SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 08 July 2026

Generated on 08 July 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-2026-48316	ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	10.0	More Details
CVE-2026-57572	Crawl4AI is an open-source LLM-friendly web crawler and scraper. Prior to 0.9.0, the Docker API server accepted request-supplied browser_config.extra_args, which flowed into Chromium's launch arguments. An attacker could inject Chromium switches that replace a child-process launch command together with --no-zygote, causing Chromium to fork or exec an attacker-controlled command as the container's runtime user. The Docker API is unauthenticated by default, so a single request yields arbitrary command execution. This issue is fixed in version 0.9.0.	10.0	More Details
CVE-2026-57624	Unauthenticated Remote Code Execution (RCE) in Blocksy Companion Pro <= 2.1.46 versions.	10.0	More Details
CVE-2026-13768	Gardyn devices expose a privileged iothubowner key. Access to this key will allow a malicious user to invoke an IoTHub Registry Manager function which returns connection information for all Gardyn Home Kit and Studio devices. Access to this key also allows a malicious user to execute arbitrary commands on a specific connected device and may allow the malicious user to pivot to other devices on the user's network.	10.0	More Details
CVE-2026-56004	A shellcode injection in the mercurial handler of the obs tar_scm source service before version 0.12.4 could be used by attackers able to provide a _service file to execute code as the source service or the local user checking out the malicious services	10.0	More Details
CVE-2026-50160	Hoppscotch is an API development ecosystem. In self-hosted deployments of hoppscotch-backend from version 2026.4.1 and earlier, the unauthenticated POST /v1/onboarding/config endpoint is vulnerable to mass assignment. The global NestJS ValidationPipe is configured without whitelist: true, so extra properties on the request body that are not declared in SaveOnboardingConfigRequest are not stripped and are iterated in the service layer as if they were legitimate InfraConfig entries. Because keys such as JWT_SECRET and SESSION_SECRET are valid InfraConfigEnum values and are not explicitly rejected during validation, an unauthenticated attacker who can reach a fresh instance before onboarding completes (or when no users exist) can overwrite these values in the database. Overwriting JWT_SECRET gives the attacker control of the JWT signing key, allowing them to forge tokens for any user, including administrators, and results in full server compromise. The issue is fixed in hoppscotch 2026.5.0.	10.0	More Details

CVE-2026-50746	A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi Connect Application to execute a Command Injection on the host device.	10.0	More Details
CVE-2026-50747	A malicious actor with access to the network and low privileges could exploit a series of authenticated SQL Injection vulnerabilities found in UniFi Talk Application to escalate privileges on the host device.	9.9	More Details
CVE-2026-50195	containerd is an open-source container runtime. Versions prior to 2.3.2, 2.2.5 and 2.1.9 contain a vulnerability in the CRI checkpoint import process where it fails to validate the image references specified within a checkpoint image's configuration. An attacker with permissions to create pods can use a crafted checkpoint image to force containerd to pull a malicious image and assign it an arbitrary local tag, thereby poisoning the node's local image cache. Subsequently, if other pods on the same node attempt to use the poisoned tag with an IfNotPresent (or Never) pull policy, they will unknowingly execute the attacker's malicious image instead of the legitimate one. This can lead to a compromise of the affected pods, allowing the attacker to execute arbitrary code under the victim pod's identity. This issue has been fixed in versions 2.3.2, 2.2.5 and 2.1.9.	9.9	More Details
CVE-2026-45499	Server-side request forgery (ssrf) in Azure OpenAI allows an authorized attacker to elevate privileges over a network.	9.9	More Details
CVE-2026-44935	Missing validation of "valuesFrom" references in Helm Deployer of SUSE Rancher Fleet 0.15 before 0.15.2, 0.14 before 0.14.6, 0.13 before 0.13.11 and 0.12 before 0.12.15 could be used by owners of one tenant to access fleet credentials of other tenants.	9.9	More Details
CVE-2026-50748	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi Access Application to execute a Command Injection on the host device.	9.9	More Details
CVE-2026-27419	Subscriber Arbitrary File Upload in Zegen <= 1.1.9 versions.	9.9	More Details
CVE-2026-40141	A high-severity vulnerability exists in a web application component of BeyondTrust Remote Support and Privileged Remote Access related to the processing of certain input parameters. Insufficient validation of user-supplied input may allow an authenticated attacker with limited privileges to access unintended resources or data beyond their authorization scope. Exploitation is restricted to accounts with specific permissions.	9.9	More Details
CVE-2026-48614	An improper authorization vulnerability in the Plesk XML API allows an authenticated user to inject arbitrary configuration directives, resulting in arbitrary file write as root and full privilege escalation on the underlying server.	9.9	More Details
CVE-2026-34038	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.469, an authenticated remote command injection vulnerability in application deployment handling allows users with application write permissions to achieve remote code execution and exfiltrate sensitive environment variables through deployment logs via fields such as dockerfile_location and deployment commands. This issue is fixed in version 4.0.0-beta.469.	9.9	More Details
CVE-2026-34037	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.464, the cloneTo() Livewire action in ResourceOperations.php authorizes the source resource but resolves destination resources with unscoped Eloquent lookups, allowing an authenticated user to clone resources into destinations owned by other teams and access cross-tenant resources. This issue is fixed in version 4.0.0-beta.464.	9.9	More Details
CVE-2026-34047	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, terminal WebSocket bootstrap routes did not enforce the expected authorization middleware, allowing an authenticated user to access terminal functionality for resources outside the authorized scope and potentially execute commands. This issue is fixed in version 4.0.0-beta.471.	9.9	More Details
CVE-2026-34048	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, terminal websocket bootstrap routes only check authentication and do not enforce terminal authorization, allowing a low-privileged team member to connect to terminal routes and execute commands on team servers. This issue is fixed in version 4.0.0-beta.471.	9.9	More Details
CVE-2026-55115	A malicious actor with access to the network and low privileges could exploit a Server-Side Request Forgery (SSRF) in UniFi Protect Application to escalate privileges on the host device.	9.9	More Details
CVE-2026-54402	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi OS to execute a Command Injection on the host device.	9.9	More Details
CVE-2026-57100	Server-side request forgery (ssrf) in Microsoft Entra Provisioning Service (SyncFabric) allows an authorized attacker to elevate privileges over a network.	9.9	More Details
	A use-after-free vulnerability exists in libcurl when an application configures an HTTP/2 stream-dependency tree via `CURLOPT_STREAM_DEPENDS` or `CURLOPT_STREAM_DEPENDS_E`, subsequently		

CVE-2026-10536	invokes `curl_easy_reset()`, and finally terminates the handle with `curl_easy_cleanup()`. During this final cleanup phase, libcurl attempts to access and modify an internal structure that was already freed during the reset operation.	9.8	More Details
CVE-2026-9079	libcurl had a flaw that when instructed to clear proxy authentication credentials which made it not do so, leaving the old credentials around to get used for subsequent transfers that should not know nor use them.	9.8	More Details
CVE-2026-8925	The curl logic that works with SASL authentication could end up cleaning up the GSASL context *twice* without clearing the pointer in between, making it `free()` the same pointer twice.	9.8	More Details
CVE-2026-11856	Successfully using libcurl to do a transfer to a specific HTTP origin (`hostA`) with **Digest** authentication and then changing the origin to a different one (`hostB`) for a second transfer, reusing the same handle, makes libcurl wrongly pass on the `Authorization:` header field meant for `hostA`, to `hostB`.	9.8	More Details
CVE-2024-14037	Redsea Cloud eHR contains an arbitrary file upload vulnerability that allows unauthenticated attackers to achieve remote code execution by uploading malicious files through the PtFjk.mob servlet endpoint. Attackers can submit a multipart POST request with a JSP webshell disguised using a spoofed image/jpeg Content-Type to bypass the absence of extension and MIME type validation, with the uploaded file stored at a predictable path under the uploadfile directory and executed directly by the web server. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-11-03 (UTC).	9.8	More Details
CVE-2026-5524	The Divi Form Builder plugin for WordPress is vulnerable to Arbitrary File Upload leading to Remote Code Execution in all versions up to and including 5.1.8. This is due to insufficient file extension validation in the do_image_upload() function where user-supplied input from the acceptFileTypes POST parameter is directly interpolated into a regular expression used to validate uploaded files. Attackers can specify PHP-executable extensions such as .phtml, .phar, .php5, or .php7 to bypass the plugin's .htaccess protection which only blocks .php files specifically. Additionally, on Nginx-based servers, the .htaccess protection is completely ineffective as Nginx does not process .htaccess files. This makes it possible for unauthenticated attackers (who can obtain a nonce from any public page containing a form) to upload executable PHP files to the publicly accessible /wp-content/uploads/de_fb_uploads/ directory and achieve Remote Code Execution by accessing the uploaded file via HTTP. The vulnerability was partially patched in version 5.1.3.	9.8	More Details
CVE-2026-38968	ntopng through 6.6 is vulnerable to Predictable Session Identifier which can lead to Session Hijacking. HTTP session identifiers in src/HTTPserver.cpp use weak time-seeded pseudo-randomness during session creation. As a result, fresh authenticated logins can receive deterministic or colliding session cookies under attacker-controlled timing.	9.8	More Details
CVE-2026-58466	AutoBangumi before 3.2.8 contains a hard-coded default credentials vulnerability that allows unauthenticated attackers to authenticate as the administrator by using the publicly known default credentials seeded at startup via add_default_user() in the database user module when the users table is empty. Attackers can submit the default credentials to the authentication login endpoint to gain full control of the application, including RSS feed configuration, downloader configuration, and all authenticated API endpoints.	9.8	More Details
CVE-2026-58455	Dockwatch through 0.6.567 contains an unauthenticated OS command injection vulnerability that allows remote attackers to execute arbitrary shell commands by exploiting a missing exit() after an authentication redirect in loader.php combined with unsanitized input passed to shell_exec() in ajax/compose.php. Attackers can seed the required session flag through the incomplete auth check, then inject arbitrary commands via the composePath POST parameter in the composePull action to achieve full host compromise, facilitated by the standard deployment mounting of the Docker socket.	9.8	More Details
CVE-2026-14544	A flaw was found in HPLIP (HP Linux Imaging and Printing Software). This vulnerability, an incomplete fix for CVE-2026-8631, may allow a remote attacker to escalate privileges or achieve arbitrary code execution. This can occur through an integer overflow in the hpcups processing path when handling specially crafted print data.	9.8	More Details
CVE-2026-4767	Missing authentication for critical function vulnerability in TR7 Cyber Defense Inc. WAF-ASP allows Authentication Abuse. This issue affects WAF-ASP: from v1.0.324.900 before v1.4.0.117.	9.8	More Details
CVE-2022-50973	Yonyou KSOA 9.0 contains an unauthenticated arbitrary file upload vulnerability in the com.sksoft.bill.ImageUpload servlet that allows unauthenticated attackers to upload arbitrary files by submitting a POST request with attacker-controlled filepath and filename parameters without any authentication, file type, extension, or content validation. Attackers can upload a JSP webshell by specifying a malicious filename and root filepath, with the uploaded file stored under the pictures directory and directly executed by the web server, resulting in unauthenticated remote code execution. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-11-07 (UTC).	9.8	More Details
CVE-2026-58422	Improper authorization on OAuth sign-in callback silently re-enables administrator-disabled accounts	9.8	More Details

CVE-2026-4321	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Raera - Ankara Web Design and Digital Advertising Agency Destekz allows SQL Injection. This issue affects Destekz: through 02062026. NOTE: The vendor was contacted and it was learned that the product is not supported.	9.8	More Details
CVE-2026-56140	Improper Input Validation vulnerability in Apache Camel AWS SNS component. The camel-aws2-sns component filters Camel headers through a component-specific HeaderFilterStrategy, Sns2HeaderFilterStrategy. Like the sibling Sqs2HeaderFilterStrategy, it originally configured only an outbound filter (setOutFilterPattern, which blocks Camel*, breadcrumbId and org.apache.camel.* headers from being written out) and did not configure an inbound filter rule. For the related camel-aws2-sqs component this inbound gap was exploitable, because the Sqs2Consumer maps inbound SQS message attributes into the Camel Exchange via HeaderFilterStrategy.applyFilterToExternalHeaders, allowing a message sender to inject Camel control headers (tracked as CVE-2026-46456). camel-aws2-sns, by contrast, is producer-only: Sns2Endpoint does not support consumers (createConsumer throws UnsupportedOperationException, 'You cannot receive messages from this endpoint'), so no externally-supplied message attributes are ever mapped inbound into a Camel Exchange through SNS, and the missing inbound filter rule on Sns2HeaderFilterStrategy was therefore not reachable by an attacker. As part of the same fix (CAMEL-23506), an inbound filter rule (setInFilterStartsWith for the Camel namespace) was added to Sns2HeaderFilterStrategy so that its configuration matches the corrected Sqs2HeaderFilterStrategy and the other sibling strategies. This is a defense-in-depth alignment with no known exploit path in camel-aws2-sns. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. This is a defense-in-depth hardening change with no known exploit path in camel-aws2-sns, which is producer-only, so no urgent action or workaround is required. Users who want the aligned behaviour can upgrade to version 4.21.0, or to 4.14.8 on the 4.14.x LTS releases stream, or to 4.18.3 on the 4.18.x releases stream, which contain the change. As a general best practice, operators should continue to apply least-privilege IAM permissions on their SNS topics.	9.8	More Details
CVE-2026-59800	9Router before 0.4.44 contains an OS command injection vulnerability in the unauthenticated POST /api/tunnel/tailscale-install endpoint (this route is not covered by the dashboard middleware matcher, so no authorization check is applied). The sudoPassword field from the request body is written to the stdin of a 'sudo -S sh' child process. When sudo does not prompt for a password (the process runs as root, NOPASSWD is configured, or a recent sudo timestamp cache exists), the sudoPassword value is interpreted by sh as a shell command, allowing a remote unauthenticated attacker to execute arbitrary OS commands. Exploitation evidence was first observed by the Shadowserver Foundation on 2026-07-04 (UTC).	9.8	More Details
CVE-2026-13019	Esri Portal for ArcGIS versions 12.1 and earlier on Windows, Linux and Kubernetes have a missing authentication for critical function vulnerability allows a remote, unauthenticated attacker to access an unprotected API.	9.8	More Details
CVE-2026-53483	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 an improper authentication vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. This is a critical severity vulnerability as it allows an attacker to take complete control of system; so Dell recommends customers to upgrade at the earliest opportunity.	9.8	More Details
CVE-2026-53481	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access to the system. This is a critical severity vulnerability as it allows an attacker to take complete control of system; so Dell recommends customers to upgrade at the earliest opportunity.	9.8	More Details
CVE-2011-10043	Module::Load versions before 0.22 for Perl allow arbitrary modules outside of @INC to be loaded. Module names starting with "::" could be passed to the load function to specify arbitrary module paths. Attackers able to influence module names passed to load could use that bug to execute arbitrary code.	9.8	More Details
CVE-2026-33264	A bug in `BaseSerialization.deserialize()` allowed unrestricted `import_string()` of attacker-controlled class paths when the Scheduler / API Server loaded a serialized DAG: a DAG author could embed a malicious trigger into a DAG to gain remote code execution on the API Server / Scheduler process, crossing the Airflow security boundary that DAG-author code must never execute in those processes. Users are advised to upgrade to `apache-airflow` 3.3.0 or later. As a defense-in-depth mitigation, deployments where DAG-author trust is limited can restrict the `[core] allowed_deserialization_classes` config to a narrow allowlist.	9.8	More Details
	The WPFunnels – Funnel Builder for WooCommerce with Checkout & One Click Upsell plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 3.12.7 via the 'postData' parameter parameter. This is due to unsanitized write of attacker-controlled postData values		

CVE-2026-14345	into a PHP-includeable .log file combined with the use of include_once to render that file in wpfnl_show_log. This makes it possible for unauthenticated attackers to execute code on the server. Exploitation requires that the Log Settings "Enable Logs" toggle is on and that an administrator subsequently opens the polluted log file via the plugin's Log Settings View UI; however, the nonce required to reach the optin endpoint is publicly emitted on every funnel step page, so the injection step itself is fully unauthenticated.	9.8	More Details
CVE-2026-12375	The uncanny-automator-pro WordPress plugin before 7.3.0.6 was distributed with malicious code after the vendor's uncanny-automator-pro WordPress plugin before 7.3.0.6 update/distribution infrastructure was compromised; the injected backdoor grants unauthenticated attackers an administrator session on affected sites and beacons the site's secret keys and administrator details to attacker-controlled servers.	9.8	More Details
CVE-2026-9181	ArcGIS Server contains a directory traversal vulnerability. An unauthenticated attacker could exploit this issue by sending crafted path parameters. Successful exploitation could allow access to sensitive files on the system. This issue impacts all versions of ArcGIS Server 12.0 and prior.	9.8	More Details
CVE-2026-40139	A critical pre-authentication vulnerability exists in the authentication subsystem of BeyondTrust Remote Support. Improper processing of authentication requests may allow an unauthenticated remote attacker to bypass access controls and gain unauthorized access to the appliance, including accounts with elevated privileges. Exploitation requires a specific authentication configuration to be enabled.	9.8	More Details
CVE-2026-53913	Improper Authentication, Missing Authentication for Critical Function, Not Failing Securely ('Failing Open') vulnerability in Apache Camel Keycloak Component. The KeycloakSecurityPolicy of camel-keycloak guards a route by running KeycloakSecurityProcessor.beforeProcess(), which performs three checks in sequence: it rejects a request that carries no access token, then - only if requiredRoles is non-empty - validates the roles, and - only if requiredPermissions is non-empty - validates the permissions. The actual cryptographic verification of the bearer access token (signature, issuer and expiry for a local JWT, or active-state and issuer for token introspection) is performed exclusively inside those role and permission checks. KeycloakSecurityPolicy defaults requiredRoles and requiredPermissions to empty - which is the documented 'Basic Setup' - so on a route configured that way the role and permission checks are skipped and the access token is therefore never verified. The token-presence check still rejects a missing token, but an invalid token is accepted: any non-null value in the Authorization: Bearer header - including an arbitrary string or a forged, unsigned JWT - passes the policy and the request reaches the protected route, with no signature, issuer or expiry check and no request to Keycloak. The token is read from the inbound request header because allowTokenFromHeader defaults to true. Because the normal reason to place a route behind this policy is that the route performs server-side work, the bypass results in unauthenticated access to that work; where the protected route forwards to a code-execution-capable producer, it can result in unauthenticated remote code execution. This defect is independent of CVE-2026-23552: that issue concerned the issuer claim and was fixed by adding a check inside the verification routine, but here the verification routine is not reached at all in the default configuration, so the defect remains. This issue affects Apache Camel: from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. For deployments that cannot upgrade immediately, configure a non-empty requiredRoles or requiredPermissions on every KeycloakSecurityPolicy so that the token-verification path is exercised, set allowTokenFromHeader to false where the token is not expected from the request header, or perform token verification at the framework layer ahead of the policy.	9.8	More Details
CVE-2026-20896	Gitea Docker image versions up to and including 1.26.2 use REVERSE_PROXY_TRUSTED_PROXIES=* by default, allowing any source IP to impersonate a user when reverse-proxy authentication headers such as X-WEBAUTH-USER are enabled.	9.8	More Details
CVE-2026-48204	Improper Input Validation, Improper Access Control vulnerability in Apache Camel in Camel Mongodb Gridfs component. The camel-mongodb-gridfs producer selects the GridFS operation to perform from the gridfs.operation Exchange header when the endpoint's operation parameter is not set - which is the default. The control-header constants (GridFsConstants.GRIDFS_OPERATION, GRIDFS_OBJECT_ID, GRIDFS_METADATA, GRIDFS_CHUNKSIZE, GRIDFS_FILE_ID_PRODUCED) were the plain strings gridfs.operation, gridfs.objectid, gridfs.metadata, gridfs.chunksize and gridfs.fileid. Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that bridges an HTTP consumer (for example platform-http) into a mongodb-gridfs: producer with no explicit operation, any HTTP client could therefore set the gridfs.operation header to override the route's intended operation - switching, for example, a file upload to remove (deleting a file identified by the attacker-supplied gridfs.objectid), listAll (enumerating every file in the bucket) or findOne (reading a file) - and supply a gridfs.metadata value that is parsed as a MongoDB document, enabling NoSQL operator injection. No credentials are required when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that drive GridFS operations or metadata via the raw header names must use	9.8	More Details

