.c:84 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f5f6
CVE-2026-93812	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix sd_ndr.data memory leak in ksmbd_vfs_set_sd_xattr ndr_encode_v4_ntacl() allocates s
CVE-2026-93811	In the Linux kernel, the following vulnerability has been resolved: ksmbd: Fix acl.sd_buf memory leak and invalid sd_size error handling 1. When ndr_decode_v4_nt
CVE-	

2026-93246	In the Linux kernel, the following vulnerability has been resolved: octeontx2-af: fix out-of-bounds read setting MSI-X irq affinity rvu_register_interrupts() walks even
CVE-2026-93809	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: flush pending RCU callbacks on module unload Call rcu_barrier() in module exit to v CR3: 00000104a980a001 CR4: 0000000002770ee0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6:
CVE-2026-93808	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: caiaq: validate EP1 reply lengths usb_ep1_command_reply_dispatch() uses buff
CVE-2026-93807	In the Linux kernel, the following vulnerability has been resolved: wifi: rsi: avoid reading TKIP MIC keys for non-TKIP ciphers rsi_hal_load_key() copies tx_mic_key an
CVE-2026-79616	Out-of-bounds read while parsing untrusted SVG path strings in Qt Quick's Context2D.path / PathSvg.path.
CVE-2026-93247	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: mgmt: fix 'hdev->discovery.uuids' NULL dereference 'uuid_count' member of struct 'di assign uuid_count value only after success kmemdup() allocation in start_service_discovery(), otherwise uuids is NULL, because kmemdup failed, but uuid_count is end trace 0000000000000000]--
CVE-2026-93805	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: validate rx/tx MLME callback frame lengths before access cfg80211_rx_mlme_mgr subtype's minimum frame size in an if/else-if chain that mirrors the dispatch logic. Trace only after the frame is known to be well-formed. Side effects of this chang
CVE-2026-93820	In the Linux kernel, the following vulnerability has been resolved: PCI: rockchip: Protect root bus removal with rescan lock Hold the pci_rescan_remove_lock lock wh
CVE-2026-93822	In the Linux kernel, the following vulnerability has been resolved: PCI: iproc: Protect root bus removal with rescan lock Hold the pci_rescan_remove_lock lock while
CVE-2026-93804	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: ibss: wait for in-flight TX on disconnect While leaving an IBSS in ieee80211_ibss_
CVE-2026-93823	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Let driver decide buffer size at AMDKFD_IOC_GET_DMABUF_INFO ioctl amdkgd driver
CVE-2026-93233	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau/dmem: fix allocated underflow on large folio split nouveau_dmem_folio_free() drop
CVE-2026-96559	Rejected reason: This ID was for testing
CVE-2026-93234	In the Linux kernel, the following vulnerability has been resolved: drm/gud: validate TV mode names before creating enum property The GUD protocol returns TV n
CVE-2026-12974	A Security Policy Bypass vulnerability exists in Forcepoint Security Engine (NGFW). This issue affects Forcepoint Security Engine (NGFW): from 7.1.0 through 7.1.13
CVE-2026-93235	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to zero post-EOF data when extending file size generic/794 4s ... - output mismatch (see , [4080,4096) 7. sync range 4096 from offset 4096; shutdown -f (flush meta before shutdown) 8. umount; mount; verify [4080,4096) is zeroed or not. When extendin
CVE-2026-93236	In the Linux kernel, the following vulnerability has been resolved: media: meson: vdec: fix NULL pointer deref in vdec_try_fmt_common When VIDIOC_TRY_FMT is ca
CVE-2026-98163	In the Linux kernel, the following vulnerability has been resolved: cgroup: Avoid iteration of dying tasks with zero refcount The commit 260fbc92bbea ("cgroup: M task on the dying list because that won't distinguish regular zombies waiting to be reaped from RCU remnant tasks that are going to be free'd. Therefore add an ex another iteration take css_set_lock it->task_pos = &L->cg_list get_task_struct(L) => addition on 0 drop css_set_lock cgroup_task_free(L) css_set_skip_task_iters() /
CVE-2026-95676	A missing/improper authentication vulnerability in the WatchGuard AuthPoint Gateway's LDAP Sync first-factor authentication allows a remote attacker to bypass s
CVE-2026-93238	In the Linux kernel, the following vulnerability has been resolved: s390/vfio-ap: fix potential use of uninitialized apm_filtered bitmap The DECLARE_BITMAP(apm_filt
CVE-2026-94604	Rejected reason: This CVE is a duplicate of another CVE.
CVE-2026-93239	In the Linux kernel, the following vulnerability has been resolved: arm64: mm: Fix the lockless page-table walk in show_pte() show_pte() walks page tables lockless
CVE-	

CVE-2026-93240	In the Linux kernel, the following vulnerability has been resolved: memcg: make the v1 soft limit knob inert The v1 soft limit has been deprecated since v6.12 and is no longer used by the kernel.
CVE-2026-93829	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix races in cifs thread creation The cifs demultiplex thread can run and access tcp connections before it is fully initialized, leading to a race condition where the thread may attempt to access a connection that has not yet been established.
CVE-2026-93828	In the Linux kernel, the following vulnerability has been resolved: exfat: fix handling of damaged volume in exfat_create_upcase_table() When the size of the upcase table is not a multiple of the page size, the kernel may attempt to access memory outside the allocated buffer, leading to a potential crash or data corruption.
CVE-2026-93241	In the Linux kernel, the following vulnerability has been resolved: memcg: bypass the reclaim and oom killer for dying tasks once oom_reaper is done At Meta, we noticed that the kernel's memory cgroup (memcg) reclaim and out-of-memory (OOM) killer were not properly handling tasks that had reached the OOM state but were still running. This could lead to memory leaks and system instability.
CVE-2026-78253	Uncontrolled recursion in QDomStreamReader::readElementText() in Qt Group Qt allows attackers to cause a denial of service (application crash via stack exhaustion) by sending a crafted XML stream.
CVE-2026-93242	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Fix response queue over-consumption in __qla_consume_iocb() qla2xxx_process_response() can consume more response queue entries than are available, leading to a denial of service.
CVE-2026-93825	In the Linux kernel, the following vulnerability has been resolved: spi: Add NULL check for spi_get_device_id() in spi_get_device_match_data() Prevent NULL pointer dereference in spi_get_device_match_data() by adding a NULL check for spi_get_device_id().
CVE-2026-93824	In the Linux kernel, the following vulnerability has been resolved: tls: reject the combination of TLS and sockmap TLS and sockmap (BPF psock) integration hides a race condition where a TLS session may be established before the sockmap is fully initialized.
CVE-2026-92378	A session management vulnerability exists in the Legacy UI Reduced Function Login feature of NT-ware uniFLOW Online. Under specific timing conditions during Session Setup, an attacker could potentially manipulate the session state.
CVE-2026-93803	In the Linux kernel, the following vulnerability has been resolved: wifi: libipw: fix key index receive bound checks libipw_rx() reads skb->data[hdrlen + 3] to extract the key index, but the bound check was incorrect, allowing access to memory outside the expected range.
CVE-2026-97407	In the Linux kernel, the following vulnerability has been resolved: ASoC: rockchip: rockchip_pdm: Handle runtime PM resume failures in set_fmt rockchip_pdm_set_fmt() can fail to handle runtime PM resume failures, leading to a denial of service.
CVE-2026-93254	In the Linux kernel, the following vulnerability has been resolved: arm64: entry: Avoid unnecessary local_irq_disable() on kernel exit Currently, when exiting to kernel mode, the kernel disables local interrupts unnecessarily, which can lead to performance issues.
CVE-2026-93270	In the Linux kernel, the following vulnerability has been resolved: bpf: Disallow interpreter fallback for BPF_ADDR_PERCPU insn The BPF_MOV64_PERCPU_REG insn can be misinterpreted by the BPF interpreter, leading to incorrect behavior.
CVE-2026-93788	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: acpi: validate WGDS table revision index Check tbl_rev bounds before BIT(tbl_rev) to ensure the correct revision index is used for the WGDS table.
CVE-2026-93255	In the Linux kernel, the following vulnerability has been resolved: btrfs: make sure EXTENT_BUFFER_READING is cleared under refs_lock [FALSE ALERTS] There is a race condition where the EXTENT_BUFFER_READING flag is not properly cleared, leading to incorrect buffer management.
CVE-2026-93256	In the Linux kernel, the following vulnerability has been resolved: arm64: hibernate: mask DAIF before restoring hibernated kernel The arm64 hibernate code may not properly mask the DAIF (Data Abort Interrupt Flag) before restoring the hibernated kernel, leading to unexpected behavior.
CVE-2026-93785	In the Linux kernel, the following vulnerability has been resolved: cifs: validate idmap key payload length The cifs.idmap key type stores its payload length in key->value, but the validation was incorrect, allowing for oversized payloads.
CVE-2026-93784	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: validate IEs in cfg80211_wext_siwgenie() The KASAN allocation trace shows that a buffer overflow occurs when validating IEs in cfg80211_wext_siwgenie().
CVE-2026-93783	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: RFCOMM: validate skb length in rfcomm_recv_frame rfcomm_recv_frame() casts skb->len to unsigned short, which can lead to a buffer overflow if the length is too large.
CVE-2026-93257	In the Linux kernel, the following vulnerability has been resolved: block: handle nogenerate/noverify properly in fs-integrity Check the BIP_CHECK flags before generating integrity checksums to ensure proper handling of data integrity.
CVE-2026-93781	In the Linux kernel, the following vulnerability has been resolved: scsi: core: Do not block on tag allocation in scsi_eh_lock_door() scsi_eh_lock_door() is called from USB storage) it is a guaranteed deadlock and I/O that can never be submitted. This problem has also been reproduced in our environment. Locking the door is a bad idea.
CVE-2026-93258	In the Linux kernel, the following vulnerability has been resolved: ocfs2: do not use make_bad_inode() in ocfs2_read_inode_block_full() This reverts commit 58b6fcc which introduced a bug in ocfs2's inode management.
CVE-	

CVE-2026-93259	In the Linux kernel, the following vulnerability has been resolved: powerpc/irq: Fix missing r2 clobber in PCREL inline assembly In CONFIG_PPC_KERNEL_PCREL mod 10 06 pla r31,53297316 ... 3d e8 ff 4b bl c0000000000165ac <__do_irq> 00 00 21 e8 ld r1,0(r1) 28 00 4d e9 ld r10,40(r13) 40 00 21 38 addi r1,r1,64 2a f9 aa 7f st r1,r10,40(r13) 40 00 21 38 addi r1,r1,64 2a f9 aa 7f st r1,r10,40(r13)
CVE-2026-93261	In the Linux kernel, the following vulnerability has been resolved: locking/lockdep: Fix NULL pointer dereference in __lock_set_class() register_lock_class() can retur
CVE-2026-93263	In the Linux kernel, the following vulnerability has been resolved: clk: eswin: Zero-initialize stack-allocated clk_init_data eswin_clk_register_pll() and eswin_register_ happens to contain when the registration helpers run. Zero-initialize both structures.
CVE-2026-93269	In the Linux kernel, the following vulnerability has been resolved: ext4: fix circular lock dependency in ext4_ext_migrate Move iput(tmp_inode) after ext4_writpage
CVE-2026-93264	In the Linux kernel, the following vulnerability has been resolved: RDMA/efa: Fix PBL chunk length computation On register MR, when creating the PBL, if it's an ind
CVE-2026-93266	In the Linux kernel, the following vulnerability has been resolved: arm64: RSI: fix field-spanning write warning in attestation token init The challenge is passed in re
CVE-2026-93286	In the Linux kernel, the following vulnerability has been resolved: net: appletalk: fix NULL pointer dereference in aarp_send_ddp() aarp_send_ddp() calls atalk_find_
CVE-2026-93268	In the Linux kernel, the following vulnerability has been resolved: ext4: skip extra isize expansion during mount to prevent deadlock ext4_try_to_expand_extra_isiz
CVE-2026-93285	In the Linux kernel, the following vulnerability has been resolved: f2fs: embed f2fs_gc_kthread in f2fs_sb_info Instead of allocating f2fs_gc_kthread dynamically, em
CVE-2026-93789	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: bound aligned TLV advance in FW parser Validate ALIGN(tlv_len, 4) against remaining
CVE-2026-93791	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: add a check on the tid coming from the firmware ba_notif->tid is a firmware-co
CVE-2026-93802	In the Linux kernel, the following vulnerability has been resolved: wifi: rsi: validate beacon length before fixed buffer copy rsi_prepare_beacon() copies the mac802
CVE-2026-93792	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: fix a possible underflow We shouldn't trust the firmware about the length of th
CVE-2026-93248	In the Linux kernel, the following vulnerability has been resolved: drm/xe: don't WARN on kernel job timeout when device already wedged igt@xe_wedged@wedge
CVE-2026-93800	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix use-after-free on reloc root after error in insert_dirty_subvol() If during relocation we fail >reloc_root field to NULL, but root X is not in the dirty_subvol_roots list, so its ->reloc_root still points to a reloc root; 5) Relocation finishes, with an error and a trar T1061] BTRFS: error (device loop0 state A) in cleanup_transaction:2067: errno=-5 IO failure [106.044382][T5339] BTRFS info (device loop0 state EA): forced read T5338] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [106.694300][T5338] Call Trace: [106.694308][T5338]
CVE-2026-93249	In the Linux kernel, the following vulnerability has been resolved: spi: amlogic-spisg: Make sure clk_init_data is fully initialized The clk_init_data structure contains s
CVE-2026-88383	libical 4.0.6 contains an incompatible function pointer in icalparameter_string_to_kind(). When parsing iCalendar data containing a parameterized property, the fun
CVE-2026-93251	In the Linux kernel, the following vulnerability has been resolved: ACPI: bus: Introduce acpi_bus_get_primary_device() The function used for obtaining the first "phy functional impact.
CVE-2026-88385	Mini-XML 4.0.5 contains a memory leak vulnerability in mxml_load_data() during malformed XML parsing. Specially crafted XML input can cause text nodes allocate
CVE-2026-93797	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: fix an off-by-1 boundary check Before looking at the 11th byte, check the lengt
CVE-2026-93252	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix circular locking dependency in ocfs2_init_acl() A lockdep warning indicates a circular loc waiting for Path 1 to release `ip_xattr_sem`. The patch fixes the lock ordering by precomputing the ACL state before starting the OCFS2 transaction, while preservi
CVE-2026-93272	In the Linux kernel, the following vulnerability has been resolved: remoteproc: qcom_wcnss: Fix handling the lack of PD regulators in v3 The changes introduced to