	CamelGridFsOperation / CamelGridFsObjectId / CamelGridFsMetadata / CamelGridFsChunkSize / CamelGridFsFileId instead of the gridfs.* names. For deployments that cannot upgrade immediately, set an explicit operation on the mongodb-gridfs: endpoint so the operation is not taken from a header, and strip the gridfs.* headers from any untrusted ingress before the producer.		
CVE-2026-46456	Improper Input Validation vulnerability in Apache Camel AWS2-SQS Component. The camel-aws2-sqs component map inbound message attributes into the Camel Exchange through a component-specific HeaderFilterStrategy. Sqs2HeaderFilterStrategy configured only an outbound filter (setOutFilterPattern, which blocks Camel*, breadcrumbId and org.apache.camel.* headers being written to the broker) but did not configure an inbound filter. As a result, when Sqs2Consumer copies each SQS MessageAttribute into the Exchange via HeaderFilterStrategy.applyFilterToExternalHeaders, DefaultHeaderFilterStrategy applied no inbound rule and treated every header name as not filtered - including Camel-internal control headers such as CamelHttpUri, CamelFileName or CamelSqlQuery - copying them unmodified onto the Camel message. Any principal able to send messages to the consumed SQS queue (for example a cross-account sender or a lower-privileged in-account component holding sqs:SendMessage) could therefore set arbitrary Camel control headers that influence the behaviour of downstream producers in the route (for example redirecting an HTTP producer, changing a file name, or overriding a query); the injected headers also persist across internal direct, seda and vm hops. The concrete downstream impact depends on which producers the route uses. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix adds an inbound HeaderFilterStrategy rule to Sqs2HeaderFilterStrategy that filters the Camel header namespace case-insensitively on inbound mapping, so sender-supplied Camel* / camel* headers are no longer copied into the Exchange. For deployments that cannot upgrade immediately, strip the Camel control headers from inbound messages before they reach any downstream producer (for example removeHeaders('Camel*') and removeHeaders('camel*') at the start of the route), and restrict who may send to the consumed SQS queue by applying least-privilege sqs:SendMessage permissions on the queue resource policy.	9.8	More Details
CVE-2026-46455	Insufficient Session Expiration vulnerability in Apache Camel Keycloak Component. The camel-keycloak security helper KeycloakSecurityHelper.parseAndVerifyAccessToken builds a Keycloak TokenVerifier using withChecks(...) with only the subject-exists check and the realm-URL (issuer) check. Keycloak's TokenVerifier.withChecks(...) appends to an initially empty check list - the upstream default checks are installed only when withDefaultChecks() is called - so the built-in IS_ACTIVE predicate, which validates the token's exp (expiration) and nbf (not-before) claims, is never applied. As a result the helper verifies the token signature, subject and issuer but does not enforce the token's validity window: an access token that is expired, or not yet valid, is accepted as valid. Routes that rely on this helper to authenticate inbound requests therefore accept access tokens that are outside their intended lifetime. This issue affects Apache Camel: from 4.18.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix makes KeycloakSecurityHelper.parseAndVerifyAccessToken include the TokenVerifier.IS_ACTIVE check so that expired or not-yet-valid access tokens are rejected, aligning the helper with Keycloak's default check set. For deployments that cannot upgrade immediately, enforce token expiration outside the helper - for example validate the access token's exp/nbf claims in the route before trusting it, keep Keycloak access-token lifetimes short, and ensure any upstream gateway or resource server also validates the token validity window.	9.8	More Details
CVE-2026-46454	Improper Input Validation vulnerability in Apache Camel Cometd Component. The camel-cometd component maps inbound Bayeux (CometD) message headers into the Camel Exchange without applying a HeaderFilterStrategy. CometdBinding.populateExchangeFromMessage copies the entire ext.CamelHeaders map supplied by the CometD client directly onto the Camel message (message.setHeaders), so any header name - including Camel-internal control headers such as CamelHttpUri, CamelFileName or CamelJmsDestinationName - is accepted unmodified. Because a CometdComponent installs no Bayeux SecurityPolicy by default, any client that can complete the Bayeux handshake against the CometD endpoint can publish such a message without authentication. An attacker can therefore inject arbitrary Camel control headers that influence the behaviour of downstream producers in the route (for example redirecting an HTTP producer, changing a file name, or overriding a JMS destination); the injected headers also persist across internal direct, seda and vm hops. The concrete downstream impact depends on which producers the route uses. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix implements a HeaderFilterStrategy in the camel-cometd binding (a long-standing TODO in the code) that filters the Camel header namespace case-insensitively on inbound mapping, so client-supplied Camel* / camel* headers are no longer copied into the Exchange. For deployments that cannot upgrade immediately, strip the Camel control headers from inbound CometD messages before they reach any downstream producer (for example removeHeaders('Camel*') and removeHeaders('camel*') at the start of the route), and install an explicit	9.8	More Details

	Bayeux SecurityPolicy on the CometdComponent so that only authenticated clients can publish.		
CVE-2026-43867	Deserialization of Untrusted Data vulnerability in Apache Camel PQC Component. The camel-pqc component persists post-quantum key metadata (KeyMetadata) through pluggable KeyLifecycleManager implementations. AwsSecretsManagerKeyLifecycleManager.deserializeMetadata() reads that metadata back from the configured AWS Secrets Manager secret by Base64-decoding the stored value and deserializing it with a raw java.io.ObjectInputStream.readObject() and no ObjectInputFilter or class allow-list; the cast to KeyMetadata happens only after readObject() returns, so any readObject() side effects in a crafted object run before the type check. A principal who can write to the AWS Secrets Manager secret that holds this metadata (requiring secretsmanager:PutSecretValue on that secret) could store a crafted serialized object that is deserialized during normal key-lifecycle operations, potentially leading to code execution in the context of the application that manages the keys. This is the same underlying defect, in the same code path and remediated by the same fix, as CVE-2026-46590, which was reported independently and additionally covers the HashiCorp Vault and file-based sibling managers; both are incomplete-remediation follow-ons to CVE-2026-40048 (CAMEL-23200). This issue affects Apache Camel: from 4.18.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.18.x LTS releases stream, then they are suggested to upgrade to 4.18.3. For deployments that cannot upgrade immediately, restrict write access to the AWS Secrets Manager secret that holds the camel-pqc key metadata so that only the application’s own identity holds secretsmanager:PutSecretValue on it (least-privilege IAM), and keep the PQC key material in a secret separate from any data that less-trusted principals can write.	9.8	More Details
CVE-2026-24014	Apache IoTDB DataNode’s internal RPC interface for creating Trigger instances uses the uploaded Trigger JAR name to build a file path without sufficient validation. If the internal DataNode RPC port is exposed to an untrusted network, an attacker may use path traversal sequences in the JAR name to write files outside the intended Trigger installation directory. This could allow arbitrary file write with the permissions of the IoTDB process. This issue affects Apache IoTDB: from 1.3.3 before 2.0.8. Users are recommended to upgrade to version 2.0.8, which fixes the issue.	9.8	More Details
CVE-2026-14808	Prog Management System developed by PROG MIS has a Exposure of Sensitive Information vulnerability, allowing unauthenticated remote attackers to view a specific page and obtain the database account and password.	9.8	More Details
CVE-2026-14807	ERP App developed by PROG MIS has a Use of Hard-coded Credentials vulnerability, allowing unauthenticated remote attackers to log in to view application code and obtain the database account and password.	9.8	More Details
CVE-2026-27780	Gitea versions before 1.26.0 do not fail closed on bufio.Scanner errors while processing pre-receive hook input, allowing oversized input to bypass branch-protection checks.	9.8	More Details
CVE-2026-26292	Gitea versions before 1.25.5 do not use the migration HTTP transport for LFS push and sync mirror operations, bypassing the configured migration transport protections for those LFS requests.	9.8	More Details
CVE-2026-57677	Unauthenticated PHP Object Injection in Novalnet Payment Gateway for WooCommerce <= 12.10.3 versions.	9.8	More Details
CVE-2026-59705	mem0's openmemory/api component contains an unauthenticated access vulnerability that allows unauthenticated attackers to read, write, and delete arbitrary user memories by accessing API routers registered without authentication middleware. Attackers can supply arbitrary user_id parameters or directly access memory retrieval endpoints to expose private memory content, or invoke pause endpoints with global_pause=true to cause denial-of-service across all users.	9.8	More Details
CVE-2025-15646	HTML::Gumbo versions before 0.19 for Perl disclose heap memory via type confusion. Support for the <template> element was added to libgumbo 0.10.0 in 2015, but the walk_tree function in lib/HTML/Gumbo.xs was not updated to support it. The element was treated as a text-node, where strlen() over-reads the heap block that the pointer addresses. Any caller that runs parse() with the default format => 'string', or with format => 'tree', on input containing a <template> element serializes the over-read bytes into the returned result, disclosing bounded heap contents. format => 'callback' reaches a croak on the unhandled node type and is unaffected.	9.8	More Details
CVE-2026-34116	Guardian language-system passes the id GET parameter directly into a PHP exec() call in transcribe.php (line 15) without sanitization: exec(\"php jobs/transcribe.php \".$login_session.\" \".$_GET['id'].\" ...\"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	9.8	More Details
CVE-2026-34104	Guardian language-system passes the name GET parameter directly into an unsanitized SQL query in designer.php (line 124): SELECT * FROM complex WHERE name='\".$_GET['name'].\"'. An authenticated attacker can perform error-based SQL injection to extract database contents.	9.8	More Details
CVE-2026-24270	NVIDIA AIStore framework contains a vulnerability where an attacker could bypass authentication. A successful exploit of this vulnerability might lead to denial of service, escalation of privileges,	9.8	More Details

	information disclosure, and data tampering.		
CVE-2026-57517	Control Web Panel before 0.9.8.1225 contains a blind SQL injection vulnerability that allows unauthenticated remote attackers to execute arbitrary SQL queries by submitting unsanitized input through the userRes POST parameter at the user endpoint. Attackers can exploit MySQL root privileges obtained via the injection to write arbitrary files using INTO DUMPFILE, enabling deployment of a PHP webshell to the web-accessible roundcube logs directory and achieving remote code execution as the cwpsvc account.	9.8	More Details
CVE-2026-51947	An issue in Pivotal CRM 6.6.4.08 and systems using patch-ghi-15381-cwe-502-20251225.zip (fixed in Pivotal CRM 6.6.5.10 and Patch_CWE502_20260316.zip) allows a remote attacker to execute arbitrary code via the Pivotal.Engine.Client.Services.Conversion.dll component. NOTE: this issue exists because of an incomplete fix for CVE-2026-39253.	9.8	More Details
CVE-2026-58521	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in The Wikimedia Foundation Mediawiki - Cargo Extension allows SQL Injection. This issue affects Mediawiki - Cargo Extension: from * before 1.43.9,1.44.6,1.45.4.	9.8	More Details
CVE-2026-58453	JAIOTlink C492A-W6 Wi-Fi IP cameras running firmware 4.8.30.57701411 contain a hard-coded credentials vulnerability that allows network-adjacent attackers to gain unauthorized access by using the default admin username with an empty password accepted by the anyka_ipc HTTP service on port 80. Attackers can authenticate with these hardcoded credentials to access camera snapshots, video streams, network configuration, and factory-level API endpoints including the SetMAC command injection surface.	9.8	More Details
CVE-2026-58126	PACSgear PACS Scan 5.2.1 contains an unauthenticated remote code execution vulnerability that allows remote attackers to read and write arbitrary files by exploiting an exposed .NET Remoting TCP service on port 22222 via PGImageExchQueue.exe without any authentication requirement. Attackers can chain the arbitrary file write primitive with DLL hijacking in PGImageExchangeQueueSvc.exe, which loads missing DLLs such as CRYPTSP.DLL from the application directory, to achieve remote code execution as NT Authority\SYSTEM upon service restart.	9.8	More Details
CVE-2026-34117	Guardian language-system passes the id GET parameter directly into a PHP exec() call in text_to_subtitles.php (line 19) without sanitization: exec(\"php jobs/text_to_subtitles.php \".$login_session.\" \".$_GET['id'].\" ...\"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	9.8	More Details
CVE-2026-58127	PACSgear MediaWriter 5.2.1 exposes a .NET Remoting TCP service on port 9000 via PacsgearMediaServerEngine.dll, registered with ObjectURIs RemoteObj and UIRemoteObj, without any authentication requirement. By exploiting the MarshalByRefObject object unmarshalling technique and implementing .NET WebClient class methods, an unauthenticated remote attacker can read and write arbitrary files on the host filesystem. The ObjectURIs are identical across all installations by default. Chaining the arbitrary file write primitive with DLL hijacking opportunities in the MediaWriter service (which runs as NT Authority\\SYSTEM and loads missing DLLs such as CRYPTBASE.DLL from the application directory) enables unauthenticated remote code execution as SYSTEM upon service restart.	9.8	More Details
CVE-2026-34099	Guardian language-system passes the id GET parameter directly into an unsanitized SQL query in job_info.php (line 16): SELECT * FROM jobs where id = '\".$_GET['id'].\"'. No authentication is required. An unauthenticated attacker can perform error-based SQL injection to extract the database version, current user, schema names, and table contents.	9.8	More Details
CVE-2026-34100	Guardian language-system passes the id GET parameter directly into an unsanitized SQL query in media.php (line 17): SELECT id, filename, extension, type, duration, owner, private FROM files where id = '\".$_GET['id'].\"'. An authenticated attacker can perform error-based SQL injection to extract database contents.	9.8	More Details
CVE-2026-57621	Unauthenticated PHP Object Injection in Booktics <= 1.0.21 versions.	9.8	More Details
CVE-2026-34115	Guardian language-system passes the id GET parameter directly into a PHP exec() call in transcribe_amazon.php (line 15) without sanitization: exec(\"php jobs/transcribe_amazon.php \".$login_session.\" \".$_GET['id'].\" ...\"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	9.8	More Details
CVE-2026-58457	Shenzhen Aitemi M300 Wi-Fi Repeater (hardware model MT02) contains an unauthenticated OS command injection vulnerability that allows network-adjacent attackers to execute arbitrary shell commands by injecting unsanitized input through the smacfilter_conf handler in the commuos web backend. Attackers can append semicolon-delimited payloads to the name, enable, or mac GET parameters, which are passed without sanitization into sprintf() to build uci shell commands executed via doSystemCmdComlib(), granting full root-level control of the device.	9.8	More Details
	Guardian language-system passes the id GET parameter directly into an unsanitized SQL query in		

CVE-2026-34101	text_file.php (line 17): SELECT id, filename, extension, type, duration, owner, private FROM files where id = '\".$_GET['id'].\"'. An authenticated attacker can perform error-based SQL injection to extract database contents.	9.8	More Details
CVE-2026-34114	Guardian language-system passes the id GET parameter directly into a PHP exec() call in translate_text.php (line 18) without sanitization: exec(\"php jobs/translate_text.php \".$login_session.\" \".$_GET['id'].\" ...\"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	9.8	More Details
CVE-2026-34113	Guardian language-system passes the id GET parameter directly into a PHP exec() call in speech_text.php (line 18) without sanitization: exec(\"php jobs/speech_audio_text.php \".$login_session.\" \".$_GET['id'].\" ...\"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	9.8	More Details
CVE-2026-34112	Guardian language-system passes the id GET parameter directly into a PHP exec() call in speechmac.php (line 18) without sanitization: exec(\"php jobs/speech_audio_mac.php \".$login_session.\" \".$_GET['id'].\" ...\"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	9.8	More Details
CVE-2026-34102	Guardian language-system passes the id GET parameter directly into an unsanitized SQL query in job_info_get.php (line 16): SELECT * FROM jobs where input1 = '\".$_GET['id'].\"'. An authenticated attacker can perform error-based SQL injection to extract database contents.	9.8	More Details
CVE-2026-34103	Guardian language-system passes the id GET parameter directly into an unsanitized SQL query in subtitles.php (line 16): SELECT id, filename, extension, type FROM files where id = '\".$_GET['id'].\"'. An authenticated attacker can perform error-based SQL injection to extract database contents.	9.8	More Details
CVE-2026-34111	Guardian language-system passes the id GET parameter directly into a PHP exec() call in speechmac_text.php (line 18) without sanitization: exec(\"php jobs/speech_audio_mac_text.php \".$login_session.\" \".$_GET['id'].\" ...\"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	9.8	More Details
CVE-2026-34110	Guardian language-system passes the id GET parameter directly into a PHP exec() call in complex_start.php (line 14) without sanitization: exec(\"php jobs/complex.php \".$login_session.\" \".$_GET['id'].\" ...\"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	9.8	More Details
CVE-2026-34109	Guardian language-system passes the id GET parameter directly into a PHP exec() call in speech.php (line 18) without sanitization: exec(\"php jobs/speech_audio.php \".$login_session.\" \".$_GET['id'].\" ...\"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	9.8	More Details
CVE-2026-34108	Guardian language-system passes the id GET parameter directly into a PHP exec() call in text.php (line 15) without sanitization: exec(\"php jobs/text.php \".$login_session.\" \".$_GET['id'].\" ...\"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	9.8	More Details
CVE-2026-34107	Guardian language-system passes the id GET parameter directly into a PHP exec() call in translate.php (line 14) without sanitization: exec(\"php jobs/translate.php \".$login_session.\" \".$_GET['id'].\" ...\"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	9.8	More Details
CVE-2026-34106	Guardian language-system passes the id GET parameter directly into a PHP exec() call in subtitles.php (line 19) without sanitization: exec(\"php jobs/subtitle_rendering.php \".$login_session.\" \".$_GET['id'].\" ...\"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to the id parameter to execute arbitrary OS commands on the server.	9.8	More Details
CVE-2026-14363	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in The Wikimedia Foundation Mediawiki - Cargo Extension allows SQL Injection. This issue affects Mediawiki - Cargo Extension: from * before 1.43.9,1.44.6,1.45.4.	9.8	More Details
CVE-2026-34105	Guardian language-system passes the id GET parameter directly into an unsanitized SQL query in translate_text.php (line 15): SELECT id, filename, extension, type FROM files where id = '\".$_GET['id'].\"'. An authenticated attacker can perform error-based SQL injection to extract database contents.	9.8	More Details
CVE-2026-57692	Incorrect Privilege Assignment vulnerability in LCweb PrivateContent allows Privilege Escalation. This issue affects PrivateContent: from n/a through 9.9.2.	9.8	More Details
CVE-2026-52186	SQL Injection vulnerability in UTT nv518G nv518GV3v3.2.7-210919-161313 allows a remote attacker to execute arbitrary code via the gohead/sub_463bbc component	9.8	More Details

CVE-2026-11387	The SMS Alert – SMS & OTP for WooCommerce, Order Notifications & Abandoned Cart Recovery plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.9.5. This is due to the plugin not properly validating a user's identity prior to updating their details like reset the password of any user account, including administrators, and gain full access to those accounts. This makes it possible for unauthenticated attackers to change arbitrary user's email addresses, including administrators, and leverage that to reset the user's password and gain access to their account. This is only vulnerable on sites with OTP verification for password resets enabled, and where the administrator (or other user) has set a phone number for OTP verification.	9.8	More Details
CVE-2026-7840	UltraVNC repeater through 1.8.2.2 contains a global buffer overflow in its embedded HTTP administration server. The functions wi_senderr() and wi_replyhdr() in repeater/webgui/webutils.c write the caller-supplied HTTP request URI into a fixed 1000-byte global buffer (hdrbuf) via unchecked sprintf calls. The HTTP receive buffer accepts URIs up to approximately 150 KB (WI_RXBUFSIZE = 153600), so an unauthenticated attacker who can reach the repeater HTTP port (default TCP 80) can overflow hdrbuf by at least 500 bytes with a single HTTP request containing a URI of 1500 bytes or longer, corrupting adjacent .bss-segment globals. The overflow occurs before any authentication check, making it reachable without credentials. A remote, unauthenticated attacker can achieve arbitrary code execution on the host running the repeater.	9.8	More Details
CVE-2026-14398	Use after free in ANGLE in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-57625	Unauthenticated Cross Site Scripting (XSS) in Admin and Site Enhancements (ASE) Pro <= 8.8.5 versions.	9.6	More Details
CVE-2026-14425	Use after free in ANGLE in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-14424	Use after free in Dawn in Google Chrome on Mac prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-14423	Type Confusion in Tint in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-14420	Out of bounds read and write in Dawn in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-14419	Use after free in Skia in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-58426	Gitea Actions Artifacts V4 signed URL HMAC ambiguity allows cross-repository artifact read and cross-task upload-state write	9.6	More Details
CVE-2026-14417	Use after free in Dawn in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-14416	Out of bounds read in Dawn in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	9.6	More Details
CVE-2026-14405	Uninitialized Use in V8 in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	9.6	More Details
CVE-2026-14411	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-22874	Gitea versions up to and including 1.26.2 have incomplete SSRF protection in webhook and migration allow-list filtering.	9.6	More Details
CVE-2026-53492	containerd is an open-source container runtime. In Versions prior to 2.3.2, 2.2.5 and 2.1.9, the CRI implementation improperly trusts Container Device Interface (CDI) annotations found within untrusted checkpoint image metadata during container restoration. When restoring a container from a checkpoint, containerd preserves CDI-related annotations from the checkpoint archive rather than relying solely on the pod's create-time specification. This allows a user with pod creation permissions to bypass standard Kubernetes resource allocation and device plugin enforcement, injecting arbitrary CDI edits (such as device nodes and host mounts) into the restored container. Successful exploitation requires that the node has CDI enabled and contains a matching host CDI specification for the requested device; environments where CDI is disabled or lacking sensitive device specifications are not affected. This issue has been fixed in versions 2.3.2, 2.2.5 and 2.1.9.	9.6	More Details
CVE-2026-	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security	9.6	More

14382	severity: High)		Details
CVE-2026-14392	Out of bounds write in Tint in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-57571	Crawl4AI is an open-source LLM-friendly web crawler and scraper. Prior to 0.9.0, when the crawler saves a downloaded file, the destination filename was taken from attacker-influenced input and joined to the downloads directory with no confinement. A filename containing an absolute path or traversal escaped the downloads directory, giving an arbitrary file write with attacker-controlled contents; the HTTP crawler path uses the response Content-Disposition filename and the browser crawler path uses the download's suggested filename. Because the written bytes are attacker-controlled, this can escalate to remote code execution. This issue is fixed in version 0.9.0.	9.6	More Details
CVE-2026-14390	Use after free in ANGLE in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-14397	Out of bounds write in ANGLE in Google Chrome on Mac prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-14387	Integer overflow in Skia in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-52830	fast-mcp-telegram is a Telegram MCP Server. Prior to 0.19.1, fast-mcp-telegram validates HTTP Bearer tokens by joining the raw token string into a session-file path. The verifier rejects the exact reserved token telegram, but it does not reject path separators or normalize the path before checking whether the session file exists. A remote HTTP client can therefore authenticate as the default legacy session with a token such as ../fast-mcp-telegram/telegram when the documented default session file ~/.config/fast-mcp-telegram/telegram.session exists. This bypasses the reserved session name control that is intended to prevent HTTP multi-user sessions from colliding with the default stdio or legacy account. With account-prefixed MCP tools enabled, the attacker still sees and calls the prefixed tools for the default account, so the prefix middleware does not stop the session selection bypass. This vulnerability is fixed in 0.19.1.	9.4	More Details
CVE-2026-59706	mem0 contains unauthenticated config API endpoints that expose LLM API keys in plaintext and allow server-side request forgery via attacker-controlled ollama_base_url parameter. Unauthenticated attackers can retrieve stored secrets like OpenAI API keys via GET /api/v1/config/ or trigger SSRF attacks by setting ollama_base_url to internal addresses like cloud IMDS via PUT /api/v1/config/mem0/llm endpoint.	9.3	More Details
CVE-2026-57679	Unauthenticated SQL Injection in GeekyBot <= 1.2.5 versions.	9.3	More Details
CVE-2026-57683	Unauthenticated SQL Injection in WP Fast Total Search <= 1.80.280 versions.	9.3	More Details
CVE-2026-41106	Url redirection to untrusted site ('open redirect') in M365 Copilot allows an unauthorized attacker to elevate privileges over a network.	9.3	More Details
CVE-2026-5268	An authentication bypass vulnerability exists in the default SFTP server component utilized across the Ciena products listed. This vulnerability allows a remote, unauthenticated attacker to bypass security controls and gain unauthorized access to the underlying filesystem. Successful exploitation could allow an attacker to read or modify system files.	9.1	More Details
CVE-2026-14198	@fastify/middie versions 9.1.0 through 9.3.2 decode the encoded slash %2F inside path parameter values before matching middleware paths, while Fastify's underlying router preserves the encoding during route lookup. The two layers disagree on the canonical request path, so the middleware fails to match a URL that the route handler does match. When middleware is used for authentication, authorization, rate limiting, or auditing on parameterized paths, an attacker can reach the protected handler by sending a single crafted URL with an encoded slash in the parameter position. The bypass is HTTP method agnostic and requires no authentication or special preconditions. Patches: upgrade to @fastify/middie 9.3.3. Workarounds: avoid parameterized middleware paths for security decisions, or enforce authentication at the route handler or via a Fastify hook that runs after the router has resolved the request.	9.1	More Details
CVE-2026-46354	Coder allows organizations to provision remote development environments via Terraform. In versions prior tp 2.24.5, 2.29.13, 2.30.8, 2.31.12, 2.32.2, and 2.33.3, `azureidentity.Validate()` verifies that the PKCS#7 signer certificate chains to a trusted Azure CA but never verifies the PKCS#7 signature itself. An attacker can embed a legitimate Azure certificate alongside arbitrary content e.g. `{"vmId":"<target>"}` and the forged `vmId` will be accepted returning the victim workspace agent's session token. No authentication is required. The attacker only needs to know a target VM's `vmId` which is a	9.1	More Details

	`UUIDv4`. That's a practical limitation which would typically require prior access to be exploited. Versions 2.24.5, 2.29.13, 2.30.8, 2.31.12, 2.32.2, and 2.33.3 patch the issue. As a workaround, reconfigure any Azure templates to use token authentication rather than `azure-instance-identity`.		
CVE-2026-58473	Cognee before 1.2.0 contains an improper access control vulnerability that allows unauthenticated attackers to overwrite the global LLM provider configuration by self-registering an account and calling the settings endpoint, which performs no admin or superuser check. Attackers can redirect all LLM operations instance-wide to an attacker-controlled endpoint by exploiting the process-wide singleton configuration cache, enabling exfiltration of prompts, uploaded documents, extracted entities, and knowledge graph content from all users.	9.1	More Details
CVE-2025-53830	Anti-Virus for ownCloud is an anti-virus application for file storage, synchronization, and sharing application ownCloud. Versions of Anti-Virus for ownCloud before 1.2.3 are vulnerable to Server-Side Request Forgery (SSRF). This corresponds to versions of ownCloud 10 prior to 10.15.3. Upgrade ownCloud 10 to version 10.15.3 or later or upgrade Anti-Virus for ownCloud 10 to version 1.2.3 or later to receive a fix.	9.1	More Details
CVE-2026-23537	A vulnerability has been identified in the Feast Feature Server's `/save-document` endpoint that allows an unauthenticated remote attacker to write arbitrary JSON files to the server's filesystem. Although the system attempts to restrict file locations, these protections can be bypassed, enabling an attacker to overwrite vital application configurations or startup scripts. Because this flaw requires no credentials or special privileges, any attacker with network access to the server can potentially compromise the integrity of the system. This could lead to unauthorized system modifications, denial of service through disk exhaustion, or potential remote code execution.	9.1	More Details
CVE-2025-53827	ownCloud Core is the server-side component of the file storage, synchronization, and sharing application ownCloud Classic. In versions prior to 10.15.3, the Updater on ownCloud 10 before 10.15.3 has an exposed dangerous method or function. Attackers with administrative privileges may leverage functionality to execute arbitrary code. This issue has been fixed in version 10.15.3.	9.1	More Details
CVE-2026-26247	Gitea versions before 1.25.5 do not persist the OAuth2 PKCE S256 challenge method correctly during authorization, allowing token exchange without the expected verifier check.	9.1	More Details
CVE-2026-6070	The WP-BusinessDirectory plugin for WordPress is vulnerable to Unauthenticated Arbitrary File Deletion in versions up to and including 4.0.1. This is due to insufficient path validation in the remove() method of the JBusinessDirectoryControllerUpload class. The task=upload.remove endpoint is accessible without authentication via the plugin's frontend routing system. The _filename parameter is accepted with RAW filter (no sanitization), and the helper function makePathFile() only normalizes directory separator characters without stripping path traversal sequences (../). When combined with the _path_type=2 parameter, which sets the base directory to the plugin's site folder, an attacker can supply a _filename value containing ../ sequences to traverse outside the plugin directory and call PHP's unlink() on arbitrary files — including wp-config.php, wp-config-backup.php, or other critical server files accessible to the web server process. This makes it possible for unauthenticated attackers to delete arbitrary files on the server.	9.1	More Details
CVE-2026-48205	Improper Input Validation, Server-Side Request Forgery (SSRF) vulnerability in Apache Camel DNS component. The camel-dns producers read DNS operation parameters - the resolver to query, the name or domain to look up, the record type and class, and the search term - from Exchange message headers whose constant values (DnsConstants.DNS_SERVER, DNS_NAME, DNS_DOMAIN, DNS_TYPE, DNS_CLASS, TERM) were the plain strings dns.server, dns.name, dns.domain, dns.type, dns.class and term. Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that bridges an HTTP consumer (for example platform-http) into a dns: producer, any HTTP client could therefore set the dns.server header to make the dig producer build a SimpleResolver pointing at an attacker-controlled DNS server - a server-side request forgery via DNS, through which the attacker observes the queried name and can return poisoned responses - and set the dns.name / dns.domain headers to resolve arbitrary internal hostnames, disclosing whether they exist (internal network reconnaissance). No credentials are required when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that drive DNS operations via the raw header names must use CamelDnsServer / CamelDnsName / CamelDnsDomain / CamelDnsType / CamelDnsClass / CamelDnsTerm instead of the dns.* / term names. For deployments that cannot upgrade immediately, strip the dns.* and term headers from any untrusted ingress before the dns: producer, and set the DNS server and lookup parameters from a trusted source in the route.	9.1	More Details
	UltraVNC repeater through 1.8.2.2 initializes the HTTP administration server with a hardcoded default password. In repeater/webgui/settings.c:197, when settings2.txt is absent on first run the repeater writes the literal string "adminadmi2" as the admin password via strcpy_s(saved_password, 64,		

CVE-2026-7839	"adminadmi2"). The HTTP Basic-auth handler wi_decode_auth() checks this password without rate-limiting or lockout. Any remote attacker who can reach the repeater HTTP port (default TCP 80) can authenticate as administrator using the well-known default credential on a fresh or unmodified installation, gaining full control of the repeater configuration including allow/deny rules and session visibility.	9.1	More Details
CVE-2026-38971	ardupilot through Plane-4.6.3 was found to contain an out-of-bounds read issue in libraries/GCS_MAVLink/GCS_serial_control.cpp in GCS_MAVLINK::handle_serial_control().	9.1	More Details
CVE-2026-9725	The Printcart Web to Print Product Designer for WooCommerce plugin for WordPress is vulnerable to Arbitrary File Deletion in versions up to, and including, 2.5.2 This is due to insufficient path validation in the store_design_data() function, which constructs a filesystem path from the user-supplied 'nbd_item_key' POST parameter sanitized only with sanitize_text_field() — which does not strip path traversal sequences — and then passes that path directly to Nbdesigner_IO::delete_folder() and PHP's rename(). The nonce protecting the nbd_save_customer_design AJAX action is freely obtainable by unauthenticated users via the nbd_check_use_logged_in endpoint. This makes it possible for unauthenticated attackers to delete arbitrary files on the affected site's server which may make remote code execution possible.	9.1	More Details
CVE-2026-11564	libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse if one of them matches the setup. An easy handle that first uses default native CA trust can continue trusting the native platform store after the application switches that same handle to custom CA material for a later transfer.	9.1	More Details
CVE-2026-8924	A flaw in curl’s cookie parsing logic allows a malicious HTTP server to set 'super cookies' that bypass the Public Suffix List check. This enables an attacker-controlled origin to inject cookies that curl subsequently scopes and transmits to unrelated third-party domains.	9.1	More Details
CVE-2026-54400	A malicious actor with access to the network and high privileges could exploit an Improper Access Control vulnerability found in UniFi Access Application to escalate privileges on the host device.	9.1	More Details
CVE-2026-48203	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Improper Input Validation, Server-Side Request Forgery (SSRF) vulnerability in Apache Camel Solr component. The camel-solr producer copies Exchange message headers whose names begin with the SolrParam. prefix into the parameters of the Solr request, and headers whose names begin with the SolrField. prefix into the fields of the indexed Solr document. The prefix constants (SolrConstants.HEADER_PARAM_PREFIX / HEADER_FIELD_PREFIX) were the plain strings SolrParam. / SolrField.. Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that bridges an HTTP consumer (for example platform-http) into a solr: producer, any HTTP client could therefore set SolrParam.* headers to inject arbitrary Solr request parameters - including shards or stream.url, which cause the Solr server to issue server-side requests to an attacker-chosen URL (server-side request forgery, for example to an internal service or a cloud metadata endpoint), or qt to reach administrative request handlers - and set SolrField.* headers to inject arbitrary fields into indexed documents. No credentials are required when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that set Solr parameters or fields via the raw header prefixes must use CamelSolrParam. / CamelSolrField. instead of SolrParam. / SolrField.. For deployments that cannot upgrade immediately, strip the SolrParam.* and SolrField.* headers from any untrusted ingress before the solr: producer, and set the required Solr parameters and fields from a trusted source in the route.	9.1	More Details
CVE-2026-8926	When asking curl to use a `.netrc` file to find credentials and at the same time specifying a URL with a username(without a password), like `https://user@example.com/`, curl could wrongly get and use the password for *another* user set in the `.netrc` file for that host if such a one exists and there is no match for the specified user.	9.1	More Details
CVE-2026-8927	When reusing a libcurl handle for sequential transfers driven by environment-variable proxy configuration, libcurl fails to clear the proxy authentication state between requests. Specifically, if the initial transfer authenticates against `proxyA` using Digest auth, a subsequent transfer routed through `proxyB` erroneously leaks the `Proxy-Authorization:` header intended solely for `proxyA`.	9.1	More Details
CVE-2026-56015	Net::IP::LPM versions through 1.10 for Perl allow a heap out-of-bounds read via an unbounded prefix length. add() passes the prefix string to the trie builder addPrefixToTrie() without checking it against the address width. addPrefixToTrie() then walks the prefix buffer by prefix_length bits, reading prefix[byte] for byte up to prefix_len/8, where prefix is the 4-byte (IPv4) or 16-byte (IPv6) packed address. A prefix length greater than 32 for IPv4 or 128 for IPv6, for example add("1.2.3.4/255", $v) or add("2001:db8::/255", $v), reads past the end of the packed address. The out-of-bounds read happens during trie construction and is bounded: the prefix length is stored as an unsigned char, so the bit walk	9.1	More Details