CVE-2026-50228	An unauthenticated local attacker can connect to the Electron DevTools endpoint exposed by Acer NitroSense software (versions up to and including 5.2.63) on loc
CVE-2026-100655	Rejected reason: This CVE ID has been rejected as a duplicate.
CVE-2026-100656	Rejected reason: This CVE ID has been rejected as a duplicate.
CVE-2026-100657	Rejected reason: This CVE ID has been rejected as a duplicate.
CVE-2026-100658	Rejected reason: This CVE ID has been rejected as a duplicate.
CVE-2026-50227	An unauthenticated local attacker can connect to the MQTT broker over its localhost WebSocket endpoint in Acer NitroSense software (versions up to and including
CVE-2026-93795	In the Linux kernel, the following vulnerability has been resolved: blk-cgroup: fix leaks and online flag on radix_tree_insert failure When radix_tree_insert() fails in b
CVE-2026-93794	In the Linux kernel, the following vulnerability has been resolved: smb/client: flush dirty data before punching a hole Punching a hole after a large buffered write m
CVE-2026-93253	In the Linux kernel, the following vulnerability has been resolved: sched/isolation: Defer freeing of cpumask memblock memory to initcall When testing a linux-next memory to when initcall's are being processed. The cpumask memblock memory is treated as a llist_node with the size of a "long" type which is also smallest cpun
CVE-2026-93271	In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: cap out-of-range rx MCS instead of leaving bogus rate ath11k can receive HT/VHT/HI value, so a frame with an out-of-range MCS no longer leaves partial or bogus rate metadata behind. Also downgrade the logging level since they are not treated as
CVE-2026-93232	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: fix boot panic with CONFIG_DEBUG_VM and HVO bootmem pages Patch series "mm: bugs - patches [5-12] reorder and simplify sparse/mm/hugetlb early init - patches [13-19] refactor bootmem gigantic hugepage allocation and remove obsolete hel
CVE-2026-97408	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: validate connectionless PSM length Connectionless L2CAP frames carry a two-b
CVE-2026-45234	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-57449	Actual is a local-first personal finance tool. Prior to 26.7.0, Actual Sync Server's CORS proxy is intended to let authenticated users fetch resources only from reposit
CVE-2026-93206	In the Linux kernel, the following vulnerability has been resolved: PCI/proc: Use file_ns_capable() when checking config space read access proc_bus_pci_read() deci against different credentials. Checking the credentials of the task calling read() makes the outcome depend on who reads rather than who opened, so the restricti
CVE-2026-94132	Joomla Extension - acymailing.com - Remote Code Execution vulnerability in mailbox action feature in AcyMailing Enterprise extension < 11.1.0 - MIME parts of inc
CVE-2026-63131	OpenBao is an open source identity-based secrets management system. Prior to 2.6.0, OpenBao's vault/policy/acl.go could evaluate a broader wildcard ACL grant t
CVE-2026-97477	In the Linux kernel, the following vulnerability has been resolved: RDMA/counter: Fix num_counters leak on bind_qp failure in alloc_and_bind() When __rdma_counte
CVE-2026-97476	In the Linux kernel, the following vulnerability has been resolved: rds: filter RDS_INFO_* getsockopt by caller's netns The RDS_INFO_* family of getsockopt(2) optio numbers of every RDS connection on the host. The rds-tcp transport is reachable from a non-initial netns (see rds_set_transport()), so a one-shot init_net gate at rd and decrements in rds_create()/rds_destroy_sock() and rds_tcp_set_callbacks()/rds_tcp_restore_callbacks() go away with them. Reported by the kernel test robot ur
CVE-2026-97475	In the Linux kernel, the following vulnerability has been resolved: thermal/drivers/tegra/soctherma: Switch to devm cooling device registration Use devm_thermal_(c
CVE-2026-93208	In the Linux kernel, the following vulnerability has been resolved: kasan: fix cache shrink race with CPU hotplug kasan_quarantine_remove_cache() first invokes per was observed with a virtio-9p filesystem. The mount and umount commands both returned 0, but the kernel logged the following during the userspace-triggered te WARNING: mm/slub.c:1244 at __kmem_cache_shutdown+0x363/0x500, CPU#0: busybox/111 [2994.405655][T111] Call Trace: [2994.406325][T111] kmem_cach normally empty; a non-empty list is traversed to remove objects belonging to the cache being shrunk or destroyed.
CVE-2026-97473	In the Linux kernel, the following vulnerability has been resolved: powercap: intel_rapl: Fix memory leak in rapl_add_package_cpuslocked() When topology_physica

CVE-2026-97472	In the Linux kernel, the following vulnerability has been resolved: ipv6: addrconf: fix temp address generation after prefix deprecation When a router temporarily d
CVE-2026-97456	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Fix condition check in acpi_ps_parse_loop() Fix condition check for AML_ELSE_OP in acpi_
CVE-2026-93209	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_core: use skb_get() instead of skb_clone() for req_skb BT enable fails intermittently hci_req_cmd_complete() can locate the registered completion callback. Under memory pressure this skb_clone() fails, leaving hdev->req_skb NULL. The firmware n
CVE-2026-55456	Rejected reason: This CVE is a duplicate of another CVE.
CVE-2026-52744	GoCD is a continuous deliver server. From 20.2.0 until 26.1.0, the internal GoCD UI fetch-artifact auto-suggestion API at /go/api/internal/pipelines/**/upstream does
CVE-2026-93210	In the Linux kernel, the following vulnerability has been resolved: smb: client: harden DFS cache against invalid target hints Currently, get_tgt_name() returns ERR_
CVE-2026-91775	LimeSurvey fails to safely encode attacker-controlled content from a crafted .lss survey file when displaying import warnings, resulting in XSS in the administrative
CVE-2026-97453	In the Linux kernel, the following vulnerability has been resolved: ACPICA: validate byte_count in acpi_ps_get_next_package_length() Validate package length readi
CVE-2026-93211	In the Linux kernel, the following vulnerability has been resolved: nfsd: initialize DRC hash table before registering shrinker shrinker_register() precedes the INIT_LL
CVE-2026-93212	In the Linux kernel, the following vulnerability has been resolved: nfsd: guard nfsd_serv deref in nfsd_file_net_dispose nfsd_file_net_dispose() is the consumer side o nfsd_file_dispose_list_delayed().
CVE-2026-93213	In the Linux kernel, the following vulnerability has been resolved: of: fix out-of-bounds read in of_alias_scan() stem parser The stem parser tests isdigit(*(end - 1)) b
CVE-2026-86066	Horilla is an HR and CRM software. Prior to 2.0.0, approve_validate_attendance_request at /attendance/approve-validate-attendance-request/ changes attendance_
CVE-2026-9655	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-18944	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-18944. Reason: This candidate is a reservation duplicate of CVE-2026
CVE-2026-9652	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-45235	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-45236	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-45237	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-45238	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-45239	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-45240	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-45241	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-	

CVE-2026-49117	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-49118	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-53971	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-53972	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-53973	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-97160	Joomla Extension - lomart.fr - Authenticated, privileged PHP command injection in UP plugin extension 5.0.0-5.2.0, 6.0.0-6.0.29
CVE-2026-71483	Horilla is an HR and CRM software. Prior to 1.6.0, the search parameter at /employee/employee-filter-view is reflected by jQuery .html() in employee/templates/em
CVE-2026-7799	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-7800	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-88003	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. Prior to 1.7.2, InvoicePlane fails to revoke administrative privile
CVE-2026-97480	In the Linux kernel, the following vulnerability has been resolved: tty: serial: 8250: protect against NULL uart->port.dev in register serial8250_register_8250_port()
CVE-2026-97479	In the Linux kernel, the following vulnerability has been resolved: driver core: Avoid warning when removing a device while its supplier is unbinding During driver r (consumer ---> supplier): i2c -----> OIC ----> PCI device ^ +----> pinctrl ---+ When the PCI device is removed, the OIC (interrupt controller) has to be remove device_links_busy(i2c): links->status = DL_DEV_UNBINDING __device_links_no_driver(i2c)... pinctrl--i2c link->status is DL_STATE_SUPPLIER_UNBIND oic--i2c link->st
CVE-2026-97449	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Add package limit checks in parser functions Add package limit checks in parser functio
CVE-2026-93214	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_tcm: fix deadlock in usbg_make_tpg() usbg_make_tpg() held dep_lock while calling
CVE-2026-93231	In the Linux kernel, the following vulnerability has been resolved: lockd: fix swapped arguments in nlmsvc_match_ip() When releasing locks by server IP address via sockaddr as a struct nlm_host and reads garbage at the offset of h_srcaddr; meanwhile @datap is actually the lock owner's nlm_host but is compared as a sockadd
CVE-2026-93223	In the Linux kernel, the following vulnerability has been resolved: staging: media: tegra-video: fix of_node_put() on VIP parse errors tegra_vip_channel_of_parse() ir
CVE-2026-97426	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/pm: fix SmartShift bias sysfs store PM refcount on parse error Return the parse erro
CVE-2026-97425	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix buffer overflow during vBIOS update Clamp the buffer postion to write by setting
CVE-2026-97424	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/ras: add ras_suspend callback and use it for cp_ecc_error_irq cp_ecc_error_irq is acc
CVE-2026-97423	In the Linux kernel, the following vulnerability has been resolved: cxl/region: Validate partition index before array access construct_region() reads cxled->part and
CVE-2026-97422	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: fix SMI event cross-process information leak kfd_smi_ev_enabled() skips the suser p
CVE-2026-96609	Robur Albatross 1.0.0 through 2.x before 2.7.2 does not limit use of the ring buffer, leading to an albatross-console loop with no recognized termination condition. "
CVE-	In the Linux kernel, the following vulnerability has been resolved: ipv6: use RCU iterator to dump route exceptions rt6_nh_dump_exceptions() uses hlist_for_each_e

CVE-2026-93226	fib6_dump_node+0x6d/0xf0 fib6_walk_continue+0x290/0x2d0 fib6_dump_table+0x28d/0x360 inet6_dump_fib+0x37d/0x620 rtnl_dumpit+0x7b/0xd0 netlink_dump
CVE-2026-97420	In the Linux kernel, the following vulnerability has been resolved: bpf: NUL-terminate replaced sysctl value When writing to sysctls, proc_sys_call_handler() guarant out-of-bounds in strnchrnul+0x72/0x90 Read of size 1 at addr ffff88800de57000 by task repro_patch3/66 CPU: 0 UID: 0 PID: 66 Comm: repro_patch3 Not tainted 7.
CVE-2026-97419	In the Linux kernel, the following vulnerability has been resolved: hsr: broadcast netlink notifications in the device's net namespace The HSR generic netlink family from the master port via hsr_port_get_hsr()).
CVE-2026-94130	Joomla Extension - joomlaboat.com - Unauthenticated SQL injection in YouTube Gallery extension < 5.7.3 - An SQL injection vulnerability in video search functional
CVE-2026-97418	In the Linux kernel, the following vulnerability has been resolved: ALSA: es18xx: check control allocation before private data setup snd_es18xx_mixer() creates con
CVE-2026-93227	In the Linux kernel, the following vulnerability has been resolved: mm/mm_init: deferred_grow_zone(): fix out-of-range first_deferred_pfn With CONFIG_DEFERRED_! CONFIG_DEFERRED_STRUCT_PAGE_INIT=y and CONFIG_CMA=y using the following qemu command line qemu-system-x86_64 -enable-kvm -m 8032M -kernel bzlm
CVE-2026-97416	In the Linux kernel, the following vulnerability has been resolved: btrfs: balance: fix potential bg lookup failure in btrfs_may_alloc_data_chunk() [BUG] Running btrfs missing, so no block group is ever inserted into the cache. In that case btrfs_lookup_block_group() returns NULL. The code only guards this with ASSERT(cache), wh
CVE-2026-92419	WEBCON BPS is vulnerable to Insecure Direct Object Reference (IDOR) in the /api/vacations/{path} endpoint. The selectedPeople parameter in the Gantt vacation c
CVE-2026-93230	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: initialize gigantic bootmem hugepage struct pages earlier Gigantic bootmem HugeT
CVE-2026-97414	In the Linux kernel, the following vulnerability has been resolved: ASoC: mediatek: mt8365-afe-pcm: fix possible NULL-pointer dereferences in mt8365_afe_suspend
CVE-2026-97412	In the Linux kernel, the following vulnerability has been resolved: pds_core: quiesce DMA before freeing resources pdsc_teardown() frees DMA buffers but does not
CVE-2026-97411	In the Linux kernel, the following vulnerability has been resolved: net: ibm: emac: mal: fix potential system hang in mal_remove() napi_disable() is not idempotent
CVE-2026-97410	In the Linux kernel, the following vulnerability has been resolved: netconsole: take target_cleanup_list_lock in drop_netconsole_target() drop_netconsole_target() u
CVE-2026-97427	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: bound pp_dpm_set_pp_table() memcpyy The powerplay path allocates hardcoded_pp.
CVE-2026-93222	In the Linux kernel, the following vulnerability has been resolved: signal: avoid shared siginfo namespace rewrites send_signal_locked() rewrites sender ids for the
CVE-2026-97447	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Enhance OEM ID and Table ID validation in acpi_ex_load_table_op() Enhance OEM ID and
CVE-2026-97430	In the Linux kernel, the following vulnerability has been resolved: xhci: Prevent queuing new commands if xhci is inaccessible Refuse to queue a new command on
CVE-2026-97446	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Fix NULL pointer dereference in acpi_ns_custom_package() acpi_ns_custom_package() u
CVE-2026-93215	In the Linux kernel, the following vulnerability has been resolved: cdx: Fix double free when sysfs file creation fails In cdx_create_res_attr(), if sysfs_create_bin_file(
CVE-2026-93216	In the Linux kernel, the following vulnerability has been resolved: mm/page_owner: use memcg_data snapshot to avoid TOCTOU in print_page_owner_memcg() pri
CVE-2026-97443	In the Linux kernel, the following vulnerability has been resolved: perf/trace: Fix WARNING in __unregister_ftrace_function perf_ftrace_function_unregister() unconc
CVE-2026-97516	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw88: Add NULL check for chip->edcca_th in rtw_fw_adaptivity_result() It was recently repor
CVE-	In the Linux kernel, the following vulnerability has been resolved: mm/madvise: skip device-private PMDs in cold and pageout walks madvise_cold_or_pageout_pte_