	reads at most 32 bytes from the start of the packed address, a short distance past the end of the 4-byte or 16-byte buffer. It is detectable under AddressSanitizer, valgrind, or a hardened allocator, where it can abort the process. Lookups and dump() format only the valid address width, so the out-of-bounds bytes are not exposed through the module's API.		
CVE-2026-20706	Gitea versions up to and including 1.26.1 allow repository archive downloads to bypass token scope checks on the web archive download endpoint.	9.1	More Details
CVE-2026-22547	Gitea versions before 1.25.5 lack validation constraints for repository creation fields, including length-limited template fields and trust model or object format values.	9.1	More Details
CVE-2026-25718	Gitea versions before 1.25.5 mishandle path resolution during template repository generation, allowing template processing to read or write through symlinked or otherwise non-regular paths.	9.1	More Details
CVE-2026-26232	Gitea versions before 1.25.5 do not consistently enforce OAuth2 authorization code expiry and single-use behavior during token exchange.	9.1	More Details
CVE-2026-27436	Editor Arbitrary Code Execution in Five Star Business Profile and Schema <= 2.3.19 versions.	9.1	More Details
CVE-2026-6382	The FileOrganizer WordPress plugin before 1.1.9, Advanced File Manager WordPress plugin before 5.4.12, File Manager Pro WordPress plugin before 2.1.1, File Manager WordPress plugin before 8.0.4 do not properly escape a parameter before passing it to a shell command when processing image operations, allowing authenticated users to perform OS Command Injection. This requires the server to have the ImageMagick convert CLI available without either the PHP imagick or GD extensions.	9.1	More Details
CVE-2026-24013	Authentication Bypass by Spoofing vulnerability in Apache IoTDB. Certain Thrift RPC query handlers lack strict validation of the sessionId parameter. An attacker can construct requests with a forged sessionId and, without performing openSession authentication, receive valid query results. This allows authentication bypass and unauthorized reading of time-series data. This issue affects Apache IoTDB: from 1.3.3 before 2.0.8. Users are recommended to upgrade to version 2.0.8, which fixes the issue.	9.1	More Details
CVE-2026-40047	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability in Apache Camel Docling component. The camel-docling component invokes the external `docling` command-line tool by assembling an argument list in DoclingProducer and executing it through java.lang.ProcessBuilder. Custom CLI arguments supplied through the `CamelDoclingCustomArguments` exchange header (a List<String>) were appended to that argument list with insufficient validation: the original implementation relied on a denylist of disallowed flags and only rejected path values that contained a literal `../` sequence. As a result, a Camel route that forwards externally-influenced data into the `CamelDoclingCustomArguments` header (or into the path-bearing headers used to build the invocation) could cause the producer to pass unrecognized or unintended `docling` CLI flags to the subprocess, and could supply path-like argument values that resolved outside the intended directory through traversal sequences not caught by the literal `../` check. Because Camel itself builds the `docling` invocation from these values, the component is responsible for constraining them, and the weak validation allowed CLI-argument injection and directory traversal in the arguments passed to the external tool. The invocation uses the list-based form of ProcessBuilder, so a shell does not interpret the argument values; OS command injection through shell metacharacters was not possible, and the metacharacter rejection added by the fix is defense-in-depth. This issue affects Apache Camel: from 4.15.0 before 4.18.3. Users are recommended to upgrade to a release that contains the CAMEL-23212 fix. On the mainline the fix is included from Apache Camel 4.19.0 (and later releases such as 4.20.0). For users on the 4.18.x LTS releases stream, upgrade to 4.18.3. The fix replaces the denylist with a strict allowlist of recognized `docling` CLI flags (rejecting any unrecognized flag, and rejecting producer-managed flags such as the output-directory flags), defensively rejects shell metacharacters in argument values, and normalizes path-like values with Path.normalize() before validating them so that traversal sequences which bypass a literal `../` check are detected. As defence in depth, route authors should avoid mapping untrusted message content into the `CamelDoclingCustomArguments` header and the path-bearing headers, and should strip Camel-internal headers from messages that arrive from untrusted producers.	9.1	More Details
CVE-2026-59099	Apereo CAS 7.3.0 before 8.0.0-RC6 contains a cryptographic vulnerability that allows remote unauthenticated attackers to recover plaintext conversation state by exploiting AES-GCM initialization vector reuse across the server lifetime. Attackers can collect multiple client-side webflow execution tokens from the unauthenticated login page and perform known-plaintext analysis to decrypt the webflow conversation state due to keystream reuse caused by a fixed all-zero IV paired with the same encryption key.	9.1	More Details
CVE-2026-55116	A malicious actor with access to the network and under certain network configurations could exploit an Improper Access Control vulnerability found in certain devices running UniFi OS to make unauthorized changes to such UniFi OS devices.	9.0	More Details
CVE-2025-	NVIDIA ConnectX and BlueField contain a vulnerability in the command interface where a local user with virtual function (VF) access may cause a write out of bounds by crafted input. A successful exploit of this	9.0	More

23351	vulnerability may lead to arbitrary code execution on the device.		Details
CVE-2026-10539	A Control-M/Server communication command does not sufficiently filter or sanitize user-supplied input. Under certain conditions, this issue may allow an unauthenticated attacker to execute unauthorized commands on the affected server, potentially leading to compromise of the server. This vulnerability affects Control-M/Server versions 9.0.20.x to 9.0.21.200 (included) and potentially earlier unsupported versions.	9.0	More Details
CVE-2026-4375	The DoLeads Integrator WordPress plugin through 0.65, wp2epub WordPress plugin through 0.65 have been seen to be used to achieve RCE, once they are added adding to a blog, for example using a vulnerability where unclosed extensions from wordpress.org can be installed by unauthorized users.	9.0	More Details
CVE-2025-23350	NVIDIA ConnectX and BlueField contain a vulnerability in the command interface where a local user with virtual function (VF) access may cause a write out of bounds by crafted input. A successful exploit of this vulnerability may lead to arbitrary code execution on the device.	9.0	More Details
CVE-2026-58289	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	9.0	More Details
CVE-2026-57623	Unauthenticated Arbitrary Code Execution in W3 Total Cache <= 2.9.4 versions.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-58424	Permanent Fork PR Workflow Approval Gate Bypass	8.9	More Details
CVE-2026-14721	A vulnerability has been found in UTT HiPER 1250GW up to 3.2.7-210907-180535. This affects an unknown function of the file /goform/ConfigWirelessBase_5g of the component Web Endpoint. The manipulation of the argument ssid leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-57516	Ray prior to 2.56.0 contains an unsafe deserialization vulnerability in the WebDataset reader that allows attackers to achieve remote code execution by supplying a malicious tar archive to the read_webdataset() function. The _default_decoder() function in webdataset_datasource.py unconditionally calls pickle.loads() on tar entries with .pkl/.pickle extensions and torch.load() with weights_only=False on .pt/.pth entries, executing arbitrary code inside Ray remote workers on every worker that processes the malicious archive.	8.8	More Details
CVE-2026-58452	JAIOTlink C492A-W6 Wi-Fi IP cameras running firmware 4.8.30.57701411 contain an OS command injection vulnerability that allows authenticated attackers to achieve remote code execution by supplying a malicious Wireless parameter to the HTTP PUT NetSDK/Factory SetMAC endpoint. Attackers can craft a string beginning with a valid MAC-like prefix followed by a semicolon and a shell payload, which bypasses partial sscanf() validation and is passed unsanitized into an echo shell command executed through a system() wrapper.	8.8	More Details
CVE-2026-11855	The Simple Membership WordPress plugin before 4.7.5 does not verify the authenticity of Stripe webhook requests when no signing secret is configured, nor escape a value taken from them before outputting it in an administrator notice, allowing unauthenticated attackers to inject arbitrary web scripts that execute in the context of a logged-in administrator.	8.8	More Details
CVE-2026-10830	The AllCoach WordPress plugin before 1.0.2 does not verify that an email address submitted to a public account-registration endpoint is not already associated with an existing user before overwriting that user's password, allowing unauthenticated attackers to reset the password of arbitrary accounts, including administrators, and take over the site.	8.8	More Details
CVE-2026-9085	Incorrect Permission Assignment for Critical Resource, Improper Access Control vulnerability in TUBITAK BILGEM Software Technologies Research Institute Pardus-Parental-Control allows DNS Spoofing. This issue affects Pardus-Parental-Control: from <=0.5.1 before 0.7.0.	8.8	More Details
CVE-2026-14383	Inappropriate implementation in V8 in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-14385	Heap buffer overflow in ANGLE in Google Chrome on Mac prior to 150.0.7871.46 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-	Use after free in V8 in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to execute arbitrary	8.8	More

14393	code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)		Details
CVE-2026-14394	Use after free in V8 in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-7838	UltraVNC viewer through 1.8.2.2 contains an integer overflow leading to a heap buffer overflow in the RFB protocol failure-response parsing path. In vncviewer/ClientConnection.cpp, the 4-byte network-supplied reasonLen field (type CARD32) is passed as reasonLen+1 to CheckBufferSize(). Because both operands are unsigned 32-bit, a reasonLen of 0xFFFFFFFF overflows to 0, causing CheckBufferSize to allocate only 256 bytes. The subsequent ReadString(m_netbuf, reasonLen) call then performs ReadExact for the original 4 GiB length into that 256-byte heap buffer. This overflow is reachable via rfbConnFailed (auth-scheme negotiation) and rfbVncAuthFailed (post-handshake) message types without successful authentication. A malicious VNC server, or any man-in-the-middle on the RFB stream, can trigger this condition when the victim viewer connects, potentially resulting in remote code execution as the user running the viewer. The crash was confirmed with AddressSanitizer on a portable reproduction harness (heap-buffer-overflow WRITE at offset 256).	8.8	More Details
CVE-2026-14395	Out of bounds write in V8 in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-14403	Use after free in V8 in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-14407	Inappropriate implementation in V8 in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-13696	Improper neutralization of special elements used in an LDAP query ('LDAP injection') vulnerability in HAVELSAN Inc. Liman MYS allows LDAP Injection. This issue affects Liman MYS: before release.Master.1107.	8.8	More Details
CVE-2026-10054	In affected versions of Eclipse Theia (1.8.1 and later), the browser backend exposes privileged terminal RPC over WebSocket (/services/shell-terminal, /services/terminals/:id) without service-level authentication. WebSocket origin validation in @theia/core is fail-open: connections are accepted when the Origin header is missing or when no THEIA_HOSTS allowlist is configured (the default). The Socket.IO integration additionally replaces the real Origin header with a client-supplied fix-origin header that an attacker can control or omit. As a result, a foreign-origin web page visited by a user with a running Theia instance can open the /services WebSocket namespace, invoke terminal creation, attach to the resulting terminal data channel, execute arbitrary OS commands, and read their output. This affects both local developer setups (drive-by attack) and hosted or tunneled deployments without strong external authentication. A fix is in development that enforces same-origin validation by default, removes trust in the fix-origin header, gates HTTP and WebSocket access on a SameSite=Strict; HttpOnly connection-token cookie, and sanitizes shell terminal creation options.	8.8	More Details
CVE-2026-44938	A vulnerability has been identified in Fleet's agent-side deployer, which did not filter security-sensitive keys from namespaceLabels in fleet.yaml (or BundleDeployment.spec.options.namespaceLabels) when applying them to the target namespace. An attacker with git push access to a Fleet-monitored repository could overwrite Pod Security Standards (PSS) enforcement labels on a target namespace. This allows the attacker to weaken admission controls and deploy workloads that PSS policies would otherwise block.	8.8	More Details
CVE-2026-14415	Inappropriate implementation in V8 in Google Chrome prior to 150.0.7871.46 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-11962	The FileOrganizer WordPress plugin before 1.2.0 does not validate the file type on several of its file-management operations, allowing authenticated users who have been granted file-manager access — which its premium add-on can extend to sub-administrator roles — to upload arbitrary PHP files and achieve remote code execution. This is an incomplete fix of CVE-2024-7985, which only added file-type validation to the upload operation.	8.8	More Details
CVE-	Deserialization of Untrusted Data vulnerability in Apache Camel PQC component. The camel-pqc component persists post-quantum key metadata (KeyMetadata) through pluggable KeyLifecycleManager implementations. HashicorpVaultKeyLifecycleManager and AwsSecretsManagerKeyLifecycleManager read that metadata back from the configured secret backend by deserializing a Base64-wrapped value with a raw java.io.ObjectInputStream.readObject() and no ObjectInputFilter or class allow-list; the cast to KeyMetadata happens only after readObject() returns, so any readObject() side effects in a crafted object run before the type check. The same unfiltered legacy-migration read also remained in FileBasedKeyLifecycleManager (for the stored KeyPair and KeyMetadata). A principal who can write to the operator-controlled backend that holds these values - the HashiCorp Vault KV path, or the AWS Secrets Manager secret (requiring a Vault token or secretsmanager:PutSecretValue) - could store a crafted serialized object that is deserialized during normal		

2026-46590	key-lifecycle operations, potentially leading to code execution in the context of the application that manages the keys. This is an incomplete-remediation follow-on to CVE-2026-40048 (CAMEL-23200), which changed FileBasedKeyLifecycleManager to store metadata as JSON / PKCS#8 / X.509 but did not add an ObjectInputFilter, did not cover the Vault and AWS sibling managers, and left FileBasedKeyLifecycleManager's own legacy-migration deserialization unfiltered. This issue affects Apache Camel: from 4.18.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.18.x LTS releases stream, then they are suggested to upgrade to 4.18.3. For deployments that cannot upgrade immediately, restrict write access to the key backend so that only the application's own identity can write the camel-pqc secrets (least-privilege HashiCorp Vault policies and secretsmanager:PutSecretValue IAM), and keep the PQC key material in a backend separate from any data that less-trusted principals can write.	8.8	More Details
CVE-2026-14430	Integer overflow in V8 in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-5136	A flaw was found in Foreman. The Usergroup model in Foreman does not properly validate role assignments against the calling user's permissions. This allows an authenticated user with usergroup management permissions to attach arbitrary roles, including administrative roles, to a user group and then add themselves as a member. Successful exploitation of this vulnerability leads to full privilege escalation, granting the attacker administrator-level access.	8.8	More Details
CVE-2026-13228	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Privilege Escalation to Administrator in versions up to, and including, 5.6.3 This is due to an Insecure Direct Object Reference (IDOR) in the create_or_update() function of OsOrdersController, which allows an authenticated Agent to supply an arbitrary order[customer_id] and overwrite any LatePoint customer's email field (including one linked to a WordPress Administrator's account) through the public-scope customer set_data() call, combined with a missing role verification in OsAuthHelper::authorize_customer() which logs in the linked WordPress user without checking its role. This makes it possible for authenticated attackers, with custom (Agent)-level access and above, to elevate their privileges to Administrator.	8.8	More Details
CVE-2026-34058	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the Livewire component Server\Resources exposes public methods (startUnmanaged, stopUnmanaged, restartUnmanaged) that accept a container ID parameter directly from the browser without any sanitization or escaping. This parameter is interpolated directly into shell commands executed via SSH on managed servers, enabling any authenticated team member to execute arbitrary OS commands on remote servers. This issue is fixed in version 4.0.0-beta.471.	8.8	More Details
CVE-2026-34057	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the database import Livewire component (app/Livewire/Project/Database/Import.php) allows client-controlled container and server properties to reach shell commands without locking or validation, allowing an authenticated user to inject commands through a database import container name. This issue is fixed in version 4.0.0-beta.471.	8.8	More Details
CVE-2026-42143	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, user-controlled persistent volume names are interpolated into shell commands executed on managed servers without escaping or validation, allowing an authenticated member to inject shell metacharacters and execute commands as root when volume operations are triggered. This issue appears to be fixed in version 4.0.0-beta.471.	8.8	More Details
CVE-2026-34035	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.466, log drain secret and environment values were interpolated into shell commands without sufficient encoding, allowing an authenticated user to inject commands executed on the host. This issue is fixed in version 4.0.0-beta.466.	8.8	More Details
CVE-2026-42200	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, PostgreSQL initialization script (generate_init_scripts() method in app/Actions/Database/StartPostgresql.php) filename handling did not sufficiently restrict paths, allowing an authenticated user to write files outside the intended directory and achieve command execution through database initialization. This issue is fixed in version 4.0.0-beta.474.	8.8	More Details
CVE-2026-34158	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.469, the executeInDocker() helper wraps user-controlled commands in single quotes without escaping embedded single quotes. Attackers who can edit application settings can inject a single quote into docker_compose_custom_build_command or docker_compose_custom_start_command to break out of the quoted context and execute arbitrary commands on the managed server host during deployments, escaping the intended Docker container confinement. This issue is fixed in version 4.0.0-beta.469.	8.8	More Details
CVE-2026-34034	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.466, the sentinel_token setting is used in shell commands without sufficient validation, allowing an authenticated user with access to server Sentinel settings to inject shell syntax and execute commands on	8.8	More Details

	the host when Sentinel is restarted. This issue is fixed in version 4.0.0-beta.466.		
CVE-2026-42204	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. From 4.0.0-beta.471 through 4.0.0-beta.473, a regression in SHELL_SAFE_COMMAND_PATTERN allowed ampersands in custom Docker Compose build, start, and pre/post-deployment command fields, allowing an authenticated team member to inject shell commands that execute on the host. This issue is fixed in version 4.0.0-beta.474.	8.8	More Details
CVE-2026-42153	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, PostgreSQL healthcheck command generation used attacker-controlled database settings (postgres_user and postgres_db) in shell-form commands, allowing an authenticated user to inject commands executed in the database container. This issue is fixed in version 4.0.0-beta.474.	8.8	More Details
CVE-2026-34599	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, there is an authenticated command injection vulnerability in the GetLogs Livewire component which allows users with team membership (lowest privilege member role) to execute arbitrary commands as root on managed servers. The $container Livewire public property is interpolated directly into shell commands (docker logs, docker service logs) without sanitization, and can be modified by any client via the Livewire wire protocol because it lacks the #[Locked] attribute. This issue is fixed in version 4.0.0-beta.471.	8.8	More Details
CVE-2026-34153	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, LocalFileVolume::saveStorageOnServer builds shell commands using unescaped fs_path and parent_dir values before validation, and submitFileStorage does not validate the user-controlled file-mount path before creating a volume, allowing an authenticated user who can add file storage to execute commands when the storage is saved. This issue is fixed in version 4.0.0-beta.471.	8.8	More Details
CVE-2026-11610	A heap buffer overflow flaw was found in the SASL I/O layer of 389 Directory Server (389-ds-base). After a successful SASL bind with integrity protection (SSF > 0), an authenticated attacker can send a specially crafted oversized LDAP UNBIND packet that is copied into a 512-byte heap receive buffer without a bounds check in sasl_io_recv() in sasl_io.c. This allows up to approximately 2 megabytes of attacker-controlled data to overflow the buffer, causing a denial of service (server crash). In FreeIPA and Red Hat Identity Management deployments, any domain user with a valid Kerberos ticket, any enrolled host, or any service account can trigger this vulnerability over the network after authenticating via GSSAPI. The vulnerable code path has existed since approximately 2013 (389-ds-base 1.3.2) and was not addressed by the CVE-2025-14905 fix, which patched a separate heap overflow in schema.c only.	8.8	More Details
CVE-2026-12224	The Dokan Pro plugin for WordPress is vulnerable to privilege escalation via update_capabilities REST Endpoint in all versions up to, and including, 5.0.4. This is due to the `update_capabilities()` REST handler accepting arbitrary capability strings from the request body and passing them directly to WP_User::add_cap() with no allowlist validation, only verifying that the caller holds the dokandar capability. This makes it possible for authenticated attackers with a self-provisioned Vendor-level access and above, on sites with the Vendor Staff module enabled, to grant arbitrary WordPress capabilities, including administrator, to any vendor_staff account, leading to a full site takeover.	8.8	More Details
CVE-2026-12158	The RegistrationMagic – User Registration Forms Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.0.9.1. This is due to missing or incorrect nonce validation on the process_request function. This makes it possible for unauthenticated attackers to escalate the privileges of an arbitrary form submitter to administrator by creating a malicious Chronos automation task that is executed via WordPress cron via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2026-14474	A flaw was found in SSSD's LDAP sudo provider. When the ldap_sudo_search_base option is not explicitly configured, SSSD searches the entire LDAP directory tree for sudoRole objects. An authenticated attacker with write access to any subtree can inject a sudoRole object granting root-level sudo privileges on all SSSD-enrolled hosts.	8.8	More Details
CVE-2026-25268	Memory Corruption when processing invalid HT40 channel layouts during dynamic channel switching operations.	8.8	More Details
CVE-2026-34168	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the LocalPersistentVolume.name field is interpolated directly into docker volume shell commands without shell argument escaping, allowing an authenticated user to set a storage name containing shell metacharacters and execute commands on managed servers when the resource is deleted. This issue is fixed in version 4.0.0-beta.471.	8.8	More Details
CVE-2026-14422	Out of bounds read and write in Tint in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-14431	Type Confusion in V8 in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE-2026-57766	Unauthenticated Cross Site Request Forgery (CSRF) in WPIDE – File Manager & Code Editor <= 3.5.6 versions.	8.8	More Details
CVE-2026-14459	Improper neutralization of argument delimiters in a command ('argument injection') vulnerability in TUBITAK BILGEM Software Technologies Research Institute pardus-software allows Argument Injection. This issue affects pardus-software: from <= 1.0.4 before 1.0.5.	8.8	More Details
CVE-2026-14460	Missing Authorization vulnerability in TUBITAK BILGEM Software Technologies Research Institute pardus-software allows Argument Injection. This issue affects pardus-software: from <= 1.0.4 before 1.0.5.	8.8	More Details
CVE-2026-27775	Gitea 1.25.5 caches a branch-specific write-permission result across multiple refs in one pre-receive hook session, allowing a per-branch maintainer-edit grant to be reused for other refs and escalate to full repository write access.	8.8	More Details
CVE-2026-56645	Heap-based buffer overflow in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2026-57974	Integer overflow or wraparound in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2026-57981	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2026-53488	containerd is an open-source container runtime. In versions prior to 1.7.33, 2.3.2, 2.2.5, 2.1.9, and 2.0.10 the CRI plugin propagates labels from an image config (LABEL instruction in Dockerfile) to a container without validation. This may result in executing an arbitrary command on the host, via a plugin that consumes container labels for some operations. This issue has been fixed in versions 1.7.33, 2.3.2, 2.2.5, 2.1.9, and 2.0.10.	8.8	More Details
CVE-2026-54998	Incorrect authorization in Microsoft Exchange Online allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2026-59093	Weaviate before 1.38.0 does not verify that a principal performing an RBAC role assignment holds the permissions granted by the assigned role. The assignRoleToUser and assignRoleToGroup handlers (POST /authz/users/{id}/assign and /authz/groups/{id}/assign) authorize only that the caller may assign roles to the target user or group, not the permissions contained in the assigned roles, unlike role creation which enforces that a user can only create roles with permissions less than or equal to its own. A user holding only the delegated assign_and_revoke_users or assign_and_revoke_groups permission can assign the built-in admin role, or any high-privilege custom role, to itself or others, escalating to full administrative control of the database.	8.8	More Details
CVE-2026-56841	A malicious actor with access to the network and low privileges could exploit an authenticated SQL Injection vulnerability found in UniFi Protect Application to escalate privileges on the host device.	8.8	More Details
CVE-2026-55114	A malicious actor with access to the network and low privileges could exploit an Improper Access Control vulnerability found in UniFi Network Application to escalate privileges within the UniFi Network Application.	8.8	More Details
CVE-2026-14432	Use after free in V8 in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-54404	A malicious actor with access to the network and low privileges could exploit a series of authenticated SQL Injection vulnerabilities found in UniFi OS to escalate privileges within such UniFi OS devices or instances.	8.8	More Details
CVE-2026-34152	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, pre-deployment and post-deployment commands are single-quote escaped but then sent through SSH heredoc transport that preserves newlines, allowing an authenticated user to inject additional shell statements that execute on the remote server during deployment. This issue is fixed in version 4.0.0-beta.471.	8.8	More Details
CVE-2026-27414	Contributor PHP Object Injection in Werkstatt <= 4.8.3 versions.	8.8	More Details

CVE-2026-57759	Unauthenticated Cross Site Request Forgery (CSRF) in ProfileGrid <= 5.9.9.7 versions.	8.8	More Details
CVE-2025-71380	The Execute Command node in n8n allows authenticated users to execute arbitrary commands on the host system where n8n runs. Attackers with user access or compromised credentials can exploit this node to run malicious commands, potentially leading to data exfiltration, service disruption, or complete system compromise.	8.8	More Details
CVE-2026-13125	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. In order to access the websocket server, no authentication is required. As such, any malicious website can attempt to open a connection to the server and potentially access sensitive APIs. In particular, it's possible to call a combination of the `create` method and `getScreenCapture` to retrieve the content of the user's screen.	8.8	More Details
CVE-2026-14535	In Trail of Bits fickling versions up to and including 0.1.11, the UnsafeImportsML analysis pass unconditionally calls AnalysisContext.shorten_code(node) on every import node it inspects, regardless of whether the import is flagged as unsafe. This call registers the shortened code representation in the shared AnalysisContext.reported_shortened_code set. When the MLAllowlist analysis pass subsequently runs, it calls the same shorten_code() method, receives already_reported=True for every import, and executes a continue statement that skips its allowlist check entirely. This renders MLAllowlist dead code for all imports — it never evaluates whether an import is in the ML allowlist or not. The MLAllowlist pass was designed to catch imports of modules outside the known-safe ML ecosystem (torch, numpy, transformers, etc.) that slip past the UnsafeImports denylist. With MLAllowlist inoperative, any standard library module not in the UNSAFE_IMPORTS denylist can be invoked via pickle deserialization while fickling's check_safety() returns LIKELY_SAFE. The fickling.load() API chains check_safety() into pickle.loads() as an explicit security gate, meaning a LIKELY_SAFE verdict causes the payload to be deserialized and executed. The root cause is shared mutable state between independently-correct analysis passes — UnsafeImportsML works as designed in isolation, MLAllowlist works as designed in isolation, but the shared reported_shortened_code set causes UnsafeImportsML to poison MLAllowlist's deduplication logic.	8.8	More Details
CVE-2026-27060	Contributor PHP Object Injection in ARMember Premium <= 7.0 versions.	8.8	More Details
CVE-2026-14534	Trail of Bits fickling versions up to and including 0.1.10 do not include the Python standard library modules _posixsubprocess, site, and atexit in the UNSAFE_IMPORTS denylist (fickle.py). Because these modules are absent from the denylist, fickling's check_safety() function returns LIKELY_SAFE with zero findings for pickle payloads that invoke dangerous functions including _posixsubprocess.fork_exec (C-level process spawner capable of executing arbitrary binaries), site.execsitecustomize (executes arbitrary site customization code), and atexit._run_exitfuncs (triggers all registered exit handler callbacks). The fickling.load() API chains check_safety() into pickle.loads() as an explicit security gate; a LIKELY_SAFE verdict causes the payload to be deserialized and executed. This shares the same root cause as CVE-2026-22607 (cProfile), CVE-2025-67748 (pty), and CVE-2025-67747 (marshal/types). OvertlyBadEvals does not flag these modules because they are standard library imports. UnsafeImports does not flag them because they are not in the denylist. The UnusedVariables heuristic is defeated by the SETITEMS opcode pattern.	8.8	More Details
CVE-2026-23697	Vtiger CRM before 8.4.0 contains an authenticated file upload vulnerability that allows low-privileged users to achieve remote code execution by uploading a .phar file containing arbitrary PHP code through the Documents module, bypassing the extension denylist in config.inc.php which omits the .phar extension. The uploaded file is stored with its original .phar extension under the web-accessible storage directory, and a misconfigured .htaccess using Apache 2.2 syntax is silently ignored on Apache 2.4 deployments, allowing unauthenticated HTTP requests to directly execute the uploaded PHP payload.	8.8	More Details
CVE-2026-56037	Deserialization of Untrusted Data vulnerability in Themify Themify Popup allows Object Injection. This issue affects Themify Popup: from n/a through 1.4.3.	8.8	More Details
CVE-2026-54406	A malicious actor with access to the network and high privileges could exploit a Path Traversal vulnerability found in self-hosted instances of UniFi Network Application to escalate write permission on the host device.	8.7	More Details
CVE-2026-12277	The Frontend File Manager Plugin WordPress plugin through 23.6 does not validate a file path derived from user input before deleting the referenced file, allowing unauthenticated users to delete arbitrary files on the server (such as wp-config.php) when guest upload mode is enabled. Deleting wp-config.php forces the site into its setup routine, which can be leveraged toward a full site takeover.	8.7	More Details
CVE-2026-28737	Gitea versions from 1.25.0 before 1.26.0 allow stored cross-site scripting through the extensionsRequired field in glTF files rendered by the 3D file viewer.	8.7	More Details

CVE-2026-57983	Improper authorization in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature over a network.	8.7	More Details
CVE-2026-57573	Crawl4AI is an open-source LLM-friendly web crawler and scraper. Prior to 0.9.0, the Docker API server applied its SSRF destination check on the non-streaming /crawl path but not on the streaming path. handle_stream_crawl_request passed seed URLs straight to the crawler with no destination validation, allowing a remote unauthenticated client to call POST /crawl/stream or POST /crawl with crawler_config.stream=true with a URL pointing at an internal, private, or link-local address; the server fetched it and streamed the response body back. This issue is fixed in version 0.9.0.	8.6	More Details
CVE-2026-55117	A malicious actor with access to the network could exploit a Path Traversal vulnerability found in UniFi Access Application to access files on the host device.	8.6	More Details
CVE-2026-54403	A malicious actor with access to the network could exploit a Path Traversal vulnerability found in certain devices running UniFi OS to bypass authentication of such UniFi OS devices or instances.	8.6	More Details
CVE-2026-54408	A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi Protect Application to bypass authentication for data streaming.	8.6	More Details
CVE-2026-59707	LocalAI contains an unauthenticated server-side request forgery vulnerability in the POST /models/apply endpoint that allows attackers to fetch arbitrary internal URLs. The endpoint passes unsanitized gallery URL fields directly to gallery.GetGalleryConfigFromURLWithContext without proper validation, enabling attackers to force the server to issue HTTP GET requests to private and loopback ranges with partial response content leaked through error messages.	8.6	More Details
CVE-2026-4249	The throttling event handling mechanism in multiple WSO2 products accepts user-supplied JSON payloads without sufficient validation of their structure and content. This allows an unauthenticated remote attacker to inject malicious JSON data that can lead to a persistent denial of service condition. Successful exploitation of this vulnerability can disrupt the API Gateway, preventing legitimate API traffic from being processed and impacting complete service availability. The denial of service is persistent, requiring manual intervention to restore normal operations.	8.6	More Details
CVE-2026-54407	A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi Protect Application to bypass authentication in certain UniFi Protect Application API endpoints.	8.6	More Details
CVE-2026-55418	FastGPT is an open source AI knowledge base platform. Prior to v4.15.0-beta5, two FastGPT file handlers authorize an unrelated resource and then sign or read an S3 object using a key taken directly from the request, without checking that the key belongs to the caller's team. Because S3 object keys are global within the bucket and carry the tenant id only as a path segment, an attacker can supply another team's key and obtain its file contents through the chat-file presign endpoint or dataset preview endpoint. This issue is fixed in version v4.15.0-beta5.	8.6	More Details
CVE-2026-26231	Gitea versions up to and including 1.26.1 allow the Allow edits from maintainers permission path to authorize commits to repositories that the user can read but should not be able to write.	8.5	More Details
CVE-2026-57765	Contributor SQL Injection in WP EasyCart <= 5.9.0 versions.	8.5	More Details
CVE-2025-69094	Subscriber SQL Injection in Unicamp <= 2.2.2 versions.	8.5	More Details
CVE-2026-57687	Contributor SQL Injection in Custom Field Template <= 2.7.8 versions.	8.5	More Details
CVE-2026-57752	Contributor SQL Injection in iNET Webkit 1.2.4 versions.	8.5	More Details
CVE-2025-53828	SharePoint for ownCloud is an application for using SharePoint with the file storage, synchronization, and sharing application ownCloud Classic. In SharePoint for ownCloud prior to version 0.4.1, which corresponds to ownCloud 10 prior to 10.15.3, an attacker with administrative privileges can use a SSRF vulnerability in the SharePoint app to execute arbitrary code on the system. Upgrade ownCloud 10 to version 10.15.3 or later to receive SharePoint for ownCloud 0.4.1, the fixed version.	8.5	More Details

CVE-2026-57756	Contributor SQL Injection in nicen-localize-image <= 1.4.9 versions.	8.5	More Details
CVE-2026-24260	NVIDIA Container Toolkit for Linux contains a vulnerability where an attacker could cause a time-of-check time-of-use race condition. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, and data tampering.	8.5	More Details
CVE-2026-10055	In Eclipse Theia since version 1.26.0, the backend /services/request-service RPC accepts an attacker-controlled URL from any client connected to the standard /services messaging endpoint, performs the HTTP request server-side, and returns the full response body to the caller. Because the destination URL is neither validated nor allowlisted, a remote attacker with access to the Theia service connection can issue server-side HTTP requests to localhost or other backend-reachable hosts and read their responses, exposing internal administrative endpoints, cloud instance metadata services, and other resources that are intentionally outside the browser network boundary. The vulnerability affects deployments where the Theia service connection is reachable by untrusted users (for example, multi-tenant or publicly-reachable Theia deployments).	8.5	More Details
CVE-2026-44941	A relative path traversal in the "keyhint" option in repomd.xml parsing of libzypp before 17.38.12 can be used by attackers able to supply a malicious repository to inject or overwrite files in the target system as root.	8.4	More Details
CVE-2026-54424	An Incorrect Use of Privileged APIs vulnerability in Unity Parsec on Windows hosts leads to a potential Elevation of Privilege. This issue affects Parsec through v2026-05-04.0. The patched version is Parsec for Windows version 150-104a. A user can generate a situation where there is an instance of parsecd.exe running as NT AUTHORITY\SYSTEM with a user-controlled value of the AppData environment variable.	8.4	More Details
CVE-2026-57265	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. #### audio command index-out-of-bound	8.3	More Details
CVE-2026-14413	Uninitialized Use in ANGLE in Google Chrome prior to 150.0.7871.46 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-14400	Out of bounds write in ANGLE in Google Chrome prior to 150.0.7871.46 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-14401	Insufficient validation of untrusted input in ANGLE in Google Chrome on Android prior to 150.0.7871.46 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-57271	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. #### pause command index-out-of-bound	8.3	More Details
CVE-2026-57272	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. #### byPass command index-out-of-bound	8.3	More Details
CVE-2026-14412	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 150.0.7871.46 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-57273	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. One of them, `connectionInfo` is meant to provide the necessary details to connect to a camera. The handler associated with this command that we call`handle_connection_info` contains multiple	8.3	More Details

	instances of string copy that can overflow. The function `handle_connect_info` copies attacker-controlled JSON strings into fixed-size buffers using manual byte-by-byte loops that do not enforce length limits. #### Buffer Overflow in username field (no key present)		
CVE-2026-57274	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. One of them, `connectionInfo` is meant to provide the necessary details to connect to a camera. The handler associated with this command that we call`handle_connection_info` contains multiple instances of string copy that can overflow. The function `handle_connect_info` copies attacker-controlled JSON strings into fixed-size buffers using manual byte-by-byte loops that do not enforce length limits. #### Buffer Overflow in password field (no key present)	8.3	More Details
CVE-2026-14429	Insufficient validation of untrusted input in Skia in Google Chrome prior to 150.0.7871.46 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-57275	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. One of them, `connectionInfo` is meant to provide the necessary details to connect to a camera. The handler associated with this command that we call`handle_connection_info` contains multiple instances of string copy that can overflow. The function `handle_connect_info` copies attacker-controlled JSON strings into fixed-size buffers using manual byte-by-byte loops that do not enforce length limits. #### Buffer Overflow in username field (key present)	8.3	More Details
CVE-2026-49471	Serena is a powerful MCP toolkit for coding that provides semantic retrieval and editing capabilities. Prior to v1.5.2, Serena's built-in web dashboard exposes an unauthenticated Flask API on a fixed, predictable port, with no authentication, no CSRF protection, and no Host header validation. A DNS rebinding attack allows a malicious webpage to reach this API from any browser and write arbitrary content to the agent's persistent memory store, which the agent reads and acts on autonomously. Combined with execute_shell_command using shell=True, this creates a remote code execution chain requiring only that the victim visit a malicious webpage while Serena is running. This issue is fixed in version v1.5.2.	8.3	More Details
CVE-2026-57276	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. One of them, `connectionInfo` is meant to provide the necessary details to connect to a camera. The handler associated with this command that we call`handle_connection_info` contains multiple instances of string copy that can overflow. The function `handle_connect_info` copies attacker-controlled JSON strings into fixed-size buffers using manual byte-by-byte loops that do not enforce length limits. #### Buffer Overflow in password field (key present)	8.3	More Details
CVE-2026-14427	Heap buffer overflow in Skia in Google Chrome prior to 150.0.7871.46 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-57266	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. #### 2wayAudio command index-out-of-bound	8.3	More Details
CVE-2026-57277	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. One of them, `connectionInfo` is meant to provide the necessary details to connect to a camera. The handler associated with this command that we call`handle_connection_info` contains multiple instances of string copy that can overflow. The function `handle_connect_info` copies attacker-controlled JSON strings into fixed-size buffers using manual byte-by-byte loops that do not enforce length limits. #### Buffer Overflow in key field	8.3	More Details
	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and		