CVE-2026-93217	PMD to a device-private entry before the PMD lock is acquired.
CVE-2026-97441	In the Linux kernel, the following vulnerability has been resolved: ata: ahci: fail probe if BAR too small for claimed ports When an AHCI controller is disabled in BIOS
CVE-2026-94131	Joomla Extension - acymailing.com - Unauthenticated arbitrary file deletion in AcyMailing Enterprise extension < 11.1.0 - A subscriber could store a path in a file-ty
CVE-2026-97440	In the Linux kernel, the following vulnerability has been resolved: net: qrtr: fix node refcount leak on ctrl packet alloc failure qrtr_send_resume_tx() calls qrtr_node_
CVE-2026-97439	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: preserve non-DOS attribute bits in system.dos_attr [BUG] A corrupted ntfs3 image can system.ntfs_attr updates ATTR_DATA flags via ni_new_attr_flags() and switches i_mapping->a_ops to ntfs_aops_cmpr when FILE_ATTRIBUTE_COMPRESSED is set.
CVE-2026-93218	In the Linux kernel, the following vulnerability has been resolved: mm/huge_memory: skip device-private PMDs in madvise_free_huge_pmd madvise_free_pte_rangi callee's pmd_trans_huge_lock().
CVE-2026-93219	In the Linux kernel, the following vulnerability has been resolved: clocksource/drivers/timer-sun4i: Advertise a real minimum delta sun4i_clkevt_next_event() comp
CVE-2026-97436	In the Linux kernel, the following vulnerability has been resolved: dpaa2-switch: rework FDB management on the bridge leave path On bridge leave, the dpaa2_swi
CVE-2026-97435	In the Linux kernel, the following vulnerability has been resolved: net: dsa: sja1105: flower: reject cross-chip redirect dsa_port_from_netdev() may return a valid po
CVE-2026-93769	HumHub 1.18.5 is affected by a stored cross-site scripting (XSS) vulnerability that allows any user holding the delegated, non-system-administrator Manage Users
CVE-2026-97434	In the Linux kernel, the following vulnerability has been resolved: dpaa2-switch: fix handling of NAPI on the remove path All the NAPI instances for a DPSW device a
CVE-2026-93220	In the Linux kernel, the following vulnerability has been resolved: sched_ext: Keep kick_sync waiting on the rq's own CPU kick_sync_wait_bal_cb() assumes it runs c
CVE-2026-97432	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: fix P2P-Device binding handling Our binding handling for P2P-Device can run in binding when that isn't active.
CVE-2026-97431	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Avoid DPMS-on for phantom stream [Why & How] Calling dc_update_planes_and
CVE-2026-97515	In the Linux kernel, the following vulnerability has been resolved: i3c: master: svc: Prevent IRQ storm from false SLVSTART on NPCM845 On NPCM845, when a targ
CVE-2026-4637	Paessler PRTG Network Monitor before version 26.2.120.1449 is affected by a reflected Cross-Site Scripting (XSS) vulnerability. When a request is made for a non-e
CVE-2026-67236	RabbitMQ is a messaging and streaming broker. From 4.2.0 until 4.2.8 and 4.3.2, a successful POST /login caused is_authorized/2 to set an auth cookie containing l
CVE-2026-97904	In the Linux kernel, the following vulnerability has been resolved: cpufreq: initialize policy rwsem before sysfs publication cpufreq_policy_alloc() initializes policy->r
CVE-2026-97906	In the Linux kernel, the following vulnerability has been resolved: bootconfig: Fix integer overflow in initrd size check Sashiko reported that in get_boot_config_from
CVE-2026-97907	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btrtl: Don't leak return code when parsing firmware format v2 When key_id from chip i
CVE-2026-97908	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btqcomsmd: destroy RPMsg endpoints before freeing hci_dev The command and ACL f cleanup path, return directly after freeing the hci_dev to avoid falling through to the partial-construction labels and destroying the endpoints twice.
CVE-2026-97909	In the Linux kernel, the following vulnerability has been resolved: ASoC: sti: initialize IRQ lock before requesting IRQ uni_reader_init() registers the shared IRQ befor
CVE-2026-	RabbitMQ is a messaging and streaming broker. Prior to versions 4.2.7 and 4.3.1, The runtime-parameters lookup path coerces the URL :component segment to an

67228	
CVE-2026-67224	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.1, The trace consumer constructs the output path as filename
CVE-2026-97912	In the Linux kernel, the following vulnerability has been resolved: accel: ethosu: Ensure SRAM size is 0 on mapping failure On a mapping failure of the SRAM, the SI
CVE-2026-97913	In the Linux kernel, the following vulnerability has been resolved: accel: ethosu: Ensure cmd stream ends with a stop op While the QSIZE register setting should pre
CVE-2026-97914	In the Linux kernel, the following vulnerability has been resolved: accel: ethosu: Fix ethosu_job_open() return value A WARN_ON() returns a 0 or 1, not the original i
CVE-2026-97915	In the Linux kernel, the following vulnerability has been resolved: accel/ivpu: Limit firmware log name prints to field size The name in struct vpu_tracing_buffer_he
CVE-2026-97916	In the Linux kernel, the following vulnerability has been resolved: accel/ivpu: Validate firmware log buffer metadata The tracing log headers parsed by fw_log_print
CVE-2026-97917	In the Linux kernel, the following vulnerability has been resolved: accel/ivpu: Validate full buffer range in ivpu_to_cpu_addr Add a size parameter to ivpu_to_cpu_ad
CVE-2026-97918	In the Linux kernel, the following vulnerability has been resolved: tracing: Undo the registration when enabling the histogram trigger fails Commit 6f86bdeab633 ("hist_register_trigger+0xc1/0xa00 event_hist_trigger_parse+0x3146/0x6af0 event_trigger_write+0xce/0x160 Freed by task 69: kfree+0x154/0x420 trigger_kthread
CVE-2026-97919	In the Linux kernel, the following vulnerability has been resolved: tracing: Take the reference before publishing the named histogram trigger event_hist_trigger_nai which can fail runs after the trigger becomes findable.
CVE-2026-97920	In the Linux kernel, the following vulnerability has been resolved: tracing: Keep the entry count when the histogram stats allocation fails print_entries() uses n_entries vfs_read+0x176/0xa40 The buggy address belongs to a 4-page vmalloc region starting at ffff90000041000 allocated at tracing_map_sort_entries+0x5c/0xd50 A f
CVE-2026-97921	In the Linux kernel, the following vulnerability has been resolved: tracing: Free histogram the field rejected for a bad modifier Writing a hist trigger whose value or into a value case and a variable case replaced that fall-through with a goto that skips it. With CONFIG_DEBUG_KMEMLEAK, 200 writes of # echo 'hist:keys=prev_pic
CVE-2026-97922	In the Linux kernel, the following vulnerability has been resolved: tracing: Free histogram var refs regardless of how often they are referenced Using the same variable single trigger, so nothing outside it holds the object. Removing a trigger whose variables are still referenced is already refused by check_var_refs() with -EBUSY. Dr
CVE-2026-97923	In the Linux kernel, the following vulnerability has been resolved: tracing: Free histogram the var ref when its initialization fails create_var_ref() allocates a VAR_RE
CVE-2026-97924	In the Linux kernel, the following vulnerability has been resolved: tracing/user_events: Don't destroy fields when event removal fails destroy_user_event() destroys
CVE-2026-97925	In the Linux kernel, the following vulnerability has been resolved: tick/broadcast: Plug clockevents replacement race 朱恺乾 reported and decoded the following race other which drops the module reference count. This is required because the module reference cannot be dropped while holding tick_broadcast_lock. Let clockevent
CVE-2026-67221	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.0, The AMQP 0-9-1 shovel calls amqp_uri:remove_credentials
CVE-2026-97927	In the Linux kernel, the following vulnerability has been resolved: ufs: create the root dentry after loading cylinder metadata ufs_fill_super() installed sb->s_root before so the reordering is safe.
CVE-2026-97928	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: skip the VMID 0 flush for VRAM Clear-on-release only runs on VRAM, which amdgp
CVE-2026-97905	In the Linux kernel, the following vulnerability has been resolved: cpufreq: zero-initialize policy cpumask before sysfs publication cpufreq_policy_alloc() allocates p
CVE-2026-67229	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.0, add_vhost/2 calls rabbit_data_coercion:atomize_keys/1 (f
CVE-2026-97601	In the Linux kernel, the following vulnerability has been resolved: ieee802154: 6lowpan: fix NULL dereference in lowpan_newlink TUNSETLINK allows a TUN device t
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: fs: don't return -EINVAL for successful nested thaw Commit 7366f8b6fc6a ("fs: handle freezing fro dm-1: Can't mount, blockdev is frozen There is no way for userspace to drop the leaked count; only destroying the block device (or a reboot) recovers the device. F

97902	case before the reference count is touched.
CVE-2026-97603	In the Linux kernel, the following vulnerability has been resolved: idpf: disable DIM work before freeing q_vectors idpf never drains the Tx/Rx DIM works before free return while the poll tail is still queueing the work, and a plain cancel_work_sync() would be re-armed behind the drain. Use disable_work_sync(): schedule_work() c
CVE-2026-97604	In the Linux kernel, the following vulnerability has been resolved: fbdev: vfb: defer cleanup until the last reference FBIOGETCMAP takes a shallow snapshot of info: registration reference, and fbdev calls fb_destroy after the last put_fb_info(). Move the registered framebuffer's cleanup into an fb_destroy callback so its colormap
CVE-2026-97605	In the Linux kernel, the following vulnerability has been resolved: erofs: preserve LZMA decoders on resize failure The pool-resize path frees each stream's old decod
CVE-2026-97606	In the Linux kernel, the following vulnerability has been resolved: fs: autofs: fix memory leak in autofs_fill_super() In autofs_fill_super(), we create a new inode usin
CVE-2026-97607	In the Linux kernel, the following vulnerability has been resolved: vdpa: ifcvf: Put device on unsupported feature error Route unsupported provisioned features thro
CVE-2026-67404	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.0, When no CA bundle is available, ssl_options/1 falls back t
CVE-2026-67240	RabbitMQ is a messaging and streaming broker. Prior to versions 4.2.7 and 4.3.1, pattern_to_regex maps % -> .*? and _ -> ., then compiles ^...\$ with only [unicode publish messages with long property values (write permission). This issue is fixed in versions 4.2.7 and 4.3.1.
CVE-2026-97610	In the Linux kernel, the following vulnerability has been resolved: netfs: Fix uninitialized return value in netfs_unbuffered_write() If preparation of the first subrequ
CVE-2026-67235	RabbitMQ is a messaging and streaming broker. Prior to versions 4.3.0, 4.2.6, 4.1.11, 4.0.20, and 3.13.15, The content-header BodySize (a uint64) was stored with
CVE-2026-67232	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.0, The cowboy WebSocket options at line 117 set compress to port 15675/15676 No authentication required. This issue is fixed in versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.0.
CVE-2026-97613	In the Linux kernel, the following vulnerability has been resolved: net: mana: Reserve extra CQ slot for the fence completion CQE The RX completion queue is sized
CVE-2026-97614	In the Linux kernel, the following vulnerability has been resolved: net: dsa: tag_brcm: legacy FCS: request needed tailroom The legacy FCS tagger calculates the CF belongs to the object at ffff888039708400 which belongs to the cache skbuff_small_head of size 704 The buggy address is located 0 bytes to the right of allocated
CVE-2026-97615	In the Linux kernel, the following vulnerability has been resolved: net: bridge: use option bits for CFM/MRP frame handlers CFM and MRP register a global br_frame_
CVE-2026-97616	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_api: release all action references on NEWACTION failure When a batched RTM_NEV
CVE-2026-97617	In the Linux kernel, the following vulnerability has been resolved: ring-buffer: Check resize_disabled before publishing the new subbuf order ring_buffer_subbuf_ord
CVE-2026-97618	In the Linux kernel, the following vulnerability has been resolved: io_uring/net: don't overconsume buffers when using MSG_TRUNC When a recv/recvmsg is issued
CVE-2026-97619	In the Linux kernel, the following vulnerability has been resolved: io_uring/rw: end write accounting from ->ki_complete Commit b000145e9907 moved both the fsr End the write from io_complete_rw() instead, and leave only the fsnotify calls in task_work.
CVE-2026-97620	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Flush LSC untyped L1 dataport cache after rcs/ccs batches emit_render_cache_flush() sel submissions on the same queue is userspace's responsibility and belongs in Mesa, not the kernel. However, for security we must ensure stale data can't leak throu PIPE_CONTROL0_HDC_PIPELINE_FLUSH in emit_render_cache_flush() on Xe2 and later, so the L1 data cache is known clean before memory is released for reuse, wi
CVE-2026-97621	In the Linux kernel, the following vulnerability has been resolved: drm/rockchip: analogix_dp: fix unchecked bound endpoint name length rockchip_dp_drm_encode
CVE-2026-67231	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.0, The trust-store plugin installs a verify_fun that overrides in versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.0.
CVE-2026-97899	In the Linux kernel, the following vulnerability has been resolved: drm/i915: Fix memory leak in query_perf_config_list() When krealloc() fails, free the original oa_cc
CVE-2026-97900	In the Linux kernel, the following vulnerability has been resolved: drm/drm_exec: fix up contended obj when num_objects is 0 drm_exec_prepare_array() silently re num_objects is zero, so a pending contended object dont loop infinitely.

CVE-2026-97901	In the Linux kernel, the following vulnerability has been resolved: genetlink: pin family module during policy dump The generic netlink controller's policy dump kee
CVE-2026-97929	In the Linux kernel, the following vulnerability has been resolved: ALSA: usbux2y: validate URB actual_length in interrupt callback i_usx2y_in04_int() processes the
CVE-2026-97930	In the Linux kernel, the following vulnerability has been resolved: ALSA: usbux2y: fix in04_last array size mismatch with in04_buf The in04_last array in struct usx2
CVE-2026-67220	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, 4.3.0, When a binding is created on an x-jms-topic exchange, add_b
CVE-2026-97932	In the Linux kernel, the following vulnerability has been resolved: tracing: Don't dereference trace_event_file in deferred trigger free The enable_event trigger defe
CVE-2026-97959	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_route: free emptied bucket on filter move route4_change can move an existing filt CONFIG_NET_SCH_INGRESS=y, CONFIG_NET_CLS_ACT=y. tc qdisc replace dev lo clsact tc filter add dev lo ingress protocol ip pref 100 route from 1 to 1 tc filter cha
CVE-2026-97960	In the Linux kernel, the following vulnerability has been resolved: perf/x86/intel: Prevent drain_pebs() reentry The PEBS buffer is shared by all events on a CPU, so i intel_pmu_drain_pebs_buffer() call, preventing reentry. Also add a warning in intel_pmu_drain_pebs_buffer() when the full PMU is not disabled.
CVE-2026-97961	In the Linux kernel, the following vulnerability has been resolved: perf/core: Allow list_del during perf_event_overflow() A PMU might use perf_sched_cb_inc() and pe
CVE-2026-97962	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Move representor vnic reporter to eswitch devlink port The representor vnic devlink h eswitch devlink port (un)register paths, which are already serialized by the devlink instance lock, and store the handle on mlx5_devlink_port. Use the port's mlx5_v
CVE-2026-97963	In the Linux kernel, the following vulnerability has been resolved: net: stmmac: initialize ptp_lock at probe time priv->ptp_lock is only initialized in stmmac_ptp_reg
CVE-2026-97964	In the Linux kernel, the following vulnerability has been resolved: ppp_synctty: ensure a writeable skb header ppp_sync_txmunge() checks headroom before prepe
CVE-2026-97965	In the Linux kernel, the following vulnerability has been resolved: vxlan: initialize _md in vxlan_xmit_one() If a VXLAN device is configured with both VXLAN_F_COLL receive 16 bits of uninitialized kernel stack data, leaking it onto the wire. Fix this by zero-initializing _md. If IP_TUNNEL_VXLAN_OPT_BIT is not present, md->gbp re
CVE-2026-97966	In the Linux kernel, the following vulnerability has been resolved: octeontx2-pf: reset HTB scheduler topology before freeing queues HTB offload programs NIX_AF_
CVE-2026-97967	In the Linux kernel, the following vulnerability has been resolved: hwmon: (corsair-cpro) Remove debugfs entries when probe fails ccp_debugfs_init() registers debu
CVE-2026-97968	In the Linux kernel, the following vulnerability has been resolved: hwmon: (corsair-cpro) Create debugfs entries after hwmon registration ccp_debugfs_init() registe
CVE-2026-97969	In the Linux kernel, the following vulnerability has been resolved: watchdog: msc313e: Fix clock leak and spurious timer in settimeout() msc313e_wdt_settimeout()
CVE-2026-97970	In the Linux kernel, the following vulnerability has been resolved: watchdog: msc313e: Avoid division by zero clk_get_rate() could return 0. Avoid a division by zero
CVE-2026-66074	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.0, match_value/3 passes the user-supplied ?name= regular
CVE-2026-97972	In the Linux kernel, the following vulnerability has been resolved: net: macb: put the "mdio" child node reference on success macb_mii_init() holds the reference re
CVE-2026-97973	In the Linux kernel, the following vulnerability has been resolved: net: macb: destroy the phylink instance on the probe error path macb_mii_init() creates a phylink
CVE-2026-97974	In the Linux kernel, the following vulnerability has been resolved: ipv6: null-check fib6_node before accessing in __ip6_del_rt_siblings() syzbot reported a null-ptr-de ip6_route_del+0x1054/0x1110 net/ipv6/route.c:4232 inet6_rtm_delroute+0x5d7/0x6d0 net/ipv6/route.c:5669 rtnetlink_rcv_msg+0x802/0xc00 net/core/rtnetlink.c:
CVE-2026-97975	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sysfs: Fix NULL pointer dereference in device_del() A NULL pointer dereference in l device_find_child(..., __match_tty) with device_find_any_child() in hci_conn_del_sysfs(). That change was intended to avoid a use-after-free where conn->dev outliv

CVE-2026-97976	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btintel_pcie: validate packet_len before skb_put_data btintel_pcie_submit_rx_work() re
CVE-2026-97977	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btusb: Fix UAF of btusb_data by rx_work btusb_close() and btusb_flush() cancel data->
CVE-2026-97978	In the Linux kernel, the following vulnerability has been resolved: eth: ice: don't dereference pointers from TP_printk() After forwarding net-next during the v7.3 me
CVE-2026-97979	In the Linux kernel, the following vulnerability has been resolved: ice: add missing xa_destroy for sched_node_ids Commit 16dfa49406bc ("ice: Introduce new para handle this, move the sched_node_ids out of port_info and into the hw structure. All users of the array already have a pointer to hw anyways, and there is only one
CVE-2026-97980	In the Linux kernel, the following vulnerability has been resolved: s390/debug: Fix NULL pointer dereference in debug_set_level() Commit a2cec6863709 ("s390/de
CVE-2026-97981	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: cortina: Count dropped frames as NAPI work The RX loop only consumes budget w
CVE-2026-97958	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_api: Don't replay RTM_GETCHAIN in tc_ctl_chain(). If a netlink socket sends RTM_GL (kernel/time/clockevents.c:372) ? pskb_expand_head (net/core/skbuff.c:615) ? skb_release_data (net/core/skbuff.c:1122) ? netlink_attachskb (./include/linux/skbuff. arch/x86/entry/syscall_64.c:84) ? entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) </TASK>
CVE-2026-66075	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.1, is_authorized/2 for the /federation-links/.../restart route u
CVE-2026-97956	In the Linux kernel, the following vulnerability has been resolved: net: net_failover: Fix the deadlock in net_failover_slave_name_change() This is a sibling fix of con netlink_unicast+0x28f/0x3c0 netlink_sendmsg+0x216/0x450 __sys_sendto+0x222/0x230 __x64_sys_sendto+0x24/0x40 x64_sys_call+0x1d5d/0x2390 do_syscall_64
CVE-2026-97943	In the Linux kernel, the following vulnerability has been resolved: x86/mm/pat: Acquire init_mm write lock on collapse to avoid UAF x86 implements page attribute own and thus runs the risk of a use-after-free on page tables freed underneath it. In addition, concurrent CPA collapse operations are possible which can also cause
CVE-2026-97933	In the Linux kernel, the following vulnerability has been resolved: tracing: Take trace_array reference when opening a tracer options file When a tracer option file is be increased. Note, there's a race where if an admin was deleting and creating trace instances at the same time and the memory of the old trace_array's array ma
CVE-2026-97934	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix memory corruption from a "STACKTRACE" histogram key "cpu", "CPU", "stacktrace" a </IRQ> RIP: 0010:memcpy+0xc/0x30 event_hist_trigger+0x2e7/0x12c0 Kernel panic - not syncing: Fatal exception in interrupt Leave the field NULL, which is what
CVE-2026-97935	In the Linux kernel, the following vulnerability has been resolved: tracing: Set the trace clock before registering the histogram trigger hist_register_trigger() puts th addr ffff88800915d760 by task init/1 find_named_trigger+0xac/0xc0 hist_register_trigger+0xc1/0x900 event_hist_trigger_parse+0x3146/0x6af0 event_trigger_writ
CVE-2026-97936	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix memory corruption from the histogram stacktrace modifier parse_field() sets HIST_FILE enqueue_hrtimer+0x39/0xb0 __hrtimer_run_queues+0x10f/0x1f0 </IRQ> RIP: 0010:memcpy+0xc/0x30 event_hist_trigger+0x165/0x690 The timer interrupt lande
CVE-2026-67219	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.0, add_binding/3 parses the routing key as an integer weigh
CVE-2026-97938	In the Linux kernel, the following vulnerability has been resolved: reboot: fix cad_pid use-after-free race cad_pid is a single kernel-wide struct pid pointer. proc_do_ rcu_head twice can corrupt the RCU callback list. Original KASAN crash stack: kernel/pid.c:545 pid_nr_ns() # reads freed pid->level kernel/pid.c:556 pid_vnr() # cal
CVE-2026-97939	In the Linux kernel, the following vulnerability has been resolved: ipmr: account multicast table and route memory A netadmin in a user+net namespace can creat
CVE-2026-67218	RabbitMQ is a messaging and streaming broker. Prior to versions 4.0.22, 4.1.11, 4.2.6, and 4.3.0, accept_content/2 at line 56 calls rabbit_stream_manager:create_s 4.2.6, and 4.3.0.
CVE-2026-66080	RabbitMQ is a messaging and streaming broker. Prior to versions 4.1.11, 4.2.6, and 4.3.0, validate_partitions only checks that the requested partition count is at le
CVE-2026-97942	In the Linux kernel, the following vulnerability has been resolved: x86/alternatives: Exclude text poking against change_page_attr() From time to time, the followin entry_SYSCALL_64_after_hwframe+0x76/0x7e which matches the following BUG_ON() in alternative.c: /* * If something went wrong, crash and burn since recovery
CVE-2026-97944	In the Linux kernel, the following vulnerability has been resolved: x86/cfi: Fix FinelBT hash offset in cfi_get_func_hash() The switch of the FinelBT preamble from "st CONFIG_FINEIBT, the only configuration in which cfi_mode can take that value. cfi_get_func_arity() does not need the same treatment: the __bhi_args call whose di
CVE-2026-97955	In the Linux kernel, the following vulnerability has been resolved: net: mana: restore the XDP program pointer when pre-allocation fails mana_xdp_set() publishes t
CVE-	

CVE-2026-97945	In the Linux kernel, the following vulnerability has been resolved: x86/mm: Fix user-space data loss with MADV_FREE and THP Some of users of Polars (a data anal 0x5A, size); // hardware sets _PAGE_DIRTY again mprotect(buf, size, PROT_READ); // pmd_modify() drops the dirty bit mprotect(buf, size, PROT_READ PROT_WRITE)
CVE-2026-97946	In the Linux kernel, the following vulnerability has been resolved: x86/amd_node: Fix PCI device reference counting in amd_smn_init() The local "root" pointer is a t
CVE-2026-97947	In the Linux kernel, the following vulnerability has been resolved: x86/amd_node: Fix potential NULL pointer dereference amd_smn_read/write() are exported functi Rebase & further touchups.]
CVE-2026-97948	In the Linux kernel, the following vulnerability has been resolved: powerpc/eeh: Fix recursive locking on devices without EEH sensitive driver The commit 1010b4cc returns PCI_ERS_RESULT_NEED_RESET, and driver being not EEH sensitive(i.e no error handlers like slot_reset(), resume() etc defined).
CVE-2026-97949	In the Linux kernel, the following vulnerability has been resolved: configfs: unhash the dentry before dropping the item in rmdir configfs_get_config_item() treats a
CVE-2026-97950	In the Linux kernel, the following vulnerability has been resolved: configfs: pin the symlink target's dirent instead of chasing ->ci_dentry create_link() reads the targ
CVE-2026-97951	In the Linux kernel, the following vulnerability has been resolved: scsi: target: iscsi: Fix hang for aborted WRITE_PENDING commands When a LUN_RESET aborts a I
CVE-2026-97952	In the Linux kernel, the following vulnerability has been resolved: sunvdc: unmap LDC cookies when the descriptor send fails __send_request() maps the request's I fragmentation makes large multi-segment requests fail first as the table drains, until ldc_map_sg() fails permanently and the disk is dead until reboot. It also make:
CVE-2026-66077	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, and 4.2.6, The management UI uses EJS 1.0 in which <%= ... %> does NC session, allowing full account takeover (create users, export definitions, etc.). The management UI's CSP includes 'unsafe-inline', so inline script execution is not blo
CVE-2026-97954	In the Linux kernel, the following vulnerability has been resolved: net/rds: fix tcp stream corruption with large pages rds_message_map_pages() assigns PAGE_SIZE
CVE-2026-67405	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.0, Neither the Web-MQTT handler (deps/rabbitmq_web_mq)
CVE-2026-97600	In the Linux kernel, the following vulnerability has been resolved: ieee802154: cc2520: fix FIFO work use-after-free The FIFO interrupt handler queues cc2520_fifo
CVE-2026-97517	In the Linux kernel, the following vulnerability has been resolved: wifi: nl80211: reject beacons with bad HE operation The HE operation element not only needs to l
CVE-2026-6083	Stored Cross-Site Scripting (XSS) vulnerability in StockAgile API and management panel. The vulnerability is present on the server side in REST endpoint '/inventor
CVE-2026-6085	Stored Cross-Site Scripting (XSS) vulnerability in StockAgile API and management panel. The vulnerability is present on the server side in REST endpoint '/inventory
CVE-2026-6086	Stored Cross-Site Scripting (XSS) vulnerability in StockAgile API and management panel. The vulnerability is present on the server side in REST endpoint '/inventory
CVE-2026-6087	Stored Cross-Site Scripting (XSS) vulnerability in StockAgile API and management panel. The vulnerability is present on the server side in REST endpoint '/inventory
CVE-2026-6088	Stored Cross-Site Scripting (XSS) vulnerability in StockAgile API and management panel. The vulnerability is present on the server side in REST endpoint '/inventory
CVE-2026-97149	In OpenStack Swift before 2.38.2, the tempurl middleware does not reject the X-Copy-From header on PUT requests. A TempURL signature only covers the method
CVE-2026-82372	Improper handling of sensitive data during IPsec policy creation and modification in Brocade SANnav versions before 3.0.1a results in pre-shared keys being record
CVE-2026-97863	The cisco_firesight_manager_ACL_rule_export module in misp-modules generates a shell script (.sh) that authenticates to and calls the Cisco fireSIGHT Manager AP afterward, causing a NameError (denial of service) when the request payload lacked a 'config' key. The vulnerability requires the attacker to have the ability to sub
CVE-2026-92106	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dashbitco lazy_html allows mutation XSS via a parse and serial
CVE-	

CVE-2026-97898	Insecure Direct Object Reference / missing object-level authorization in the Akia keyless entry cloud service. The unlock action is relying on a client-supplied room/
CVE-2026-27867	An attacker with access via network to the Regesta Smart HD-PLC of the provider Teldat (in this case, registration action is required) who has the vulnerable firmw
CVE-2026-97522	In the Linux kernel, the following vulnerability has been resolved: mptcp: fix bad accounting in __mptcp_subflow_push_pending() If __subflow_push_pending() errors
CVE-2026-88360	libvips 8.19.0 contains a memory access vulnerability when processing little-endian PFM images. If the PFM text header length is not a multiple of four bytes, the m
CVE-2026-97526	In the Linux kernel, the following vulnerability has been resolved: s390/pai: Support CPU hotplug for PMU PAI The command 'perf stat -e pai_crypto/CRYPTO_ALL/ -- used inside that function. Add CPU hotplug support for CPU add and delete and create the necessary per-CPU data infrastructure during CPU hotplug add processin
CVE-2026-91187	Improper Verification of Cryptographic Signature vulnerability in dashbit nimble_zta allows an unauthenticated remote attacker to authenticate as an arbitrary Clou
CVE-2026-97529	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Validate BSG request_len before reading vendor_cmd[] The FC BSG transport allocat qla84xx_reset(), qla84xx_updatefw(), qla2x00_read_optrom(), qla2x00_update_optrom(), qlafx00_mgmt_cmd() and qla28xx_validate_flash_image().
CVE-2026-97530	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Fix soft lockup polling continuation IOCB signature qla27xx_copy_multiple_pkt() and STATUS_CONT_TYPE guard instead. Remove the signature busy-wait from both helpers, keeping the entry_type guard, and gate the FPIN path with qla_chk_cont_io
CVE-2026-86860	ServiceNow has remediated a missing authorization vulnerability that was identified in the ServiceNow AI Platform. This vulnerability could enable an unauthentica
CVE-2026-97532	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Null out freed pointers in qla2x00_mem_alloc() error path When qla2x00_mem_allo
CVE-2026-97533	In the Linux kernel, the following vulnerability has been resolved: x86/mm/pat: Acquire init_mm read lock on attribute changes to avoid UAF A previous commit pro __change_page_attr_set_clr(). However, the lock must not be held over an allocation, as allocation can trigger reclaim and shrinkers may call into CPA recursively, r set_memory_rox(), which exclusively operates upon vmalloc ranges, and on x86 only within the module mapping space. This is important, because some callers di
CVE-2026-97534	In the Linux kernel, the following vulnerability has been resolved: f2fs: accurately adjust free_sections during free_segment_range In free_segment_range(), MAIN_§
CVE-2026-97535	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Bound VP index against VP_CTRL IOCB bitmap size The VP control IOCB selects its t
CVE-2026-97537	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Fix queue teardown NULL dma_free and bitmap locking qla25xx_free_req_que() and atomically NULL the map entry and clear the bitmap bit. - Removing the now-redundant clear_bit blocks from the create error paths since the free functions handle
CVE-2026-97538	In the Linux kernel, the following vulnerability has been resolved: hwmon: (asus_rog_ryujin) Validate HID report lengths rog_ryujin_raw_event() parses response hei
CVE-2026-6084	Stored Cross-Site Scripting (XSS) vulnerability in StockAgile API and management panel. The vulnerability is present on the server side in REST endpoint '/inventory
CVE-2026-6082	Stored Cross-Site Scripting (XSS) vulnerability in StockAgile API and management panel. The vulnerability is present on the server side in REST endpoint '/inventory
CVE-2026-97599	In the Linux kernel, the following vulnerability has been resolved: ieee802154: hwsim: serialize pib updates to fix double-free hwsim_update_pib() does an unseriali
CVE-2026-97151	mammoth (aka mammoth.js) before 1.12.2 is vulnerable to prototype pollution when reading the styles defined in a document. Converting a crafted .docx file allow
CVE-2026-4638	PRTG Network Monitor before version 26.2.120.1449 ships a demo EXE/Script sensor that multiplies two integer parameters using cscript.exe. If a non-numeric val
CVE-2026-79680	Authentication bypass vulnerability in the password authentication mechanism of the Qt VNC Server module. An attacker using a specially modified VNC client that
CVE-2026-75553	Smartphone application Tohoku Electric Power "Yorisou e Net" uses a hard-coded cryptographic key, which may allow an attacker to retrieve a hard-coded cryptog
CVE-	