CVE-2026-57278	may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. One of them, `connectionInfo` is meant to provide the necessary details to connect to a camera. The handler associated with this command that we call`handle_connection_info` contains multiple instances of string copy that can overflow. The function `handle_connect_info` copies attacker-controlled JSON strings into fixed-size buffers using manual byte-by-byte loops that do not enforce length limits. #### Buffer Overflow in ip field	8.3	More Details
CVE-2026-57270	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. #### play command index-out-of-bound	8.3	More Details
CVE-2026-58284	Improper authorization in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	8.3	More Details
CVE-2026-14428	Insufficient validation of untrusted input in Dawn in Google Chrome on Android prior to 150.0.7871.46 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-58288	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	8.3	More Details
CVE-2026-13131	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. #### connectInfo command index-out-of-bound	8.3	More Details
CVE-2026-49229	Actual is a local-first personal finance app. Prior to 26.6.0, in OpenID multi-user mode, disabling a user only blocks future OpenID login for that identity, while existing Actual session tokens for the disabled user remain valid. The shared session validation path accepts any existing token row that has not expired without checking whether the associated user is still enabled, allowing a disabled user to continue calling authenticated server endpoints. This issue is fixed in version 26.6.0.	8.3	More Details
CVE-2026-50521	Use after free in Microsoft Edge (Chromium-based) allows an authorized attacker to execute code over a network.	8.3	More Details
CVE-2026-55118	A malicious actor with access to the network,low privileges and under certain conditions could exploit an Improper Access Control vulnerability found in UniFi Network Application to escalate privileges within the UniFi Network Application.	8.3	More Details
CVE-2026-58592	Ladybird contains a dangling-reference memory-safety flaw in its WebAssembly ESM-integration module loader. When a JavaScript function is imported into a WebAssembly module via the ESM path, WebAssemblyModule.cpp passes a stack-local Wasm::FunctionType by reference to create_host_function, whose host callback captures and later reads that reference; once the ESM link-loop iteration ends the FunctionType is destroyed, leaving the callback with a dangling reference (the normal instantiate path uses a long-lived reference and is not affected). Stale result-type data lets the host callback return an empty result vector for a statically non-empty result, so the destination register retains an attacker-influenced value that is then consumed by the WASM-GC array.set handler, which bit-casts the reference low bits to an ArrayInstance pointer after only a null check, yielding an arbitrary write. A web page can chain this into code execution in the WebContent process. Verified reachable from HTML content without any instrumentation or source modification.	8.3	More Details
CVE-2026-58285	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	8.3	More Details
CVE-2026-14389	Integer overflow in Skia in Google Chrome prior to 150.0.7871.46 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	8.3	More Details
	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an		

CVE-2026-13132	addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. #### setStream command index-out-of-bound	8.3	More Details
CVE-2026-58287	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	8.3	More Details
CVE-2026-57267	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. #### snapshot command index-out-of-bound	8.3	More Details
CVE-2026-57268	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. ### saveVideo command index-out-of-bound When sending the `saveVideo` command, the `index` field is extracted from the websocket message [1]. Then without checking the range of the index, it is used to trigger a CriticalSection ([2]) and releases it [3]. The release function call ([3]) is executed using a function pointer which will be read out of bounds potentially leading to code execution: v6 = get_entry(a2, "index"); result = json_is_value_int(v6); if ((_BYTE)result) { v8 = get_entry(a2, "index"); index = json_value_to_int(&v8->value); // [1] result = CCriticalSection::EnterCritSection(&this->crit_sections[index]); //[2] if (result) { if (this->array_of_IPCams[index]) { if (this->array_of_IPCams[index]->field_20) do_PostMessageA((CViewer *)this->array_of_IPCams[index], 0x111u, 0x139Fu, v11); } return (*(int (__thiscall **)(CCriticalSection *))(this->crit_sections[index].vtbl + 20))(&this->crit_sections[index]); //[3] } }	8.3	More Details
CVE-2026-11340	Missing Authorization vulnerability in HAVELSAN Inc. Liman MYS allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Liman MYS: before release.Master.1107.	8.3	More Details
CVE-2026-57269	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. #### disconnect command index-out-of-bound	8.3	More Details
CVE-2026-57264	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. #### setPIP command index-out-of-bound	8.3	More Details
CVE-2026-58295	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature over a network.	8.3	More Details
CVE-2026-57688	Unauthenticated Broken Access Control in POS Entegratör <= 3.7.103 versions.	8.2	More Details
	Improper Neutralization of Special Elements in Data Query Logic vulnerability in Apache Camel Neo4J component. The camel-neo4j producer builds the Cypher WHERE clause for its match/retrieve and delete operations from the CamelNeo4jMatchProperties map. CVE-2025-66169 addressed Cypher injection through the property values by binding them as query parameters ($paramN), but the property names (the JSON keys		

CVE-2026-46591	of that map) were still concatenated into the query string verbatim in Neo4jProducer.retrieveNodes() and deleteNode(). A property name containing Cypher syntax therefore alters the structure of the executed query. Where a route maps untrusted input into the CamelNeo4jMatchProperties map - for example by passing a request body as the match map, or from a consumer that does not filter inbound Camel* headers - an attacker who controls the JSON key names can inject arbitrary Cypher and read, modify or delete any node or relationship in the Neo4j database. The CamelNeo4jMatchProperties header is itself Camel-prefixed and is filtered by the HTTP header-filter strategy, so a plain HTTP client cannot set it directly; the issue is reachable through routes that deliberately or inadvertently carry untrusted data into that header. This issue affects Apache Camel: from 4.10.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. For deployments that cannot upgrade immediately, do not populate the CamelNeo4jMatchProperties map from untrusted input: validate or allow-list the property names (for example against ^[A-Za-z_][A-Za-z0-9_]*$) before the Neo4j producer, and ensure that any consumer feeding such a route filters inbound Camel* / camel* headers so the match header cannot be supplied by an external sender.	8.2	More Details
CVE-2026-59195	pnpm is a package manager. Prior to 10.34.4 and 11.8.0, pnpm accepts package names from the env lockfile configDependencies section and uses those names directly when creating config dependency symlinks under node_modules/.pnpm-config. A malicious repository can commit a crafted pnpm-lock.yaml whose env-lockfile document contains a traversal-shaped config dependency name. During pnpm install, pnpm installs the config dependency and creates a symlink at a path derived from that name. This vulnerability is fixed in 10.34.4 and 11.8.0.	8.2	More Details
CVE-2025-53831	DrawIO for ownCloud is an application for using DrawIO with the file storage, synchronization, and sharing application ownCloud Classic. In DrawIO for ownCloud prior to version 1.0.2, which corresponds to ownCloud 10 prior to version 10.15.3, attackers with access to the DrawIO app can leverage improper neutralization of input during web page generation to achieve stored XSS. Upgrade ownCloud 10 to version 10.15.3 or later or upgrade DrawIO for ownCloud 10 to version 1.0.2 or later to receive a patch.	8.2	More Details
CVE-2026-14336	PIA's OIDC issuer allowlist for Jenkins tokens uses a bare string-prefix check (issuer.startswith(' https://ci.eclipse.org ') in is_issuer_known, pia/models.py:139) instead of validating the issuer as a properly host-bounded URL. An attacker can craft an issuer such as https://ci.eclipse.org@evil.host (userinfo trick) or https://ci.eclipse.org.evil.host (suffix trick) that satisfies the prefix check while pointing the OIDC discovery and JWKS fetches at a server the attacker controls. An unauthenticated caller of POST /v1/upload/sbom can use this to force PIA to make outbound HTTP(S) requests to an arbitrary attacker-chosen host, and to have oidc.verify_token accept a JWT signed with the attacker's own key.	8.2	More Details
CVE-2026-14637	A security vulnerability has been detected in kirilkirkov Ecommerce-CodeIgniter-Bootstrap up to 13fd582aaf49aeab7438acc0fc3eb973a1f5e6a7. The affected element is the function getCartItems in the library application/libraries/ShoppingCart.php. The manipulation of the argument shopping_cart leads to deserialization. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The identifier of the patch is 49b20f53de2b7ec34e920b11c863f1491d911a04. It is recommended to apply a patch to fix this issue.	8.2	More Details
CVE-2026-53906	MCO is vulnerable to Path Disclosure and Path Traversal in file handling functionality related to data export and upload. Improper validation of the filename parameter allows writing files to arbitrary locations as well as indirect disclosure of absolute server paths through error messages. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 25.3.3.1 but may also affect other versions.	8.2	More Details
CVE-2026-8377	Missing Authorization vulnerability in Armiya Information Technologies Ltd. Co. Access Control System (GKS) allows Collect Data from Common Resource Locations. This issue affects Access Control System (GKS): before Version 2.	8.2	More Details
CVE-2026-11348	Improper verification of cryptographic signature vulnerability in HAVELSAN Inc. Liman MYS allows Fake the Source of Data. This issue affects Liman MYS: before release.Master.1107.	8.1	More Details
CVE-2026-55119	A malicious actor with access to the network and low privileges could exploit an Improper Access Control vulnerability found in UniFi Talk Application to escalate privileges within the UniFi Talk Application.	8.1	More Details
CVE-2026-49297	Apache Airflow's Google provider operators `GCSToSFTPOperator` and `GCSTimeSpanFileTransformOperator` joined GCS object names returned by the bucket listing API directly to a destination filesystem path without normalisation or containment check. A user with write access to the source GCS bucket (typically a different trust principal than the DAG author — partner uploads, ingest-only service accounts, public-data buckets) could create an object whose name contains `..` segments and cause the DAG run to write the downloaded blob outside the configured destination (the SFTP `destination_path` for `GCSToSFTPOperator`; the worker-local temp directory for `GCSTimeSpanFileTransformOperator`), enabling overwrite of arbitrary files on the SFTP server or the worker host. Affects deployments that ingest from buckets writable by less-trusted principals. Users are advised to upgrade to `apache-airflow-providers-google` 22.2.1 or later.	8.1	More Details

CVE-2026-28744	Gitea versions up to and including 1.26.1 allow Git smart HTTP requests authenticated with bearer tokens to bypass repository token scope checks.	8.1	More Details
CVE-2026-58293	External control of file name or path in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	8.1	More Details
CVE-2026-42382	Unauthenticated Local File Inclusion in Audrey <= 1.5 versions.	8.1	More Details
CVE-2026-9272	In Progress Flowmon ADS versions prior to 12.5.6 and 13.0.5, a vulnerability exists whereby an adversary who is authenticated as a low-privileged user in the Anomaly Detection System (ADS) may send specially crafted requests that could result in unauthorized access to application data and its modification.	8.1	More Details
CVE-2025-71360	picklescan before 0.0.29 fails to detect malicious pickle files using idlelib.calltip.get_entity function in reduce methods. Attackers can embed undetected code in pickle files that executes remote commands when loaded by victims.	8.1	More Details
CVE-2026-7311	The TinyPNG – JPEG, PNG & WebP image compression plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_converted_image_size function in all versions up to, and including, 3.6.13. This makes it possible for authenticated attackers, with author-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). An attacker can exploit this by injecting an arbitrary server file path into the 'convert.path' field of the 'tiny_compress_images' post meta on an attachment they own, then triggering attachment deletion to invoke the vulnerable code path.	8.1	More Details
CVE-2025-71359	picklescan before 0.0.29 fails to detect malicious pickle payloads that utilize lib2to3.pgen2.grammar.Grammar.loads in the reduce method, allowing remote code execution. Attackers can craft pickle files embedding dangerous code that evades picklescan detection and executes during pickle.load() deserialization.	8.1	More Details
CVE-2026-10750	The Royal MCP WordPress plugin before 1.4.26 does not perform capability checks on the majority of its MCP tools after token authentication, allowing authenticated users with a low-privileged role such as Subscriber to read private content, enumerate all users and their roles, and create, modify, or delete content owned by other users.	8.1	More Details
CVE-2026-44454	Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7 and 2.30.2, the `dotfiles` registry module passed unsanitized user input to shell commands, allowing arbitrary code execution inside a provisioned workspace. Any user who supplied a crafted `dotfiles_uri` value (for example, one containing shell command substitution such as `$(...)`) could achieve command execution in their own workspace. The Create Workspace page's `mode=auto` deep links amplified this into a one-click attack: an attacker could craft a URL that prefilled `param.dotfiles_uri` and silently provisioned a workspace with the attacker-controlled value, with no explicit user confirmation. In versions 2.29.7 and 2.30.2, input validation was added to the dotfiles module to reject URIs and usernames containing special characters, and the unsafe `eval`/`sh -c` usage was removed. This eliminated the command injection at its source.	8.1	More Details
CVE-2026-58286	Improper access control in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	8.1	More Details
CVE-2025-71345	picklescan before 0.0.30 fails to detect malicious pickle files that invoke torch.utils.bottleneck.__main__.run_autograd_prof function. Attackers can embed undetected code in pickle files that executes during deserialization, enabling remote code execution.	8.1	More Details
CVE-2026-13020	A Weak Password Recovery Mechanism for Forgotten Password exists in Esri Portal for ArcGIS versions 12.1 and earlier on Windows, Linux and Kubernetes. A remote, unauthorized attacker may assume ownership of a user’s account by manipulating this mechanism. ArcGIS Administrators should configure an email server with ArcGIS Enterprise to facilitate user self-service password recovery. The ability for an administrator to reset a user’s password remains unchanged.	8.1	More Details
CVE-2025-71356	picklescan before 0.0.28 fails to detect malicious torch.fx.experimental.symbolic_shapes.ShapeEnv.evaluate_guards_expression function calls in pickle files. Attackers can embed undetected code in pickle files that executes remote code when loaded by victims.	8.1	More Details
CVE-2026-58283	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	8.1	More Details
CVE-	Improper access control in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform		More

2026-58282	spoofing over a network.	8.1	Details
CVE-2026-11794	The Advanced Form Integration — Connect Forms to 200+ Apps WordPress plugin before 2.1.1 does not restrict the WordPress role assigned when it creates a user from a public form submission, allowing unauthenticated visitors to create an administrator account when an active integration maps the user role to a public form field. This requires a specific, non-default multi-Advanced Form Integration — Connect Forms to 200+ Apps WordPress plugin before 2.1.1 configuration.	8.1	More Details
CVE-2026-50721	Libreswan, via the function RSA_authenticate_hash_signature_raw_rsa(), did not correctly verify the length of the authentication hash when the SIG payload of an IKEv1 packet was encoded using PKCS #1 RSA Encryption as per RFC 2313. A remote attacker can use a variation on the Bleichenbacher attack to forge the SIG payload when small public exponents are being used (e.g., e=3), which could lead to impersonation. Additionally, a remote attacker, by encoding a shorter than expected hash in the SIG payload, could trigger an assertion leading to denial-of-service. The daemon aborts and restarts; continued exploitation causes sustained denial of service. Remote code execution is not possible. X.509 certificate verifications of remote IKE peers are not affected.	8.1	More Details
CVE-2026-50722	Libreswan, via the function RSA_authenticate_hash_signature_pkcs1_1_5_rsa(), did not correctly verify the DER encoding of the ASN.1 digest when the IKEv2 AUTH payload was encoded using RSASSA-PKCS1-v1_5 (RFC 8017). A remote attacker can use a variation on the Bleichenbacher attack to forge the AUTH payload when small public exponents are used (e.g., e=3), leading to impersonation. Additionally, a remote attacker, by encoding a shorter than expected hash in the AUTH payload, could trigger an assertion leading to denial-of-service. The daemon aborts and restarts; continued exploitation causes sustained denial of service. Remote code execution is not possible. X.509 certificate verifications of the remote IKE peer are not affected.	8.1	More Details
CVE-2026-12083	The Admin and Site Enhancements (ASE) WordPress plugin before 8.8.4, admin-site-enhancements-pro WordPress plugin before 8.8.4 does not perform authentication, authorization, or nonce checks on a role-restoration request handler, allowing unauthenticated attackers to restore a previously demoted administrator account back to the administrator role. This is an incomplete fix of CVE-2024-43333 / CVE-2025-24648, which closed the issue for only one of the demotion paths the WordPress role API exposes.	8.1	More Details
CVE-2025-71353	picklescan before 0.0.28 fails to detect malicious pickle files that exploit torch._dynamo.guards.GuardBuilder.get function in reduce methods. Attackers can craft pickle files with embedded code that evades picklescan detection and executes arbitrary commands when loaded.	8.1	More Details
CVE-2025-71342	picklescan before 0.0.30 fails to detect malicious pickle files using idlelib.run.Executive.runcode in reduce methods. Attackers can embed undetected code in pickle files that executes during pickle.load, enabling remote code execution in PyTorch models and supply chain attacks.	8.1	More Details
CVE-2025-71343	picklescan before 0.0.30 fails to detect malicious pickle files that exploit lib2to3.pgen2.pgen.ParserGenerator.make_label function in the reduce method. Attackers can craft malicious pickle files with embedded code that evades detection but executes arbitrary commands when pickle.load() is called.	8.1	More Details
CVE-2026-57751	Unauthenticated Cross Site Request Forgery (CSRF) in Heateor Social Login <= 1.1.39 versions.	8.1	More Details
CVE-2026-42527	Deserialization of Untrusted Data vulnerability in Apache Camel. The default ObjectInputFilter pattern shipped with several Apache Camel components for defense-in-depth deserialization filtering ('java.**;javax.**;org.apache.camel.**;!*', or the no-'javax.**' variant in the aggregation-repository components) uses a recursive 'java.**' glob that admits classes whose hashCode/equals/readObject methods perform network I/O, notably java.net.URL and java.net.InetAddress. When an attacker can deliver a Java-serialized payload to an affected Camel consumer, deserialization of a HashMap (or any collection that calls hashCode on its elements) containing java.net.URL keys causes the JVM to issue DNS queries to the attacker-supplied host during the deserialization side-effect. The class-level filter check passes because the resulting object's class (HashMap) is allow-listed; the DNS query is observable on an attacker-controlled DNS server, providing an out-of-band side channel. The exposure is highest on the camel-jms family because JmsBinding.extractBodyFromJms invokes ObjectMessage.getObject() unconditionally when mapJmsMessage=true (default). Affected components: camel-jms, camel-sjms, camel-amqp, camel-mina, camel-netty, camel-netty-http, camel-vertx-http, camel-infinispan, and the aggregation repository components camel-leveldb, camel-cassandraql, camel-consul, camel-sql (JDBC aggregation repository). This issue affects Apache Camel: from 4.14.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to a version that contains the CAMEL-23372 fix once available: 4.21.0 for the 4.21.x line, 4.18.3 for the 4.18.x line, and 4.14.8 for the 4.14.x line. For deployments that cannot upgrade immediately, configure a JMS-provider-side allow-list (Apache ActiveMQ Artemis 'deserializationAllowList' / 'deserializationDenyList', Apache ActiveMQ Classic 'org.apache.activemq.SERIALIZABLE_PACKAGES') as the primary mitigation, and/or override the in-code default via the endpoint-level 'deserializationFilter' option or the JVM-wide '-Djdk.serialFilter' system property with an explicit deny: '!java.net.**;java.**;javax.**;org.apache.camel.**;!*' (or '!java.net.**;java.**;org.apache.camel.**;!*' for the aggregation-repository components, which do not include javax.**).	8.1	More Details