CVE-2026-85417	Incomplete property masking in the SANnav logging subsystem permits SNMP authentication and privacy passwords to be recorded in application logs under speci
CVE-2026-53493	containerd is an open-source container runtime. Prior to versions 1.7.36, 2.0.13, 2.2.9, 2.3.6, and 2.4.1, a crafted OCI index graph can force very high CPU/memory
CVE-2026-87739	An improper authentication vulnerability in PaperCut MF/NG allows an unauthenticated, remote attacker to trigger report generation. By submitting report generati
CVE-2026-82077	An improper limitation of a pathname to a restricted directory (path traversal) vulnerability in the Scan-to-Fax component of PaperCut NG and PaperCut MF allows i
CVE-2026-85082	Root Browser Classic 3.3.0 passes the path of a selected SQLite database to an operating-system shell without safely separating the filename from the command.
CVE-2026-84283	Secure Folder 1.2 stores files selected for its password-protected vault as unencrypted files in the Android shared-storage tree. A local application or file manager t
CVE-2026-97387	Rejected reason: This CVE is a duplicate of another CVE.
CVE-2026-93477	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in ash-project ash allows a user to set the value of a private action an one referenced by an arg(...) template in the action's changes or validations. Depending on how the application uses the argument (for example an acting_user_id
CVE-2026-87722	Uncontrolled Resource Consumption (CWE-400 / CWE-1333) in regex search query predicates (such as RegexProjectPredicate, RegexRefPredicate, RegexPathPredi 3.13.9, and 3.14.3.
CVE-2026-11744	An input validation vulnerability exists in the PaperCut Hive embedded application for Ricoh devices. The application fails to properly sanitize input received during
CVE-2026-87721	Uncontrolled Resource Consumption (CWE-400 / CWE-407) in the ANTLR 3 search query parser (QueryParser / Query.g) in Gerrit Code Review versions 2.0.19 throu
CVE-2026-87720	Incorrect Authorization (CWE-863) in project name normalization (ProjectUtil.stripGitSuffix) and ProjectCache eviction logic (ProjectCacheImpl) in Gerrit Code Review
CVE-2026-97168	Rejected reason: it is a suggestion
CVE-2026-7169	a vulnerability involving an unchecked search path element in Evope Collector, versions prior to 1.1.7.13, allows a local attacker without privileges to load a malicio
CVE-2026-14443	Incomplete log sanitization during bulk IPsec policy collection in Brocade SANnav versions before 3.0.1a permit extension switch pre-shared keys to be written to s
CVE-2026-14442	An information exposure vulnerability in the job scheduling component of SANnav allows sensitive credentials to be written to application logs in plain text. When s
CVE-2026-14441	A logic flaw in Java cache key handling object comparison handling could lead to improper identifier resolution when processing specific user account structures. Th
CVE-2026-14780	A vulnerability exists in the PaperCut NG/MF platform's device-scripting functionality due to insufficient sanitization and access restrictions within the embedded ex
CVE-2026-96515	This vulnerability exists in the Netlink ICT HG323RW router due to insufficient authorization and input validation controls in the diagnostic script import functionalit
CVE-2026-97152	Nanomsg versions 0.5-beta through 1.x before 1.2.3 has a remotely exploitable buffer overflow in the WebSocket transport, due to an unchecked copy of the Sec-V
CVE-2026-97539	In the Linux kernel, the following vulnerability has been resolved: usb: xusbatm: don't rely on id table pointer arithmetic The current code is broken when dynamic
CVE-2026-97540	In the Linux kernel, the following vulnerability has been resolved: net: usb: pegasus: don't rely on id table pointer arithmetic The current code is broken when dyna
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: wifi: ath9k_htc: don't store usb_device_id usb_device_id is not guaranteed to live longer than prol

97541	
CVE-2026-97542	In the Linux kernel, the following vulnerability has been resolved: xfs: bail out on bitmap errors in xrep_agfl_fill LOLLM also points out that the xagb_bitmap_set call
CVE-2026-97572	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Propagate RX ring init failures in bnxt_init_nic() bnxt_init_rx_rings() returns an error whe
CVE-2026-97574	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Don't free the live ring's TPA state on queue restart failure bnxt_queue_mem_alloc() sha
CVE-2026-82370	Unauthenticated remote command injection in the Brocade SANnav orchestrator HTTP service permits network-adjacent attackers to execute arbitrary administrat
CVE-2026-86857	ServiceNow has remediated an authorization bypass security issue that was identified in the ServiceNow AI Platform. This security issue, if exploited, could enable
CVE-2026-82371	Plaintext exposure of sensitive authentication data in Brocade SANnav discovery service log files enables individuals with file read access to retrieve administrative
CVE-2026-59980	hpack is an HTTP/2 Header Encoding for Python. Prior to version 4.2.0, unbounded variable integer decoding can cause run-away computation on malformed input
CVE-2026-97581	In the Linux kernel, the following vulnerability has been resolved: media: verisilicon: hantro: bound G2 HEVC tile loop to the buffer capacity prepare_tile_info_buffer
CVE-2026-97582	In the Linux kernel, the following vulnerability has been resolved: hwmon: (gpio-fan) Fix use-after-free in alarm work fan_alarm_irq_handler() queues fan_data->ala
CVE-2026-57168	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-56120. Reason: This candidate is a duplicate of CVE-2026-56120. Not
CVE-2026-57854	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-97585	In the Linux kernel, the following vulnerability has been resolved: afs: Fix double-unmap of directory block Fix afs_edit_dir_remove() to use a cleanup function to ur
CVE-2026-97586	In the Linux kernel, the following vulnerability has been resolved: afs: Fix missing kunmap in afs_dir_search_bucket() Fix afs_dir_search_bucket() to kunmap the blo
CVE-2026-97587	In the Linux kernel, the following vulnerability has been resolved: perf: RISC-V: store available counter mask as bitmap The available-counter mask was a single un
CVE-2026-97588	In the Linux kernel, the following vulnerability has been resolved: s390/crypto: Map EBUSY to EIO when key conversion fails repeatedly When hardware persistently
CVE-2026-82369	Insufficient input sanitization of shell metacharacters in the Brocade SANnav CLI scripting component permits authenticated users to break out of restricted execut
CVE-2026-97590	In the Linux kernel, the following vulnerability has been resolved: s390/crypto: Fix missing scrub of temp buffers with PAES algorithm In function ctr_paes_do_crypt
CVE-2026-97591	In the Linux kernel, the following vulnerability has been resolved: s390/crypto: Fix handling of EBUSY in PHMAC when req is pushed to crypto engine When a reques
CVE-2026-97592	In the Linux kernel, the following vulnerability has been resolved: s390/crypto: Fix missing scrub of temp buffers with AES ctr and gcm algorithm In function ctr_aes
CVE-2026-97593	In the Linux kernel, the following vulnerability has been resolved: iommu/s390: Fix NULL dereference in iova_to_phys() with ZPCI_TABLE_TYPE_RFX When using a 5-
CVE-2026-12559	A Stored Cross-Site Scripting (XSS) vulnerability has been identified in OpenText Vendor Invoice Management for SAP Solutions Capture Validation application. Und
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: ipv6: reject invalid states in connection template sync records IPV6 sync receivers validate protoc

97596	
CVE-2026-97597	In the Linux kernel, the following vulnerability has been resolved: ipv6: flowlabel: cap duplicate leases per socket ipv6_flowlabel_get() allocates an ipv6_fl_socklist entry before updating linger and expires so a rejected GET does not refresh the shared label, matching the existing socket-list allocation failure path.
CVE-2026-97598	In the Linux kernel, the following vulnerability has been resolved: ipv4: fib: bound automatic table ID allocation fib_empty_table() probes every table ID from 1 until it finds a free one, which can cause a denial of service if the table ID space is exhausted.
CVE-2026-97571	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Propagate TPA buffer allocation failures in bnxt_queue_mem_alloc() bnxt_alloc_one_tpa() can fail to allocate a TPA buffer, which can cause a denial of service if the TPA buffer pool is exhausted.
CVE-2026-97569	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Prevent queue stop with deferred completions When the driver receives a burst of packets, it can stop the queue with deferred completions, which can cause the queue to stop and never be restarted. Assuming default CONFIG_MAX_SKB_FRAGS, this is only possible if the queue is stopped for more than 100ms.
CVE-2026-97568	In the Linux kernel, the following vulnerability has been resolved: mptcp: syncookies: remember the request backup flag Instead of using an uninitialised bit when a request is received, the driver should remember the request backup flag, which can cause a denial of service if the request backup flag is not set.
CVE-2026-97553	In the Linux kernel, the following vulnerability has been resolved: xfs: lock the healthmon when inserting unmount event LOLLM complains that xfs_healthmon_unmount() can be called without the healthmon lock, which can cause a denial of service if the healthmon lock is not held.
CVE-2026-97543	In the Linux kernel, the following vulnerability has been resolved: xfs: destroy seen inode bitmap when we fail to add a dirpath LOLLM observes a memory leak in xfs_destroy_inode_bitmap() when it fails to add a dirpath, which can cause a denial of service if the inode bitmap is not destroyed.
CVE-2026-97544	In the Linux kernel, the following vulnerability has been resolved: xfs: don't leak dqacct if rhashtable insertion fails LOLLM observes that xqcheck_mod_live_ino_dqt() can leak memory if the rhashtable insertion fails, which can cause a denial of service if the memory is not freed.
CVE-2026-97545	In the Linux kernel, the following vulnerability has been resolved: xfs: don't leak new_bp if xfs_btree_bload_drop_buf fails LOLLM observes that in xfs_btree_bload_drop_buf() if it fails to drop a buffer, it can leak memory, which can cause a denial of service if the memory is not freed.
CVE-2026-97546	In the Linux kernel, the following vulnerability has been resolved: xfs: don't spin forever on zero-length dirents when salvaging them LOLLM noticed that xrep_dir_entry() can spin forever if it encounters a zero-length dirent, which can cause a denial of service if the loop is not broken.
CVE-2026-97547	In the Linux kernel, the following vulnerability has been resolved: xfs: fix exchange-range reflink flag clearing issue with INO1_WRITTEN When exchanging two full-height reflinks, the driver should clear the INO1_WRITTEN flag, which can cause a conservative outcome is that both inodes keep the reflink flag. The regular reflink flag cleanup path can drop the extra flag later once the inode no longer has shared blocks.
CVE-2026-86859	ServiceNow has remediated an authorization bypass security issue that was identified in the ServiceNow AI Platform. This security issue, if exploited, could enable an attacker to bypass authorization controls and access sensitive information.
CVE-2026-97549	In the Linux kernel, the following vulnerability has been resolved: xfs: fix under-reservation of blocks when repairing sf directories Whilst running QA on XFS for-next, I discovered a bug in xfs_sf_repair() that can cause a denial of service if the transaction is not committed. The bug is caused by a miscalculation of the space reserved for the transaction, which can cause a filesystem shutdown. Note that the xfs_dabuf_nfsb helper will compute the correct value for directories and xattr, so it is not affected by this bug.
CVE-2026-97550	In the Linux kernel, the following vulnerability has been resolved: xfs: fix unit conversions in per_binval computation LOLLM noticed that we're doing the unit conversions incorrectly, which can cause a denial of service if the computation is not done correctly.
CVE-2026-97551	In the Linux kernel, the following vulnerability has been resolved: xfs: initialise args->total for parent pointer updates xfs_parent_da_args_init() builds an xfs_da_args structure, but it does not initialise the args->total field, which can cause a denial of service if the total is not initialised.
CVE-2026-97552	In the Linux kernel, the following vulnerability has been resolved: xfs: initialise error in xfs_defer_finish_one() xfs_defer_finish_one() declares error without an initial value, which can cause a denial of service if the error is not initialised.
CVE-2026-97554	In the Linux kernel, the following vulnerability has been resolved: smb: client: avoid using uninitialized SIDs in cifs_posix_to_fattr() cifs_posix_to_fattr() ignores the result of the posix_to_fattr() call, which can cause a denial of service if the SIDs are not initialised.
CVE-2026-97567	In the Linux kernel, the following vulnerability has been resolved: mptcp: prevent race between disconnect() and rtx Sashiko noted that the two event can race, leading to a denial of service if the race is not handled correctly.
CVE-2026-97556	In the Linux kernel, the following vulnerability has been resolved: smb: client: avoid leaking refcount when cifs_sb_tlink() fails cifs_oplock_break() takes over the refcount, which can cause a denial of service if the refcount is not managed correctly.
CVE-2026-86858	ServiceNow has remediated an improper access control security issue that was identified in the ServiceNow AI Platform. This security issue could enable an unauthorized user to access sensitive information.
CVE-2026-97558	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix cifsFileInfo reference leak in deferred close When cifs_close() defers a close, it has a reference to the cifsFileInfo structure, but it does not decrement the reference count, which can cause a denial of service if the reference is not decremented.
CVE-	

CVE-2026-97559	In the Linux kernel, the following vulnerability has been resolved: smb: client: fail DACL rewrite when the new DACL exceeds 64K replace_sids_and_copy_aces() and because a DACL can only hold 2^16-1 bytes on the wire and larger DACLs cannot be represented. set_chmod_dacl() carries the same pattern and is fixed the same way
CVE-2026-97560	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix one-byte OOB read in smb2_parse_native_symlink() When parsing a share-root relative path, the code incorrectly used the wrong offset to calculate the end of the path. This could lead to a read beyond the end of the buffer. The fix is to use the correct offset to calculate the end of the path.
CVE-2026-97561	In the Linux kernel, the following vulnerability has been resolved: smb: client: honor forceuid/forcegid when mapping SIDs to uid/gid When the administrator mounts a share, the kernel should honor the forceuid/forcegid option and map the SIDs to the corresponding uid/gid. The fix is to use the correct uid/gid when mapping SIDs.
CVE-2026-97563	In the Linux kernel, the following vulnerability has been resolved: smb: client: reject out-of-bounds DataOffset in CIFSSMBRead() The SMB1 synchronous read helper incorrectly used the DataOffset to calculate the end of the buffer. This could lead to a read beyond the end of the buffer. The fix is to use the correct offset to calculate the end of the buffer.
CVE-2026-97564	In the Linux kernel, the following vulnerability has been resolved: smb: client: reject userspace cifs.idmap descriptions cifs.idmap key descriptions carry authority-tokens and should not be used for mapping SIDs to uid/gid
CVE-2026-97565	In the Linux kernel, the following vulnerability has been resolved: smb: client: reject short READ responses in CIFSSMBRead() CIFSSMBRead() reads DataLengthHigh and DataLengthLow to calculate the total length of the response. The fix is to use the correct offset to calculate the end of the buffer.
CVE-2026-97566	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: kernel: drop pending ADD_ADDR when removing ID0 The in-kernel MPTCP path manager patch will ensure that. mptcp_pm_announced_remove() uses use_port=true for comparison. So clear the port before the lookup.
CVE-2026-97982	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: cortina: Fix budget accounting The gmac_rx() function returns the remaining NAPI budget. The fix is to use the correct offset to calculate the end of the buffer.
CVE-2026-97983	In the Linux kernel, the following vulnerability has been resolved: vduse: return compat ioctl results directly The compat handler handles VDUSE_IOTLB_GET_FD and VDUSE_IOTLB_SET_FD. The fix is to use the correct offset to calculate the end of the buffer.
CVE-2026-97984	In the Linux kernel, the following vulnerability has been resolved: net: ipv6: Fix UDP length overflow with PMTU discover and big MTU This commit bounds cork->len to avoid breaking sending UDP jumbograms over raw IPv6 sockets, limit the change to UDP sockets only. The original overflow bug with IPv6 and IPV6_PMTUDISC_PATHMTU was fixed by commit 1d1e1e1d.
CVE-2026-98127	In the Linux kernel, the following vulnerability has been resolved: smb/client: validate new EOF for insert range smb3_insert_range() does not check if the new file size is greater than the current file size. File too large size after write: 3145728 fallocate: fallocate failed: File too large size after insert: 2097152
CVE-2026-98129	In the Linux kernel, the following vulnerability has been resolved: scsi: mpi3mr: Fix NULL pointer dereference in mpi3mr_sas_port_add() sas_port_alloc_num() can return NULL. The fix is to use the correct offset to calculate the end of the buffer.
CVE-2026-82406	Klever-Go is the Go implementation of the Klever blockchain protocol. Prior to 1.7.20, the native marketplace function core/kapp/market/market.go Buy does not check if the user has enough funds to buy the item.
CVE-2026-98131	In the Linux kernel, the following vulnerability has been resolved: net: stmmac: fix dma mapping leak in stmmac_tso_xmit() In stmmac_tso_xmit(), if the DMA mapping is not released, it will lead to a memory leak. The fix is to use the correct offset to calculate the end of the buffer.
CVE-2026-98132	In the Linux kernel, the following vulnerability has been resolved: bpf: don't downgrade half-dead scalar zero spills to STACK_ZERO states.c: __clean_func_state() can be called with a half-dead scalar zero spill. The fix is to use the correct offset to calculate the end of the buffer.
CVE-2026-98133	In the Linux kernel, the following vulnerability has been resolved: ntfs: leave HasEA flag untouched on setattr failure In ntfs_set_ea(), the exit path unconditionally clears the HasEA flag. The fix is to use the correct offset to calculate the end of the buffer.
CVE-2026-98134	In the Linux kernel, the following vulnerability has been resolved: bpf: check_cond_jump_op(): properly infer if register is null Nicholas Carlini reported a bug when verifying a BPF program with a conditional jump. The fix is to use the correct offset to calculate the end of the buffer.
CVE-2026-98135	In the Linux kernel, the following vulnerability has been resolved: ntfs: reject invalid sectors_per_cluster in the boot sector is_boot_sector_ntfs() checks the boot sector for invalid sectors_per_cluster. The fix is to use the correct offset to calculate the end of the buffer.
CVE-2026-98136	In the Linux kernel, the following vulnerability has been resolved: ntfs: bound \$AttrDef table walk to the loaded table size ntfs_attr_find_in_attrdef() walks the in-memory \$AttrDef table. The fix is to use the correct offset to calculate the end of the buffer.
CVE-2026-98137	In the Linux kernel, the following vulnerability has been resolved: ntfs: treat any nonzero dio zero-range return as an error ntfs_dio_zero_range() returns either 0 or -EINVAL. The fix is to use the correct offset to calculate the end of the buffer.
CVE-2026-98138	In the Linux kernel, the following vulnerability has been resolved: ntfs: do not mark the volume clean in sync_fs when errors were recorded ntfs_put_super() and the sync_fs function. The fix is to use the correct offset to calculate the end of the buffer.
CVE-2026-98139	In the Linux kernel, the following vulnerability has been resolved: ntfs: only count successfully cleared runs when freeing clusters ntfs_cluster_free_from_rl_nolock() counts all runs. The fix is to use the correct offset to calculate the end of the buffer.
CVE-	

CVE-2026-98140	In the Linux kernel, the following vulnerability has been resolved: ntfs: fix kmap_local leak in write_mft_record_nolock() error paths write_mft_record_nolock() maps
CVE-2026-98141	In the Linux kernel, the following vulnerability has been resolved: ntfs: propagate reparse index insertion failure update_reparse_data() ignores the return value of
CVE-2026-98142	In the Linux kernel, the following vulnerability has been resolved: drm/cirrus-qemu: Validate BAR0 size during probe The `cirrus-qemu` driver relies on `CIRRUS_VR cirrus_primary_plane_helper_atomic_update+0x98a/0xb00 drivers/gpu/drm/tiny/cirrus-qemu.c:358 drm_atomic_helper_commit_planes+0x626/0xea0 drivers/gpu/d
CVE-2026-82405	Klever-Go is the Go implementation of the Klever blockchain protocol. Prior to 1.7.20, the KleverUpdateAccountPermission built-in authorizes replacement of a targ
CVE-2026-98144	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: put the chained BO when its mapping fails amdxdna_cmd_set_error() looks up th
CVE-2026-98145	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: reject a command chain that carries no commands A chain whose command_cou
CVE-2026-98146	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Remove __counted_by from struct amdxdna_cmd_chain struct amdxdna_cmd_ch
CVE-2026-98147	In the Linux kernel, the following vulnerability has been resolved: printk: Don't WARN on kthread_run failure. Since __kthread_create_on_node() returns -EINTR upon
CVE-2026-98148	In the Linux kernel, the following vulnerability has been resolved: drm/gud: validate GUD_ROTATION_0 is present in supported rotations The rotation argument to d
CVE-2026-98149	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix percpu map update indexing with sparse CPU IDs Per-CPU array, hash, and cgroup storag the same value for every CPU.
CVE-2026-68492	An untrusted search path vulnerability in Plesk from 18.0.34 before 18.0.80.8 and 18.0.81 before 18.0.81.1 allows remote authenticated users to execute arbitrary
CVE-2026-98151	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix REG INVARIANTS VIOLATION on speculative pointer arithmetic Take the following unprivl directly as a speculative path. 4. That snapshot is taken between step 2 and the final reg_bounds_sync(): at this point dst_reg's var_off still holds the (const) origina
CVE-2026-98128	In the Linux kernel, the following vulnerability has been resolved: scsi: mpi3mr: Fix target device refcount leak in mpi3mr_sas_port_add() mpi3mr_get_tgtdev_by_ar
CVE-2026-98126	In the Linux kernel, the following vulnerability has been resolved: smb/client: validate new EOF for zero range When FALLOC_FL_ZERO_RANGE is used without FALL
CVE-2026-97985	In the Linux kernel, the following vulnerability has been resolved: af_unix: Update last skb marker in manage_oob(). Fahad Alharbi reported that blocking recv(MSG peek case, @last matches the returned value (when !copied) because OOB is unlinked. Note that manage_oob() is inlined and no stack canary is added.
CVE-2026-98125	In the Linux kernel, the following vulnerability has been resolved: smb/client: fix stale page cache in insert/collapse range smb3_insert_range() and smb3_collapse_ on the server. cat "\$FILE" > /dev/null fallocate --insert-range -o 0 -l 4K "\$FILE" if cmp -s /tmp/expected "\$FILE"; then echo "readback: OK" else echo "readback: STA
CVE-2026-98099	In the Linux kernel, the following vulnerability has been resolved: ipv6: mcast: use rcu_assign_pointer() for __rcu list updates Several places in net/ipv6/mcast.c up
CVE-2026-98101	In the Linux kernel, the following vulnerability has been resolved: ipv6: mcast: use copy-on-write RCU updates in ip6_mc_source() pmc->sflist is read locklessly unc
CVE-2026-98102	In the Linux kernel, the following vulnerability has been resolved: ipv6: mcast: fix RCU list diversion in ip6_mc_del1_src() When removing a source filter whose cour
CVE-2026-98103	In the Linux kernel, the following vulnerability has been resolved: igmp: convert struct ip_sf_list to RCU Commit 23d2b94043ca ("igmp: Add ip_mc_list lock in ip_ch __rcu pointers. 2. Use rcu_assign_pointer() and kfree_rcu() for list updates and deletions. 3. Remove spin_lock_bh(&im->lock) from ip_check_mc_rcu() and traverse
CVE-2026-98104	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_u32: fix duplicate handle when node ID pool is exhausted gen_new_kid() falls back allowing cross-tcf_proto knode add/lookup/delete. Add the same exhaustion check that the divisor path already has. Return an error so u32_change() fails with ENC
CVE-2026-98105	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: oa_tc6: Improve the error recovery When oversubscribed traffic causes lot of buffe
CVE-	In the Linux kernel, the following vulnerability has been resolved: drm/pagemap: Prevent double migration of device pages A device-private folio migrated to syste

CVE-2026-98106	covered by a migrated folio so retirement remains valid if the folio is later split. v3: - Store the migrated state in a low bit of zone_device_data instead of adding vir Tainted: [S]=CPU_OUT_OF_SPEC, [O]=OOT_MODULE [10109.860524] Hardware name: ASUS System Product Name/PRIME Z790-P WIFI, BIOS 0812 02/24/2023 [101 [10109.860704] ? drm_pagemap_evict_to_ram+0x96/0x370 [drm_gpuvm_helper] [10109.860709] xe_svm_bo_evict+0x15/0x20 [xe] [10109.860819] ? xe_svm_bo
CVE-2026-98107	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: fix out-of-bounds write in l2cap_ecred_connect l2cap_chan_connect() tries to e
CVE-2026-52001	An issue in geelen mcp-remote 0.1.18 through 0.1.38 allows a remote attacker to obtain sensitive information via the SSE transport eventSourceInit fetch wrapper
CVE-2026-98109	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_core: Fix race condition during device registration In hci_register_dev(), the power_ WARNING: kernel/locking/mutex.c:625 at __mutex_lock+0x12d8/0x1550 kernel/locking/mutex.c:821 ... Call Trace: <TASK> msft_do_close+0x308/0x7b0 net/blueto
CVE-2026-98110	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btintel: bound firmware ID by TLV length The firmware ID is treated as a NUL-terminat
CVE-2026-98111	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btintel: validate version TLV value lengths btintel_parse_version_tlv() verifies that a co
CVE-2026-98113	In the Linux kernel, the following vulnerability has been resolved: ksmbd: rate limit unmapped SID errors A client can include many structurally valid but unmappe
CVE-2026-98114	In the Linux kernel, the following vulnerability has been resolved: ksmbd: propagate DACL parsing errors parse_dacl() silently accepts truncated ACEs and allocatio
CVE-2026-82409	Klever-Go is the Go implementation of the Klever blockchain protocol. Prior to 1.7.20, indexer/common.go serializedDataForUpdateAccounts places the attacker-co
CVE-2026-98117	In the Linux kernel, the following vulnerability has been resolved: cachefiles: Fix potential UAF/KASAN warning Currently, trace_cachefiles_coherency() is being pas
CVE-2026-98118	In the Linux kernel, the following vulnerability has been resolved: netfs: Fix readahead synchronisation issues by loading all folios upfront There are some synchror count, not a folio count). The folio refs acquired from readahead are then dropped in bulk once the first subrequest is dispatched as it's quite a slow operation. The
CVE-2026-98119	In the Linux kernel, the following vulnerability has been resolved: netfs: break unbuffered write when netfs_alloc_subrequest() fails syzbot reported a null-ptr-deref netfs_unbuffered_write_iter+0x442/0x720 fs/netfs/direct_write.c:382 v9fs_file_write_iter+0xbf/0x100 fs/9p/vfs_file.c:409 new_sync_write fs/read_write.c:595 [inline
CVE-2026-98120	In the Linux kernel, the following vulnerability has been resolved: netfs: Fix subreq ref leak Fix a subrequest ref leak in netfs_unbuffered_write() in the event that s
CVE-2026-98121	In the Linux kernel, the following vulnerability has been resolved: watchdog: msc313e: Fix NULL pointer dereference in PM callbacks msc313e_wdt_probe() doesn't
CVE-2026-82407	Klever-Go is the Go implementation of the Klever blockchain protocol. Prior to 1.7.20, core/kapp/validators/validators.go Register and the runtime validator update
CVE-2026-98123	In the Linux kernel, the following vulnerability has been resolved: sctp: fix soft lockup from unpadded ASCONF-ACK parameter iteration sctp_verify_asconf() walks / SCTP_PARAM_ERR_CAUSE case of sctp_verify_asconf() also performs no length check, letting a parameter without a complete error header reach the consumer, wh
CVE-2026-98124	In the Linux kernel, the following vulnerability has been resolved: smb/client: invalidate fscache for fallocate range operations smb3_zero_range(), smb3_punch_ho /proc/sys/vm/drop_caches fallocate --zero-range -o 1M -l 1M "\$FILE" if cmp -s /tmp/expected "\$FILE"; then echo "readback: OK" else echo "readback: STALE DATA" ;
CVE-2026-98152	In the Linux kernel, the following vulnerability has been resolved: nvmet-rdma: fix queue leak when connect backlog is exceeded When pending disconnecting que
CVE-2026-98153	In the Linux kernel, the following vulnerability has been resolved: nvme: fix racy access to FDP placement id array nvme_query_fdp_info() is called per-path and the
CVE-2026-68490	Incorrect permission assignment allows local users to obtain sensitive CalDAV/CardDAV information belonging to other accounts.
CVE-2026-98155	In the Linux kernel, the following vulnerability has been resolved: accel/qaic: Address potential out-of-bounds read in resp_worker() Although 'commit 2feec5ae5df,
CVE-2026-80430	Improper Link Resolution Before File Access in the drag source staging path of the drag and drop protocol in kitty from 0.47.0 before 0.49.0 allows a program writin O_EXCL at mode 0644, so existing files cannot be overwritten, and directories are created with mkdirat() at mode 0755, so the attacker can create intermediate di
CVE-	

CVE-2026-80431	Out-of-bounds Write in the natural width branch of the text sizing protocol in kitty from 0.40.0 before 0.49.0 allows a program writing to the terminal to write past t
CVE-2026-13016	ServiceNow has remediated a SQL injection vulnerability that was identified in the ServiceNow AI Platform. This vulnerability could enable an unauthenticated user,
CVE-2026-90481	In PortSwigger Burp Suite DAST (formerly Burp Suite Enterprise Edition) before 2026.8, an authentication bypass can occur via an alternate path or channel.
CVE-2026-98160	In the Linux kernel, the following vulnerability has been resolved: staging: rtl8723bs: fix mismatched free of HalData in rtw_sdio_if1_init() padapter->HalData is alloc
CVE-2026-98161	In the Linux kernel, the following vulnerability has been resolved: nvdimmm: pmem: keep PREFLUSH before data writes pmem_submit_bio() records a REQ_PREFLUSH
CVE-2026-98162	In the Linux kernel, the following vulnerability has been resolved: smb/server: fix tree connection leak in smb2_tree_connect() See the procedure below: smb2_tree
CVE-2026-60096	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-60097	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-60098	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-60099	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-60100	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-60101	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-97404	In OpenStack Zaqr before 22.0.2, WSGI transport mishandles the URL-Signature header. By sending a request with an empty URL-Signature header, an unauthent
CVE-2026-56739	Logto is the modern, open-source auth infrastructure for SaaS and AI apps. Prior to 1.43.0, Logto fetches administrator-controlled outbound destinations without va
CVE-2026-67233	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.1, The shovel management resource's is_authorized/2 dele
CVE-2026-96812	Improper Exposure of Resource to Wrong Sphere in the host file helper (gofer) in Google gVisor prior to commit 573a9e73cf844f on Linux platforms with CUSE enab
CVE-2026-61742	DBHub is a database MCP server for Postgres, MySQL, SQL Server, Oracle, MariaDB, SQLite. Versions prior to 0.22.5 expose an unauthenticated HTTP MCP endpoint permissions and database credentials. Version 0.22.5 fixes the issue.
CVE-2026-61604	The ixo Blockchain is a Layer 1 blockchain that runs on both Testnet and Mainnet. Prior to version 8.0.0, the x/bonds module moved funds from an address that wa message is rejected on all routes (top-level, authz, CosmWasm, and ICA), and the bonds batch EndBlocker is a no-op so no further reserve movements can occur. A
CVE-2026-88355	An incorrect buffer size calculation vulnerability exists in tinyexpr commit 4a7456e in new_expr(). For arity-0 expression nodes, including constants, variables, and
CVE-2026-97521	In the Linux kernel, the following vulnerability has been resolved: gfs2: fix quota init duplicate scan gfs2_quota_init() checks for duplicate quota_change IDs while h
CVE-2026-97519	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix null pointer dereference in devcoredump cleanup In xe_devcoredump_snapshot_free()
CVE-2026-97518	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: reject duplicate wiphy cipher suite entries Duplicate entries in wiphy->cipher_suit
CVE-	