CVE-2026-43865	Deserialization of Untrusted Data vulnerability in Apache Camel Hazelcast component. The camel-hazelcast component creates and manages Hazelcast instances using a default configuration that applies no Java deserialization filter. When Camel builds the Hazelcast Config itself - that is, when no user-supplied HazelcastInstance, hazelcastConfigUri, or referenced Config bean is provided - neither Hazelcast's JavaSerializationFilterConfig nor a Camel-side ObjectInputFilter is configured, so objects received over the Hazelcast cluster protocol are deserialized inside Hazelcast's own serialization layer (ObjectInputStream.readObject) before Camel ever processes them. An attacker who can join or otherwise reach the Hazelcast cluster can publish a crafted serialized Java object that is then deserialized on every Camel node, resulting in remote code execution. The exposure is present by default and requires no opt-in endpoint configuration: any route using a hazelcast consumer (hazelcast-topic, hazelcast-queue, hazelcast-seda, hazelcast-map, hazelcast-multimap, hazelcast-replicatedmap, hazelcast-list, hazelcast-set), as well as the HazelcastAggregationRepository and HazelcastIdempotentRepository, is affected whenever the managed instance is created from Camel's default configuration. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix makes Camel apply a default Hazelcast JavaSerializationFilterConfig (whitelisting the java., javax. and org.apache.camel. class-name prefixes and blacklisting java.net.) to instances it creates from its own default configuration, while leaving any user-supplied Config or HazelcastInstance untouched. For deployments that cannot upgrade immediately, configure a deserialization filter on the Hazelcast instance (Hazelcast JavaSerializationFilterConfig, or the JVM-wide system property -Djdk.serialFilter=!java.net.**;java.**;javax.**;org.apache.camel.**;!*) and enable Hazelcast cluster authentication and TLS to restrict who can reach the cluster.	8.1	More Details
CVE-2025-71347	picklescan before 0.0.33 fails to detect malicious pickle files using numpy.f2py.crackfortran.param_eval function in reduce methods, allowing attackers to bypass security checks. Remote attackers can embed undetected code in pickle files that executes during deserialization, enabling arbitrary code execution in applications loading untrusted pickle data.	8.1	More Details
CVE-2026-40859	Deserialization of Untrusted Data vulnerability in Apache Camel. The camel-vertx-http component deserializes HTTP response bodies carrying the Content-Type application/x-java-serialized-object using a raw java.io.ObjectInputStream, without applying any ObjectInputFilter (VertxHttpHelper.deserializeJavaObjectFromStream) This deserialization path is reached only when the producer endpoint is configured with transferException=true (or the component-level allowJavaSerializedObject=true) and throwExceptionOnFailure is left at its default value of true; in that case a backend HTTP response with a 5xx status and the application/x-java-serialized-object content type has its body deserialized with no class restrictions. An attacker who controls the backend the Camel producer talks to - through a man-in-the-middle position on an unencrypted (plain HTTP) connection, or by compromising the backend service - can return a crafted serialized Java object and, if a suitable gadget chain is present on the classpath, achieve remote code execution on the Camel application host. The path is not reachable in the default configuration, where transferException is false. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.20.0. Users are recommended to upgrade to version 4.20.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, the deserialization performed by both helper utilities is constrained by a default ObjectInputFilter (allow-list java.**;javax.**;org.apache.camel.**;!*), which can be customised through the new deserializationFilter endpoint option or the JVM-wide -Djdk.serialFilter system property. For deployments that cannot upgrade immediately: do not enable transferException=true (or allowJavaSerializedObject=true) on producers that talk to untrusted or network-reachable backends; ensure producer connections use TLS (https) so that a response cannot be substituted by a man-in-the-middle; and, where the option is required, set an explicit -Djdk.serialFilter allow-list (for example java.**;org.apache.camel.**;!*) to constrain deserialization.	8.1	More Details
CVE-2025-71362	picklescan before 0.0.33 fails to detect unsafe deserialization when numpy.f2py.crackfortran functions call eval on arbitrary strings. Attackers can embed malicious code in pickle files that executes when loaded from untrusted sources.	8.1	More Details
CVE-2025-71372	Picklescan before 0.0.33 fails to detect the numpy.f2py.crackfortran.getlincoef gadget in pickle __reduce__ methods, allowing arbitrary code execution. Attackers can craft malicious pickle files that execute arbitrary Python code when loaded, bypassing Picklescan's safety checks and enabling supply-chain poisoning of shared model files.	8.1	More Details
CVE-2026-5821	The Image Optimizer plugin for WordPress is vulnerable to arbitrary file deletion in versions up to and including 1.7.4. This is due to insufficient path validation in the Image_Backup::remove() function where backup file paths stored in post meta are used directly in file deletion operations without verifying they are within the uploads directory. The plugin stores backup file paths in the image_optimizer_metadata post meta field and trusts these paths completely when deleting backups on the delete_attachment hook. An authenticated attacker with Author-level access can edit the image_optimizer_metadata post meta on their own attachments via WordPress's Custom Fields interface, injecting arbitrary absolute file paths into the backups array. When the attacker subsequently deletes the attachment, the plugin calls File_System::delete()	8.1	More Details

	on each path without validation. This makes it possible for authenticated attackers, with Author-level access and above, to delete arbitrary files on the server within the web server's filesystem permissions, potentially leading to denial of service, data loss, or security degradation.		
CVE-2025-71366	picklescan before 0.0.28 fails to detect malicious torch.utils.bottleneck.__main__.run_cprofile function calls in pickle files, allowing attackers to bypass safety checks. Remote attackers can embed undetected code in pickle files to achieve arbitrary code execution when victims load the files.	8.1	More Details
CVE-2026-22555	Gitea versions before 1.26.0 allow API users to fork a repository into an organization without first passing the CanCreateOrgRepo check, which can expose organization secrets.	8.1	More Details
CVE-2025-71364	picklescan before 0.0.30 fails to detect the asyncio.unix_events._UnixSubprocessTransport._start function in pickle reduce methods, allowing remote code execution. Attackers can craft malicious pickle files embedding this built-in function that evade detection but execute arbitrary commands when loaded.	8.1	More Details
CVE-2025-58902	Unauthenticated Local File Inclusion in Lighthouse <= 1.2.12 versions.	8.1	More Details
CVE-2026-27412	Unauthenticated Local File Inclusion in Pearl - Corporate Business <= 3.4.10 versions.	8.1	More Details
CVE-2025-71375	picklescan before 0.0.34 fails to detect the _operator.methodcaller built-in function when scanning pickle files for malicious code. Attackers can craft malicious pickle payloads using _operator.methodcaller that evade detection and execute arbitrary code when loaded by pickle.load().	8.1	More Details
CVE-2025-71373	picklescan before 0.0.33 fails to detect operator.methodcaller function calls in pickle files, allowing attackers to bypass security checks. Remote attackers can craft malicious pickle payloads using operator.methodcaller that execute arbitrary code when loaded, compromising systems relying on picklescan for validation.	8.1	More Details
CVE-2026-53903	MCO is vulnerable to an Insecure Direct Object Reference (IDOR) vulnerability in the /customer/servlet/mco/webapi/trading-document/fetchPdfStatement endpoint. The application does not properly validate whether an authenticated user is authorized to access a requested document, allowing direct retrieval based on a user-supplied identifier. An attacker can access trading documents belonging to other users by providing a valid document ID. Although exploitation requires guessing the identifier, predictable ID patterns enable feasible enumeration, leading to unauthorized disclosure of sensitive information. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 25.3.3.1 but may also affect other versions.	8.1	More Details
CVE-2026-40138	A critical pre-authentication vulnerability exists in the authentication subsystem of BeyondTrust Remote Support and Privileged Remote Access. Improper validation of authentication data may allow a network-positioned attacker to bypass access controls and gain unauthorized access to the appliance, including accounts with elevated privileges. Exploitation requires a specific authentication configuration to be enabled	8.1	More Details
CVE-2026-28699	Gitea versions up to and including 1.26.1 allow OAuth2 access token scope enforcement to be bypassed through HTTP Basic authentication.	8.1	More Details
CVE-2026-14471	Improper Neutralization of Special Elements in the metrics-service retention policy management component in Amazon mcp-gateway-registry before 1.0.13 might allow an authenticated remote user to execute arbitrary SQL queries via a crafted table_name value that is interpolated into SQL statements in identifier position. To remediate this issue, users should upgrade to version 1.0.13 or later.	8.1	More Details
CVE-2026-59712	Leantime's Users::getUser method in the JSON-RPC API lacks proper authorization checks, allowing authenticated users to retrieve full user credential rows including password hashes, TOTP secrets, and session tokens. Attackers can exploit this by calling users.getUser with arbitrary user IDs to enumerate all accounts and obtain credentials for offline password cracking, 2FA bypass, and session hijacking.	8.1	More Details
CVE-2026-12746	Dancer2::Plugin::Auth::OAuth::Provider versions before 0.23 for Perl do not support the OAuth 2.0 state parameter. The authentication_url method builds the provider authorization redirect without issuing a state value, and the callback method exchanges the callback code and registers the resulting token into the session without verifying that the callback corresponds to an authorization request this session initiated. Any application that uses this plugin for OAuth 2.0 login is exposed to login cross-site request forgery: because the callback is not bound to the session that began the flow, an attacker who starts an authorization with their own provider account can deliver the resulting callback to a victim, causing the victim's session to complete the attacker's authorization and associating the attacker's provider identity and access token with that session. Where the application persists this as an account link, the attacker may retain access to the victim's account through their own provider credentials.	8.1	More Details
	picklescan before 0.0.28 fails to detect malicious pickle files that use		

CVE-2025-71369	torch.utils.data.datapipes.utils.decoder.basichandlers in reduce methods, allowing attackers to bypass safety checks. Remote attackers can embed undetected malicious code in pickle files that executes during deserialization, enabling remote code execution.	8.1	More Details
CVE-2025-71367	picklescan before 0.0.34 fails to detect _operator.attrgetter function calls in pickle payloads, allowing attackers to bypass security checks. Remote attackers can craft malicious pickle files using _operator.attrgetter in reduce methods to execute arbitrary code when pickle.load() processes the file.	8.1	More Details
CVE-2026-12740	Plack::Middleware::OAuth versions through 0.10 for Perl do not support the OAuth 2.0 state parameter. RequestTokenV2 builds the provider authorization redirect without issuing a state value, and AccessTokenV2 exchanges the callback code and registers the resulting token into the session (register_session) without verifying that the callback corresponds to an authorization request this session initiated. Any application that uses this middleware for OAuth 2.0 login is exposed to login cross-site request forgery: because the callback is not bound to the session that began the flow, an attacker who starts an authorization with their own provider account can deliver the resulting callback to a victim, causing the victim's session to complete the attacker's authorization and associating the attacker's provider identity and access token with that session. Where the application persists this as an account link, the attacker may retain access to the victim's account through their own provider credentials.	8.1	More Details
CVE-2026-5120	A Race Condition vulnerability affecting BIOVIA Workbook from Release 2021 through Release 2026 could allow a user to access unauthorized data from another user.	8.1	More Details
CVE-2026-59713	Leantime contains an OIDC login CSRF vulnerability in the verifyState() method that unconditionally returns true without validating state parameters. Attackers can craft malicious callback URLs with attacker-controlled authorization codes to perform session fixation, logging victims in as the attacker.	8.1	More Details
CVE-2026-8286	A vulnerability exists where a new transfer that uses STARTTLS to upgrade the connection might reuse an existing live connection even though the TLS configuration mismatches so it should not.	8.1	More Details
CVE-2026-10538	Messaging consumer functionality allows deserialization of user-controlled data without sufficient restriction of allowed object types in the out of support Control-M/Server and Control-M/Enterprise Manager versions 9.0.20.x and potentially earlier. This issue may allow an authenticated attacker to trigger unintended server-side behavior through crafted serialized content.	8.0	More Details
CVE-2026-49091	Improper Output Neutralization for Logs (CWE-117) in Kibana can lead to log injection via Log Injection-Tampering-Forging (CAPEC-93). An attacker can supply specially crafted input that is written to log files without proper neutralization. When the log files are subsequently viewed in a terminal that interprets control sequences, the injected content may alter the displayed log data.	8.0	More Details
CVE-2026-14476	A path traversal flaw was found in SSSD's AD GPO provider. The ad_gpo_extract_smb_components() function does not sanitize .. sequences in the gPCFileSysPath LDAP attribute, allowing an attacker with AD GPO management access to write files outside the GPO cache directory as root. On default RHEL configurations with SELinux enforcing, this can be used to inject Kerberos configuration leading to authentication bypass.	8.0	More Details
CVE-2026-34171	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the GET /invitations/{uuid} endpoint can perform a state-changing password reset using an attacker-known invitation UUID, allowing an attacker who can cause a victim to visit the crafted invitation URL to reset the victim account password to a predictable value. This issue is fixed in version 4.0.0-beta.471.	8.0	More Details
CVE-2025-53829	ownCloud is a file storage, synchronization, and sharing application. In ownCloud 10 prior to version 10.15.3, an attacker with administrative privileges can exploit a path traversal vulnerability in the system to execute arbitrary code. Upgrade ownCloud 10 to version 10.15.3 or later to receive a patch.	8.0	More Details
CVE-2026-11766	The Ultimate Member WordPress plugin before 2.12.0 does not properly sanitise and escape the value of custom textarea profile fields before outputting it on user profiles, allowing authenticated users with Subscriber-level access and above to store JavaScript that executes when any user, including an administrator, views the affected profile.	8.0	More Details
CVE-2026-12250	Invocation of process using visible sensitive information vulnerability in TUBITAK BILGEM Software Technologies Research Institute Pardus Domain Joiner allows Excavation. This issue affects Pardus Domain Joiner: from 0.5.2 before 0.5.4.	7.9	More Details
CVE-2026-54074	Tina is a headless content management system. @tinacms/cli versions prior to 2.4.3 contain a Remote Code Execution vulnerability in the Forestry-to-Tina migration command. The internal helper addVariablesToCode unquotes any value matching the marker "__TINA_INTERNAL__:::(.*?):::" inside the stringified collection JSON. User-supplied label and name fields from .forestry/**/*.yml are placed into that JSON without any sanitisation. An attacker who controls a Forestry-style project can therefore inject arbitrary JavaScript into the generated tina/templates.{ts,js} file. The injected code is written at module top level, so it executes the moment the developer runs tinacms dev or tinacms build, with the developer's privileges. This issue has been fixed in version 2.4.3.	7.8	More Details

CVE-2026-42958	The application contains a use-after-free vulnerability that can be exploited to cause memory corruption while parsing specially crafted files. This could allow an attacker to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2026-24250	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause improper validation of allowed inputs. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	7.8	More Details
CVE-2026-6509	Missing Authorization vulnerability in TUBITAK BILGEM Software Technologies Research Institute Pardus Update allows Privilege Escalation. This issue affects Pardus Update: from <=0.6.3 before 0.6.6.	7.8	More Details
CVE-2026-46680	containerd is an open-source container runtime. In versions prior to 1.7.32, 2.0.9, 2.2.4 and 2.3.1, containers launched with a numeric User directive that cannot be parsed as a 32-bit integer are incorrectly treated as a username, leading to runAsNonRoot evasion. If a crafted image provides an /etc/passwd file mapping this large numeric string to root, the container ultimately runs as root (UID 0). This allows the Kubernetes runAsNonRoot restriction to be bypassed, causing unexpected behavior for environments that require containers to run as a non-root user. This issue has been fixed in versions 1.7.32, 2.0.9, 2.2.4 and 2.3.1.	7.8	More Details
CVE-2026-12168	An improper validation vulnerability for driver `GFAC_Sys_x64.sys` in Little Orbit GFAC allows a local attacker to escalate privileges to SYSTEM and execute arbitrary code in kernel mode via crafted messages sent through a Minifilter communication port.	7.8	More Details
CVE-2026-25271	Memory Corruption when processing asynchronous input parameters due to improper handling of modified values between check and use.	7.8	More Details
CVE-2026-38972	Notepad3 through 6.25.822.1 contains a DLL search-order hijacking vulnerability in the About-dialog code path in src/Notepad3.c. The application calls LoadLibrary(L"MSFTEDIT.DLL") with a bare DLL name, which allows a local attacker to place a malicious MSFTEDIT.DLL in the application directory or another preferred DLL search location and achieve arbitrary code execution in the context of the user when the About dialog is opened.	7.8	More Details
CVE-2026-49033	The application contains a stack-based buffer overflow vulnerability that can be exploited by an attacker to execute arbitrary code.	7.8	More Details
CVE-2026-12167	The Minifilter communication port for driver `GFAC_Sys_x64.sys` in Little Orbit GFAC allows a local attacker to access privileged driver functionality via a communication interface that lacks appropriate access restrictions.	7.8	More Details
CVE-2026-24251	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause improper control of dynamically managed code resources. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	7.8	More Details
CVE-2026-21379	Memory Corruption when allocating memory with sizes that exceed the maximum allowed value.	7.8	More Details
CVE-2026-24247	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	7.8	More Details
CVE-2026-14191	An out-of-bounds heap write exists in the RAR5 recovery-volume (.rev) parser in WinRAR and UnRAR (RecVolumes5::ReadHeader in recvol5.cpp). The RecItems vector is sized only when the first .rev file in a set is processed; subsequent .rev files supply an independent RecNum value that is validated against that file's own TotalCount field but never against the actual size of RecItems. A crafted set of two or more .rev files can therefore write an attacker-controlled 32-bit value (the header's RevCRC field) to RecItems[RecNum] at an attacker-controlled offset up to 65534 * sizeof(RecVolItem) bytes past the allocation, corrupting adjacent heap objects. Triggering requires the victim to run a recovery/test operation on an attacker-supplied .rev set (for example 'unrar t x.part1.rev', WinRAR 'Repair archive', or auto-recovery when extracting a volume set with a missing .rar part). This is the RAR5-path sibling of CVE-2023-40477 (which was fixed in the RAR3 path only in WinRAR 6.23). Fixed in WinRAR / RAR 7.23.	7.8	More Details
CVE-2026-24243	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	7.8	More Details
CVE-2026-24244	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	7.8	More Details
CVE-	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause deserialization of		