CVE-2026-100190	The AIL Framework crawler splash domain page (showDomain.html) is vulnerable to stored cross-site script injection (XSS). User-supplied data originating from imp
CVE-2026-100187	The Onion module in AIL Framework contained a performance shortcut in its URL extraction logic that accepted URLs as valid .onion targets based solely on a lengt processes and acts upon URLs that do not correspond to legitimate .onion services.
CVE-2026-100177	The AIL Framework crawler task creation API (api_add_crawler_task) contained an insufficient authorization check when a user supplied a cookiejar UUID to attach t
CVE-2026-95832	Improper Neutralization of Special Elements in Output Used by a Downstream Component in the colour control escape code handler in kitty from 0.47.3 before 0.49 before any credential carried in the request is checked. The reply is framed as an OSC sequence carrying the escape code number, the field name, and the literal v
CVE-2026-67238	RabbitMQ is a messaging and streaming broker. Prior to versions 4.2.7 and 4.3.1, rabbit_pid_codec:decompose_from_binary/1 parses a caller-supplied ETF-encoded
CVE-2026-98157	In the Linux kernel, the following vulnerability has been resolved: EDAC/device_sysfs: Use kstrtouint() for poll_msec to prevent truncation The poll_msec sysfs store
CVE-2026-98158	In the Linux kernel, the following vulnerability has been resolved: ppp_async: drop the errored frame instead of resetting its headroom ppp_receive_nonmp_frame(net/core/skbuff.c:214! RIP: 0010:skb_panic+0x13e/0x230 Call Trace: skb_push+0xbd/0x100 ppp_receive_nonmp_frame+0x48a/0x1d10 ppp_input+0x4e9/0x2f80 p PPP receive path with a mutating peer on a pty; it is an interesting (remote) DoS: root configures PPP, the peer supplies two crashing frames. The reproducer (repr
CVE-2026-98159	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7921: validate CLC firmware records The CLC region is supplied by firmware, but th
CVE-2026-97622	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-62062. Reason: This candidate is a reservation duplicate of CVE-2026
CVE-2026-66079	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, and 4.2.6, parse_array_primitive/2 for constructor 0x45 (list0) returns an c service. Preconditions include Network reachability to the AMQP listener (port 5672, enabled by default) No authentication required. This issue is fixed in versions 3
CVE-2026-66076	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.0, is_authorized/2 calls rabbit_mgmt_util:is_authorized/2, w
CVE-2026-66070	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.17, 4.0.22, 4.1.13, and 4.2.6, match_origin/1 returned the bare reflected Origin and allowed i
CVE-2026-96872	Improper handling of insufficient permissions or privileges vulnerability in The Wikimedia Foundation Mediawiki - WikiLambda Extension on Linux, MacOS, and Winc
CVE-2026-96770	All published s2s-proxy versions through 0.2.2 are affected. In versions 0.1.16 through 0.2.2, TLS server listeners use Go's RequireAnyClientCert mode when skipC/
CVE-2026-100070	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_nat_sip: rewind offset when NAT shrinks the packet sashiko says: If map_addr() chang
CVE-2026-100176	The AIL Framework's username timeline feature is vulnerable to stored cross-site scripting (XSS). Usernames imported from chats and crawled forums are stored w
CVE-2026-100071	In the Linux kernel, the following vulnerability has been resolved: net: hsr: free learned nodes on device setup failure hsr_dev_finalize() can fail after a lower-device
CVE-2026-100072	In the Linux kernel, the following vulnerability has been resolved: ACPI: platform: Use acpi_bus_get_primary_device() The acpi_get_first_physical_node() usage in ac
CVE-2026-100073	In the Linux kernel, the following vulnerability has been resolved: ext4: fix transaction overflow during writeback Commit 95ad8ee45cdb ("ext4: correct the reserve
CVE-2026-100074	In the Linux kernel, the following vulnerability has been resolved: bpf: Mark bpf_refcount field as unique BPF_REFCOUNT is not marked as a unique field, while it sh
CVE-2026-100076	In the Linux kernel, the following vulnerability has been resolved: staging: rtl8723bs: fix xmit_frame/xmit_buf leaks on mgnt-frame error paths issue_beacon(), issu orphaned pair is on no list and referenced by nobody, so it is only reclaimed at driver teardown. Repeated hits progressively exhaust the management-TX pools un
CVE-2026-100077	In the Linux kernel, the following vulnerability has been resolved: drm/msm: Recover HW before retire hung submit During recovery, it is not safe to retire the hung
CVE-	

CVE-2026-100078	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mei: pass correct argument to function The first argument to iwl_mei_write_cyclic_bu
CVE-2026-100079	In the Linux kernel, the following vulnerability has been resolved: usb: typec: ucsi: unregister debugfs entries on teardown ucsi_register() creates per-instance debu
CVE-2026-100172	The AIL Framework (ail-project/ail-framework) contains a stored cross-site scripting (XSS) vulnerability in two Jinja2 templates that render popovers for matched, tr affected match, tracking, or tag-related data and be delivered to users who view the affected content.
CVE-2026-100174	The AIL Framework tag selector component (var/www/static/js/tags.js) is vulnerable to stored cross-site scripting (XSS). A user with the ability to create a custom te stored (persistent) and does not require the victim to perform any action beyond loading the page. Security impact: successful exploitation allows arbitrary JavaScr
CVE-2026-98098	In the Linux kernel, the following vulnerability has been resolved: tipc: fix NULL deref in tipc_named_node_up() on empty publication list User-space applications ca Thread 2 (named_distribute) ----- ----- ... list_for_each_entry(publ, pls, binding_node) { ... __skb_queue_tail(list, skb); ... }
CVE-2026-98097	In the Linux kernel, the following vulnerability has been resolved: tipc: Dont send random pad bytes in RESET/ACTIVATE messages The interface name is passed in
CVE-2026-98095	In the Linux kernel, the following vulnerability has been resolved: af_packet: Don't cast tpacket_hdr.tp_len to int in tpacket_parse_header(). syzbot reported BUG() i 0010:sock_sendmsg_nosec+0x145/0x180 net/socket.c:803 Code: 06 67 48 0f b9 3a eb 95 e8 e8 3a 22 f8 48 89 df 4c 89 f6 4c 89 e2 4d 89 fb 2e e8 32 a5 5c 16 e9 do_syscall_x64 arch/x86/entry/syscall_64.c:61 [inline] do_syscall_64+0x166/0x520 arch/x86/entry/syscall_64.c:84 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIL
CVE-2026-98037	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject untrusted allocated-object pointers When the final RCU read-side critical section ends,
CVE-2026-98013	In the Linux kernel, the following vulnerability has been resolved: net/sched: fq_pie: clamp quantum in change path fq_pie_change() accepts any quantum value fr
CVE-2026-98014	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: E-Switch, prevent mc_list repopulation during vport disable In mlx5_esw_vport_disable(BUG: unable to handle page fault for address: 0000000003000055 down_write+0x1c/0x60 mlx5_del_flow_rules+0x33/0x1f0 [mlx5_core] esw_del_mc_addr+0x7b/0
CVE-2026-98015	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: E-Switch: fix use-after-free in mlx5_eswitch_termtbl_put In mlx5_eswitch_termtbl_put(),
CVE-2026-98016	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix use-after-free race in sample_restore_put() Concurrent teardown of TC sample rule
CVE-2026-66067	RabbitMQ is a messaging and streaming broker. Prior to versions 4.2.7 and 4.3.1, The stream open handler calls only check_vhost_access; it omits the node/vhost/
CVE-2026-98018	In the Linux kernel, the following vulnerability has been resolved: net: mctp: i3c: serialize probe with bus removal mctp_i3c_probe() drops busdevs_lock after findin
CVE-2026-98019	In the Linux kernel, the following vulnerability has been resolved: bpf: mark a NULL call argument precise check_func_arg() allows bpf_register_is_null() for nullable
CVE-2026-98020	In the Linux kernel, the following vulnerability has been resolved: pds_core: fix cmd_regs access racing BAR unmap on reset pdsc_reset_prepare() and pdsc_reset_c those are quiesced before the unmap by pdsc_fw_down(), which frees the interrupts and tears down the queues. The debugfs readers are not, since those files outl
CVE-2026-98021	In the Linux kernel, the following vulnerability has been resolved: net: reject oversized tx_queue_len at netlink parse time rtnl_create_link() assigns IFLA_TXQLEN di CONFIG_NET_SCHED=y, CONFIG_VETH=y, CONFIG_USER_NS=y, CONFIG_NET_NS=y. - Unprivileged user in a fresh user+net namespace (unshare -Urn): ip link add
CVE-2026-98022	In the Linux kernel, the following vulnerability has been resolved: net: cap tx_queue_len at S16_MAX to prevent oversized ring allocations Several subsystems alloc truncation test, and a negative ifr_qlen from the ioctl lands far above the cap after conversion, so both old failure modes are covered by the one comparison. tx_qu guest. - On the fixed kernel the oversized tx_queue_len is rejected with -ERANGE at set time (all four paths: RTM_SETLINK, RTM_NEWLINK create, sysfs, ioctl - the la
CVE-2026-53979	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-98024	In the Linux kernel, the following vulnerability has been resolved: s390/ism: folio_put() after error dmb->cpu_addr was allocated via folio_alloc(). Use folio_put() ins
CVE-2026-98025	In the Linux kernel, the following vulnerability has been resolved: net: usb: cx82310_eth: drop URB after 0xffff reboot sentinel to prevent partial_data heap overflow 61441) from the new URB's ~4KB skb, both well past their allocations, and delivers the spliced result as a 64KB "frame" to the network stack. Bail out of rx_fixup a
CVE-2026-98026	In the Linux kernel, the following vulnerability has been resolved: net: bridge: mcast: properly convert mglist to rcu Sashiko reported a bug [1] that br_multicast_de
CVE-	

CVE-2026-53978	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-98028	In the Linux kernel, the following vulnerability has been resolved: eth: nfp: drop the replaced rule from the list when reprogramming fails nfp_net_fs_add() replaces
CVE-2026-53969	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-53968	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-96873	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Mediawiki - CirrusSearch extension allows Reflected XSS. This is
CVE-2026-98032	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix subbuf resize races with trace_pipe_raw readers Concurrent subbuffer resizes may cr
CVE-2026-98033	In the Linux kernel, the following vulnerability has been resolved: bpf: Preserve inner map identity in callback frames Callback frame constructors initialize map-ty
CVE-2026-98034	In the Linux kernel, the following vulnerability has been resolved: bpf: Mark NULL kptr stores precise check_map_kptr_access() permits a scalar store into an untrus
CVE-2026-98035	In the Linux kernel, the following vulnerability has been resolved: bpf: Cancel special fields when recycling rhtab elements rhtab_map_update_existing() and rhtab_
CVE-2026-98012	In the Linux kernel, the following vulnerability has been resolved: net/sched: sfq: clamp quantum in change path sfq_change() accepts any non-negative quantum (
CVE-2026-98011	In the Linux kernel, the following vulnerability has been resolved: net/sched: hhf: clamp quantum in change and init paths hhf_change() accepts any quantum from
CVE-2026-98010	In the Linux kernel, the following vulnerability has been resolved: net/sched: drr: clamp quantum in change class drr_change_class() rejects explicit quantum==0 b
CVE-2026-97996	In the Linux kernel, the following vulnerability has been resolved: virtio: fix use-after-free in unregister_virtio_device() device_unregister() is device_del() plus put_d uml device: BUG: KASAN: slab-use-after-free in virtio_debug_device_exit+0x36/0x4d Read of size 8 at addr 00000000616e0b10 by task init/1 __asan_report_load8_
CVE-2026-97986	In the Linux kernel, the following vulnerability has been resolved: virtio_input: stop callbacks before unregistering input device virtinput_remove() unregisters the in
CVE-2026-97987	In the Linux kernel, the following vulnerability has been resolved: virtio_input: reset device if input_register_device() fails Probe marks the device DRIVER_OK with v
CVE-2026-97988	In the Linux kernel, the following vulnerability has been resolved: vhost: invalidate vring access on IOTLB transitions When VIRTIO_F_ACCESS_PLATFORM changes, i new address mode. vhost_vq_invalidate_access() clears desc, avail, and used together. Treat the VQ as invalidated only when all three are NULL, since a single GIC
CVE-2026-97989	In the Linux kernel, the following vulnerability has been resolved: vduse: validate virtqueue alignment vduse_validate_config() only checks the upper bound of vq_a __dev_change_flags+0x368/0x3b0 netif_change_flags+0x56/0xc0 do_setlink.isra.0+0x68c/0x1e30 Validate the value before it reaches the virtio ring helpers.
CVE-2026-66072	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.1, get_chunk_selector/1 calls binary_to_atom on the raw cli
CVE-2026-66069	RabbitMQ is a messaging and streaming broker. Prior to versions 4.1.13, 4.2.7, and 4.3.0, is_authorized/2 uses is_authorized_monitor for all methods. DELETE reset
CVE-2026-97992	In the Linux kernel, the following vulnerability has been resolved: vhost-vdpa: protect config_ctx from being freed under the config callback vhost_vdpa_config_cb() unprotected. With VDUSE as the parent this is reachable from userspace with access to /dev/vduse (root by default). VDUSE_DEV_INJECT_CONFIG_IRQ queues dev- vhost_vdpa_unlocked_ioctl+0x116c/0x2190 Add a spinlock covering every access to config_ctx, so the callback either signals a context that is still alive or observe
CVE-2026-97993	In the Linux kernel, the following vulnerability has been resolved: vhost-vdpa: don't install the eventfd_ctx_fdget() error in config_ctx vhost_vdpa_set_config_call() s down a config interrupt that was working: until now the swap replaced the live context and put it, so after an EBADF the device silently stopped delivering config in
CVE-2026-97994	In the Linux kernel, the following vulnerability has been resolved: vhost/vdpa: reject VRING_NUM larger than device max vhost_vring_set_num() accepts any non-ze validation, vq->num, and set_vq_num(). This ensures that validation and use operate on the same copied values.
CVE-	

CVE-2026-97995	In the Linux kernel, the following vulnerability has been resolved: virtio_console: do not free control-out buffers on remove __send_control_msg() publishes &portdev->control_out_bufs on remove, which can lead to a use-after-free if the buffers are not properly managed.
CVE-2026-97997	In the Linux kernel, the following vulnerability has been resolved: virtio_ring: fix stale descriptor flags after a failed packed add In a packed ring the AVAIL and USED pointers are updated atomically. When the driver now attempts to issue the C command, the next add starts at the same head as B. If C spans the entire ring, the next add starts at the same head as B. If C spans the entire ring, the next add starts at the same head as B.
CVE-2026-98009	In the Linux kernel, the following vulnerability has been resolved: net/sched: ets: clamp quantum in parse and fallback paths ets_qdisc_change() falls back to psched_qlen if the quantum is not set.
CVE-2026-97998	In the Linux kernel, the following vulnerability has been resolved: netfilter: nfnetlink_log: cope with concurrent instance destruction Instances are refcounted. However, if a log instance is destroyed while it is still being used by a user, it can lead to a use-after-free.
CVE-2026-98000	In the Linux kernel, the following vulnerability has been resolved: hwmon: Fix potential UAF in pec_store Sashiko reports: In pec_store(), a guard(mutex)(&hwdev->lock) is used to protect the hwmon_data structure. However, if the hwmon_data structure is freed while it is still being used by a user, it can lead to a use-after-free.
CVE-2026-98001	In the Linux kernel, the following vulnerability has been resolved: hwmon: (ltc4282) Make sure clk_init_data is fully initialized The clk_init_data structure contains several fields that are used to initialize the clock driver. If these fields are not properly initialized, it can lead to a use-after-free.
CVE-2026-66068	RabbitMQ is a messaging and streaming broker. Prior to versions 3.13.15, 4.0.20, 4.1.11, 4.2.6, and 4.3.0, ?LOG_DEBUG("shutting down Shovel '~ts', ... Shovel statistics are updated. This can lead to a use-after-free if the statistics are not properly managed.
CVE-2026-98003	In the Linux kernel, the following vulnerability has been resolved: iommu/amd: Do not reallocate GA log buffers on resume Commit c5e1a1eb9279 ("iommu/amd: Stop using GA log buffers for resume") introduced a vulnerability where the GA log buffers were not properly managed during resume, leading to a use-after-free.
CVE-2026-98004	In the Linux kernel, the following vulnerability has been resolved: iommu/riscv: Serialize command queue publishing Serialize command queue publishing so software can safely access the command queue without race conditions.
CVE-2026-98005	In the Linux kernel, the following vulnerability has been resolved: erofs: delimit inode_share cache key components Previously, inode_share keys were encoded as a single string, which could lead to a use-after-free if the keys were not properly managed.
CVE-2026-98006	In the Linux kernel, the following vulnerability has been resolved: ALSA: caiaq: Decoupling ep1_in_urb in caiaq dev The epq_in_urb object belonging to the caiaq device is freed when the device is removed. However, if the device is removed while it is still being used by a user, it can lead to a use-after-free.
CVE-2026-98007	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject non-scalar bpf_loop iteration counts bpf_loop() declares its nr_loops argument as ARG_PTR_TO_CONST_LEN, which means it should only accept scalar values.
CVE-2026-98008	In the Linux kernel, the following vulnerability has been resolved: net: macb: fix NULL pointer dereference on unbind with fixed-link When the device tree describes a fixed-link, the driver should not dereference a NULL pointer.
CVE-2026-98036	In the Linux kernel, the following vulnerability has been resolved: bpf: Preserve special fields in recycled rhtab elements rhtab_map_update_elem() initializes special fields in recycled elements. However, if these fields are not properly managed, it can lead to a use-after-free.
CVE-2026-98038	In the Linux kernel, the following vulnerability has been resolved: bpf: Keep refcount_acquire nullable for borrowed RCU kptrs bpf_refcount_acquire() is fallible for a borrowed RCU kptr, which means it should return an error if the refcount is not properly managed.
CVE-2026-98094	In the Linux kernel, the following vulnerability has been resolved: staging: fbft: make dirty_lock IRQ-safe fbft_mkdirty() can be reached from the fbcon rendering process, which can lead to a race condition if the dirty_lock is not properly managed.
CVE-2026-98039	In the Linux kernel, the following vulnerability has been resolved: bpf: Require MEM_PERCPU for percpu kptr stores map_kptr_match_type() treats perm_flags as the permission flags for a percpu kptr, which means it should require MEM_PERCPU.
CVE-2026-87899	Execution with unnecessary privileges in cPanel allows remote authenticated users to execute arbitrary code with root privileges.
CVE-2026-87898	OS command injection in Plesk allows remote authenticated users to execute arbitrary code with root privileges.
CVE-2026-98071	In the Linux kernel, the following vulnerability has been resolved: net/rds: clear cp_flags bits individually in rds_conn_path_reset() rds_conn_path_reset() wipes the connection path flags, which can lead to a race condition if the flags are not properly managed.
CVE-2026-98072	In the Linux kernel, the following vulnerability has been resolved: net/rds: use wq_has_sleeper() in release_in_xmit() release_in_xmit() clears RDS_IN_XMIT with clear_bit_unlock() until commit 1422f28826d2 ("rds: introduce acquire/release ordering in acquire/release_in_xmit()") folded both into clear_bit_unlock(), which can lead to a race condition.
CVE-2026-98074	In the Linux kernel, the following vulnerability has been resolved: bonding: do not clear curr_active_slave prematurely when releasing all slaves When releasing all slaves, the driver should not clear curr_active_slave prematurely, which can lead to a race condition.
CVE-2026-98075	In the Linux kernel, the following vulnerability has been resolved: bpf: reject BPF_PSEUDO_FUNC reference to the main program fixups.c:jit_subprogs() rewrites BPF_PSEUDO_FUNC references to the main program, which can lead to a race condition.

98075	
CVE-2026-98076	In the Linux kernel, the following vulnerability has been resolved: tracing/probes: Fix use-after-free on field name/type of events with multiple probes The fields of probe list is not empty. The event call stays registered via B while its fields now reference freed memory. Any field lookup then reads it, e.g. echo 'a1 == 1' > ever
CVE-2026-98077	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_contrack_sip: fix OOB read in sip_skip_whitespace() sip_skip_whitespace() returns d
CVE-2026-98078	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix reversed sequence option serialization hton_seq() expects the host-order source first and
CVE-2026-98079	In the Linux kernel, the following vulnerability has been resolved: btrfs: zstd: fix lost wakeup when waiting for a workspace A writer can sleep forever in zstd_get_w
CVE-2026-98080	In the Linux kernel, the following vulnerability has been resolved: btrfs: do not force reloc root creation during qgroup_account_snapshot() [BUG] When running btr btrfs_run_delayed_refs+0x9d/0xf0 [btrfs 32f09462c54d9c922fca74a3e4866f4aa7737b72] create_pending_snapshot+0x39d/0xf00 [btrfs 32f09462c54d9c922fca74 175 free space 5953 owner 2 BTRFS info (device dm-2): refs 3 lock_owner 2173 current 2173 item 0 key (166772736 METADATA_ITEM 1) itemoff 16250 itemsize 3: 18446744073709551615 BTRFS error (device dm-2): Ref action 3, root 273, ref_root 273, parent 0, owner 0, offset 0, num_refs 1 btrfs_force_cow_block+0x129/0x
CVE-2026-98081	In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: finish active block group cleanup if call_zone_finish() fails do_zone_finish() clears BL
CVE-2026-98082	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix the possible bioc_list memory leak during error There are two possible ways to leak bioc
CVE-2026-98084	In the Linux kernel, the following vulnerability has been resolved: bpf: backtracking shouldn't clear outer frame R1-R5 for callbacks When processing calls to bpf_lo conflicts when 'bpf' would be eventually merged with 'bpf-next'.
CVE-2026-98085	In the Linux kernel, the following vulnerability has been resolved: bpf: backtrack_insn(): Handle ld_{abs,ind} subprog exit edge Nicholas Carlini reported a bug in p
CVE-2026-98086	In the Linux kernel, the following vulnerability has been resolved: ALSA: ump: do not touch legacy_rmidi before it exists snd_ump_parse_endpoint() sets ump->pars
CVE-2026-98087	In the Linux kernel, the following vulnerability has been resolved: sched/rt,dl: Skip migrate-disabled tasks when picking a push candidate A migrate_disable()'d RT t equal priority shared the CPU, taskA migrate_disable()'d and queued, taskB as rq->curr. In one 89 ms window, taskB got only 52 ms of CPU. The other 37 ms went it preempts taskB v re-check compares taskB against the pushable head, which is still taskA -> give up v nothing moved, taskA still queued, rq still overlo works. But the runqueue is still marked overloaded, because the pinned task is still advertised as pushable. Other CPUs now send the push-IPIs during their own RT
CVE-2026-98088	In the Linux kernel, the following vulnerability has been resolved: scsi: mpt3sas: Avoid out-of-bounds cpumask_of_node() call in _base_assign_reply_queues() dev_t
CVE-2026-98089	In the Linux kernel, the following vulnerability has been resolved: bonding: alb: fix uninitialized transport header access in alb_determine_nd() alb_determine_nd() i
CVE-2026-98090	In the Linux kernel, the following vulnerability has been resolved: btrfs: restore active device pointers after failed sprout btrfs_init_new_device() switches latest_dev
CVE-2026-98091	In the Linux kernel, the following vulnerability has been resolved: btrfs: detach failed sprout device from transaction update list When creating the first metadata c
CVE-2026-98092	In the Linux kernel, the following vulnerability has been resolved: ASoC: amd: yc: fix memory leak in acp6x_pdm_dma_close() acp6x_pdm_dma_close() does not fre
CVE-2026-98093	In the Linux kernel, the following vulnerability has been resolved: ASoC: fsl_micfil: balance mclk enable/disable hw_params() enables mclk unconditionally and hw_
CVE-2026-98068	In the Linux kernel, the following vulnerability has been resolved: net/rds: don't let rds_conn_shutdown() consume a concurrent drop rds_conn_shutdown() finishes RDS_CONN_ERROR between that claim and the state check that follows, which accepts RDS_CONN_ERROR. The accept then installs the freshly accepted socket wit RDS_CONN_ERROR, a drop raced the teardown: cancel the reconnect timer and clear RDS_RECONNECT_PENDING - the one piece of the skipped tail that must not b without noisy logging. Any other state keeps today's rds_conn_path_error() handling; no current cp_state writer can leave a DISCONNECTING path in anything but f
CVE-2026-98067	In the Linux kernel, the following vulnerability has been resolved: erofs: disable LZ4 rolling decompression for now LZ4 rolling decompression [1] was introduced to comparison even when the source and destination ranges do not overlap (IOWs, inline decompression doesn't need to be considered here). That breaks the rolling
CVE-2026-98066	In the Linux kernel, the following vulnerability has been resolved: ALSA: caiaq: Fix potential double-free at error path The fix for caiaq driver's resource managemen
CVE-2026-98053	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: avs: Refactor and fix init_config access Existing code accesses enties found in ->init_

CVE-2026-98040	In the Linux kernel, the following vulnerability has been resolved: bpf: Mark the zero register precise for a register-form NULL check check_cond_jump_op() accepts '0' as a valid register value
CVE-2026-98042	In the Linux kernel, the following vulnerability has been resolved: bpf: Don't resurrect a scalar id dropped by collect_linked_regs() check_cond_jump_op() copies the id of a register that has been dropped by collect_linked_regs()
CVE-2026-98043	In the Linux kernel, the following vulnerability has been resolved: bpf: Don't infer non-NULL from a pointer with an unbounded offset reg_not_null() decides that a register is non-NULL if it has a non-zero offset
CVE-2026-98044	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject legacy packet loads from callbacks check_id_abs() models a failed BPF_LD_ABS or BPF_LD_ABS+KPTR. Also check the complete subprogram call graph during stack-depth validation and reject a function containing a legacy load when any caller is a callback. This covers the case where a legacy load is used in a callback that is called from a function that is called from a callback
CVE-2026-98045	In the Linux kernel, the following vulnerability has been resolved: bpf: Mark faultable stack helpers as sleepable The faultable variants of bpf_get_stack() and bpf_get_stackid() can sleep
CVE-2026-98046	In the Linux kernel, the following vulnerability has been resolved: bpf: Mark bpf_btf_find_by_name_kind() as sleepable When bpf_btf_find_by_name_kind() finds a type, it may sleep
CVE-2026-98047	In the Linux kernel, the following vulnerability has been resolved: bpf: Check ancestor frames for rbtree callbacks bpf_rbtree_add() invokes its comparator while the rbtree is locked
CVE-2026-98048	In the Linux kernel, the following vulnerability has been resolved: bpf: don't rewrite bpf_fastcall patterns entered by a jump mark_fastcall_pattern_for_call() must ensure that the jump is not rewritten
CVE-2026-98049	In the Linux kernel, the following vulnerability has been resolved: bpf: zero extend the result of an arena 32-bit cmpxchg bpf_convert_ctx_accesses() rewrites an atomic compare-and-swap to a 32-bit compare-and-swap
CVE-2026-98051	In the Linux kernel, the following vulnerability has been resolved: net: bcmasp: fix tx_spb_ring_full() checking same slot cnt times The loop initialised next_index from 0 and incremented it until it reached cnt, but it should have started from 1
CVE-2026-98054	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: avs: Fix unbalanced module reference count strace_open() invokes try_module_get() but does not call module_put()
CVE-2026-98065	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject key-less BTF for hash maps map_check_btf() allows a key-less BTF (btf_key_type_id = 0) to be used in a hash map. RBP: 0000000000000000 R08: 0000000000000001 R09: 0000000000000000 R10: fffff9000399f970 R11: 0000000000000001 R12: ffffffff9b9b9b9b fs/read_write.c:769 do_syscall_x64 arch/x86/entry/syscall_64.c:61 [inline] do_syscall_64+0x123/0x790 arch/x86/entry/syscall_64.c:84 entry_SYSCALL_64_after_hwdef
CVE-2026-98055	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: avs: Clean up the bus when fetching ML caps fails snd_hdac_ext_bus_get_ml_capabilities() does not call snd_hdac_ext_bus_put_capabilities()
CVE-2026-87900	Argument injection in WP Toolkit for cPanel 6.11.2-10794 and earlier allows remote authenticated users to read arbitrary files and execute arbitrary code across cPanel accounts via the WP Toolkit
CVE-2026-98057	In the Linux kernel, the following vulnerability has been resolved: ring-buffer: Add checking nr_subbufs to persistent ring buffer validation Sashiko reported that the ring buffer validation logic was incorrect
CVE-2026-98058	In the Linux kernel, the following vulnerability has been resolved: bpf: Mark syscall helpers as sleepable bpf_sys_bpf() executes the bpf(2) syscall body, which can sleep
CVE-2026-98059	In the Linux kernel, the following vulnerability has been resolved: bpf: Mark sched_process_wait argument as nullable do_wait() passes wo->wo_pid to the sched_process_wait() helper
CVE-2026-98060	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject resilient lock operations in rbtree callbacks __bpf_rbtree_add() keeps parent and link pointers in the rbtree
CVE-2026-98061	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject tail calls directly from callback frames A tail call from a non-zero frame is modeled as a jump to the end of the frame
CVE-2026-98062	In the Linux kernel, the following vulnerability has been resolved: bpf: Mark signal tracepoint siginfo arguments as scalar The signal_generate and signal_deliver tracepoints take siginfo_t arguments
CVE-2026-98063	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix NULL-ptr-deref in btf_var_show() btf_var_show() calls btf_type_id_resolve() unconditionally, but btf_modifier_show() does not
CVE-2026-98064	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix NULL-ptr-deref when showing a void BTF type btf_modifier_show() resolves the modifier and btf_df_show() when the resolved type has no show op; it emits the "<unsupported kind:N>" placeholder already used for kinds like FWD and FUNC. bpf_snprintf_btf() does not check for NULL

CVE-
2026-
98031

In the Linux kernel, the following vulnerability has been resolved: nexthop: Initialize extack in remove_nh_grp_entry() remove_nh_grp_entry() prints the extack mes