2026-24245	untrusted data. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	7.8	More Details
CVE-2026-24246	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause improper control of dynamically managed code resources. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	7.8	More Details
CVE-2026-24240	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	7.8	More Details
CVE-2026-24242	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause server-side request forgery. A successful exploit of this vulnerability might lead to information disclosure.	7.8	More Details
CVE-2026-14606	A security flaw has been discovered in RT-Thread up to 5.0.2. Affected by this issue is the function CAN_Receive in the library bsp/synwit/libraries/SWM341_CSL/CMSIS/DeviceSupport/SWM341.h of the component SWM341 CAN Handler. Performing a manipulation results in stack-based buffer overflow. The attack needs to be approached locally. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.8	More Details
CVE-2026-24248	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause improper control of code generation. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	7.8	More Details
CVE-2026-24249	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	7.8	More Details
CVE-2026-57851	MSI Feature Manager contains a local privilege escalation vulnerability in the KernCoreLib64.sys kernel driver that allows any locally logged-on user to perform arbitrary physical memory read/write and unrestricted I/O port operations by accessing exposed IOCTL handlers without administrator privileges. Attackers can exploit the accessible device object through IOCTL handlers to manipulate kernel objects, tamper with kernel-mode callbacks, bypass Protected Process Light protections, and disable security software.	7.8	More Details
CVE-2026-14605	A vulnerability was identified in RT-Thread up to 5.0.2. Affected by this vulnerability is the function recvmsg in the library bsp/loongson/ls1cdev/libraries/ls1c_can.h of the component ls1c CAN Handler. Such manipulation leads to stack-based buffer overflow. Local access is required to approach this attack. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.8	More Details
CVE-2026-34044	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.466, the Logs::mount() component looks up resources by UUID without scoping the lookup to the current team, allowing an authenticated user to access logs for applications owned by other teams by supplying a victim resource UUID. This issue is fixed in version 4.0.0-beta.466.	7.7	More Details
CVE-2026-59095	LobeChat before 2.2.10-canary.18 contains a server-side request forgery vulnerability that allows authenticated attackers to direct internal HTTP requests to arbitrary URLs by supplying user-controlled input to the skill import service (importFromUrl) and topic cover update (fetchImageFromUrl) endpoints, which use the global fetch without the project's ssrf-safe-fetch wrapper. Attackers can target internal addresses such as cloud instance metadata endpoints through these unprotected code paths to disclose internal service responses and cloud credentials.	7.7	More Details
CVE-2026-9165	A flaw was found in Red Hat Advanced Cluster Security for Kubernetes (RHACS). Central does not limit the depth of GraphQL queries served on the authenticated GraphQL API. An authenticated user with a valid API token can send deeply nested queries that cause excessive resource consumption in Central, resulting in a denial of service for the management plane.	7.7	More Details
CVE-2026-54401	A malicious actor with access to the network and low privileges could exploit a Server-Side Request Forgery (SSRF) to escalate privileges within such UniFi OS devices or instances.	7.7	More Details
CVE-2026-59092	JuiceFS through 1.3.1, fixed in commit a46979c, contains an authentication bypass vulnerability that allows unauthenticated remote attackers to access sensitive debug and metrics endpoints by exploiting improper handler registration on the shared http.DefaultServeMux. Attackers can request the /debug/pprof/cmdline endpoint to obtain the process command line containing metadata engine connection strings with database credentials, granting full read/write access to filesystem metadata, while other pprof handlers leak internal state and profiling handlers enable denial of service.	7.7	More Details
CVE-2026-	HashiCorp Terraform Enterprise contained an issue in its version control system (VCS) ingestion of registry modules that did not correctly enforce the intended boundary on packaged module content. This may allow an authenticated user to include files from outside the intended repository content in a module and then download them, potentially exposing sensitive files readable by the ingestion process. This vulnerability, CVE-	7.7	More Details

14468	2026-14468, is fixed in Terraform Enterprise v2.0.4 and v1.2.4.		
CVE-2026-54607	FastGPT is a knowledge-based AI application platform. Prior to 4.15.0-beta4, the HTTP-tool OpenAPI schema importer validates only the top-level URL before passing it to SwaggerParser.bundle, whose remote reference resolver fetches $ref URLs without FastGPT's internal-address guard and returns fetched content inline, allowing an authenticated team member to read internal services or cloud metadata. This issue is fixed in version 4.15.0-beta4.	7.7	More Details
CVE-2026-58460	react-native-receive-sharing-intent contains a path traversal vulnerability that allows a co-resident malicious application to write files outside the intended cache directory by supplying a crafted _display_name value containing dot-dot path components through a malicious ContentProvider. Attackers can fire an explicit ACTION_SEND intent at the consuming app's exported share-receiver activity to overwrite arbitrary files in the consuming app's private data directory, including databases, shared preferences, and cached configuration, with attacker-controlled content.	7.7	More Details
CVE-2026-58423	LFS authentication bypass via malformed SSH sub-verb allows unauthorized read access to private repositories	7.7	More Details
CVE-2026-6901	Untrusted Search Path vulnerability in B&R Industrial Automation GmbH APROL. This issue affects APROL: before R 4.4-01P5.	7.7	More Details
CVE-2026-7831	UltraVNC viewer through 1.8.2.2 contains an off-by-one stack buffer overflow in the RFB ServerInit message handler. In vncviewer/ClientConnection.cpp, when the server-supplied nameLength equals exactly 2024 the code declares a 2024-byte stack buffer _dn[2024] and calls ReadString(_dn, 2024). ReadString writes the NUL terminator at buf[length], i.e., _dn[2024], one byte past the end of the stack buffer. A malicious VNC server can trigger this condition by advertising a desktop name of length 2024 in its ServerInit message. On release builds without stack canaries the single-byte NUL overwrite adjacent stack data. On builds with /GS stack protection the canary is corrupted and the process terminates, resulting in denial of service. User interaction (connecting the viewer to the malicious server) is required.	7.6	More Details
CVE-2026-6687	FatFs R0.16 and earlier contains a stack overflow bug in f_getlabel() because exFAT label length (XDIR_NumLabel) is trusted without enforcing spec maximums. This maps to CWE-121 (Stack-based Buffer Overflow). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (7.6, High). The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Total.	7.6	More Details
CVE-2026-6688	FatFs R0.16 and earlier contains a downstream-caller vulnerability pattern associated with FatFs long filename handling. With LFN enabled, fno.fname can be up to 255 characters; many callers copy it into short fixed buffers without bounds checks, causing overflow. This maps to CWE-120 (Buffer Copy without Checking Size of Input). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (7.6, High). The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Total.	7.6	More Details
CVE-2026-6682	In FatFS R0.16 and earlier contains a FAT32 integer overflow bug in mount_volume() where fasize *= fs->n_fats can wrap, leading to attacker-controlled file-size metadata and unsafe read lengths in downstream callers. This maps to CWE-190 (Integer Overflow or Wraparound). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (7.6, High). Remote delivery is also possible in OTA/update pipelines. The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Total.	7.6	More Details
CVE-2026-57985	Improper input validation in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	7.6	More Details
CVE-2026-54409	A malicious actor with access to the network and under certain conditions could exploit an Improper Initialization vulnerability found in UniFi Protect Application to bypass authentication in UniFi Protect Cameras.	7.5	More Details
CVE-2026-55111	A malicious actor with access to the network could exploit a Path Traversal vulnerability found in UniFi Protect Floodlight devices to access files on the UniFi Protect Floodlight.	7.5	More Details
CVE-2026-20458	In Modem, there is a possible memory corruption due to a missing bounds check. This could lead to remote escalation of privilege, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01402160; Issue ID: MSV-7298.	7.5	More Details
CVE-2026-13251	The Perfmatters plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.6.4 via the 's' parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. Exploitation requires the Local Google Fonts feature to be enabled (disabled by default), pretty permalinks to be active, and RSS feed links to remain enabled in the plugin settings.	7.5	More Details

CVE-2026-13369	The Ninja Forms - File Uploads plugin for WordPress is vulnerable to Arbitrary File Read via the attach_files() function in versions up to, and including, 3.3.29. This is due to the get_files_for_attachment() function accepting a raw attacker-controlled 'files' array when the process() method returns early due to a client-supplied saveProgress flag, bypassing all upload validation, path normalization, and database record creation steps, and allowing an attacker-supplied file_path value to reach wp_mail() as an email attachment with only a file_exists() check. This makes it possible for unauthenticated attackers to read arbitrary files on the affected site's server.	7.5	More Details
CVE-2026-55113	A malicious actor with access to the network could exploit a Server-Side Request Forgery (SSRF) vulnerability found in UniFi Talk Application to execute a Denial of Service (DoS) attack and bypass authentication in certain UniFi Talk API endpoints.	7.5	More Details
CVE-2026-55112	A malicious actor with access to the network and low privileges and under certain conditions could exploit an Improper Access Control vulnerability found in UniFi OS with UniFi Protect Application to escalate privileges on the host device.	7.5	More Details
CVE-2026-55110	A malicious actor who lures an authenticated user to a malicious page could exploit a Cross-Origin Resource Sharing (CORS) misconfiguration found in UniFi OS to trigger actions in UniFi OS using that user's session.	7.5	More Details
CVE-2026-58652	luci-app-travelmate (and the travelmate package) contain a privilege-escalation flaw: a LuCI/rpcd session holding the luci-app-travelmate write ACL is granted config-wide UCI write access to the travelmate configuration. While the LuCI UI restricts the auto-login script picker to /etc/travelmate/*.login, this is only a frontend restriction. The backend travelmate service (running as root) reads the raw UCI 'script' and 'script_args' values and executes the configured path when the captive-portal auto-login branch (f_check() in travelmate-functions.sh) is reached. An attacker with delegated write permissions can set script to /bin/sh and script_args to attacker-controlled arguments, resulting in arbitrary command execution as root. Confirmed in luci-app-travelmate/travelmate 2.4.5-r3; the sink is still present in travelmate 2.4.6-1 and no patched version is known.	7.5	More Details
CVE-2026-54405	A malicious actor with access to the network could exploit an Improper Input Validation vulnerability found in UniFi Network Application to execute a Denial of Service (DoS) attack on the application.	7.5	More Details
CVE-2026-6101	The AMP for WP – Accelerated Mobile Pages plugin for WordPress is vulnerable to Arbitrary File Write in versions up to and including 1.1.12. This is due to unsafe ZIP file extraction in the ampforwp_save_local_font() function combined with inadequate cleanup that fails to remove nested directories and files. This makes it possible for authenticated attackers, with Author-level access and above, and permissions granted by an Administrator, to write arbitrary files to the server in a web-accessible location, potentially leading to remote code execution on hosts that execute PHP files in the uploads directory.	7.5	More Details
CVE-2026-14570	Crypt::DSA versions before 1.22 for Perl draw the DSA signing nonce and private key from a biased random generator, leading to private-key recovery. "Crypt::DSA::Util::makerandom forces the high bit of every value it returns to obtain an exactly N-bit integer for prime search. The signing nonce and the private key are drawn from makerandom. Because the high bit is always set, the result is not uniform: its top bit is fixed, producing insecure values." An attacker who collects a modest number of signatures under an affected key, together with the public key, can recover the private key with a lattice attack. Keys used to sign with an affected version should be considered compromised and new keys should be generated.	7.5	More Details
CVE-2026-39448	Unauthenticated Broken Access Control in NOWPayments for WooCommerce <= 1.4.0 versions.	7.5	More Details
CVE-2026-57748	Contributor Local File Inclusion in Shopify <= 1.0.0 versions.	7.5	More Details
CVE-2026-57749	Contributor Local File Inclusion in SportsPress Pro <= 2.7.29 versions.	7.5	More Details
CVE-2026-59708	The GET /api/v1/public/:accessId/portfolio endpoint in ghostfolio accepts private access IDs without validating granteeUserId filtering, allowing unauthenticated access to full portfolio data. Attackers with a private access ID can retrieve sensitive portfolio information including holdings, quantities, buy prices, and performance metrics without authentication.	7.5	More Details
CVE-2026-11946	An unauthenticated remote attacker can exhaust server memory via the GetEndpoints Discovery Service in open62541. The endpointUrl field of GetEndpointsRequest is not validated for length. An attacker can declare an arbitrarily large string (up to ~4.09 GB via the UInt32 length field) delivered across intermediate chunks without ever sending the final chunk. The server buffers all chunks in RAM indefinitely until the SecureChannel times out. The attack is pre-session and bypasses all encryption configurations. The issue affects open62541: from 1.4.0 through 1.4.16, from 1.5.0 through 1.5.4, master.	7.5	More Details

CVE-2025-69134	Unauthenticated Arbitrary Content Deletion in OpenAI Chatbot for WordPress – Helper <= 1.1.4 versions.	7.5	More Details
CVE-2026-14426	Use after free in V8 in Google Chrome prior to 150.0.7871.46 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2025-69133	Subscriber Local File Inclusion in Tourmaster <= 5.4.5 versions.	7.5	More Details
CVE-2026-58469	GNU Wget through 1.25.0, fixed in commit 37a40fc, contains a heap buffer underread vulnerability in the clean_metalink_string() function within src/metalink.c that allows a malicious server to trigger memory corruption by serving a Metalink document containing a whitespace-only URL. Attackers can cause the function to decrement a pointer past the start of the buffer when processing an all-whitespace Metalink URL, potentially leading to abnormal program behavior.	7.5	More Details
CVE-2026-12923	The Youtube Showcase plugin for WordPress is vulnerable to Arbitrary Function Call in versions up to and including 4.0.3. This is due to insufficient validation of the 'path' parameter in the emd_delete_file() AJAX handler in includes/common-functions.php. The user-supplied value is passed through sanitize_text_field(), has its trailing '_PLUGIN_DIR' substring stripped, and is then invoked as a PHP function name with no arguments via `$sess_name()`. The handler is gated only by a nonce — no current_user_can() check is present — and the nonce is emitted on any front-end page that renders a form shortcode containing file fields. This makes it possible for authenticated attackers, with Subscriber-level access and above, to invoke arbitrary zero-argument PHP functions (such as phpinfo, phpversion, get_defined_vars, error_get_last), resulting in sensitive information disclosure and potential further compromise depending on the functions available in the environment.	7.5	More Details
CVE-2026-14249	The Request a Quote plugin for WordPress is vulnerable to Code Injection in versions up to, and including, 2.5.5 via the emd_delete_file AJAX action. This is due to the emd_delete_file() handler deriving a PHP function name from the attacker-controlled $_POST['path'] parameter and invoking it dynamically via the variable-function call $sess_name(), and the handler being registered for wp_ajax_nopriv with its only protection being a nonce that the plugin prints into the public quote-form page via wp_localize_script. This makes it possible for unauthenticated attackers to invoke arbitrary zero-argument PHP functions on the server, such as phpinfo(), potentially exposing sensitive server configuration and credentials, or executing other destructive built-in PHP functions.	7.5	More Details
CVE-2026-14409	Inappropriate implementation in V8 in Google Chrome prior to 150.0.7871.46 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	7.5	More Details
CVE-2026-58421	Unauthenticated ReDoS via CODEOWNERS pattern matching allows denial of service	7.5	More Details
CVE-2026-58419	Notification API leaks private issue metadata after access revocation	7.5	More Details
CVE-2026-33592	An unauthenticated remote attacker can exhaust server memory via the FindServers Discovery Service in open62541. The serverUris field of FindServersRequest is not validated for length or array size. An attacker can declare an arbitrarily large string (up to ~3.9 GB) delivered across intermediate chunks without ever sending the final chunk. The server buffers all chunks in RAM indefinitely until the SecureChannel times out. The attack is pre-session and bypasses all encryption configuration. The issue affects open62541: from 1.4.0 through 1.4.16, from 1.5.0 through 1.5.4, master.	7.5	More Details
CVE-2026-9563	In Eclipse Parsson published Maven Central artifacts before version 1.1.8, the JSON parser did not enforce a default maximum on the number of characters consumed while parsing a single JSON document. Applications that parse attacker- controlled JSON can be forced to consume excessive CPU and memory by processing very large documents, including large arrays, objects, strings, numbers, whitespace, or nested structures, resulting in a denial of service. Eclipse Parsson 1.1.8 introduces a configurable maximum parsing limit with a default limit of 15 million parser-consumed characters.	7.5	More Details
CVE-2026-13468	The Visualizer – Tables & Charts Manager with Built-in AI Generator plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.0.3. 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 access and export the contents of any visualizer chart on the site — including charts in draft, private, pending, future, or trash status — as CSV, Excel, or HTML via the /wp-json/visualizer/v1/action/{chart}/{type}/ REST endpoint. This bypass is particularly impactful because the standard WordPress REST endpoint for the non-public 'visualizer' custom post type correctly enforces capability checks and returns HTTP 401 to unauthenticated callers, whereas this plugin-registered route circumvents that protection entirely.	7.5	More Details

CVE-2026-56842	A malicious actor with access to the network and under certain conditions could exploit an Incorrect Authorization vulnerability found in UniFi Network Application to persist privileges within UniFi Network Application after such access had been removed.	7.5	More Details
CVE-2026-14181	@fastify/middie versions 9.1.0 through 9.3.2 fail to guard the URL normalization step used by the standalone engine when incoming request paths contain malformed percent-encoded sequences. Inputs such as an incomplete percent escape or a truncated multibyte sequence cause the underlying decoder to throw synchronously, and the exception escapes the middie normalize step and terminates the Node.js process. The bypass affects applications that call middie.run directly on the standalone engine API, causing an immediate denial of service for all connected clients until restart. Applications using the Fastify plugin path are not affected because Fastifys error handler catches the exception. Patches: upgrade to @fastify/middie 9.3.3. Workarounds: migrate from the standalone engine API to the Fastify plugin path, where the framework error handler catches the exception.	7.5	More Details
CVE-2026-57984	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-13708	Imager::File::JPEG versions before 1.003 for Perl leak heap memory when reading a JPEG with repeated APP13 markers in i_readjpeg_wiol. i_readjpeg_wiol walks the marker list libjpeg returns and, for each APP13 marker, allocates a new buffer with *iptc_itext = mymalloc(...) and overwrites the previous pointer without freeing it. Only the final payload is later turned into a Perl scalar and freed, so a JPEG with N such markers leaks the first N-1 payloads on every read. In a long-lived process, such as an upload or thumbnailing service, repeated reads accumulate these leaks and exhaust available memory, a denial of service. The same handler ships bundled in the Imager distribution, where versions before 1.032 are affected and the fix ships in 1.032.	7.5	More Details
CVE-2026-13753	A missing authorization vulnerability exists in the embedded webserver of HP Deskjet 2800 Series Printers running firmware version <=TBP1CN2612AR. An unauthenticated attacker with network access can send GET requests to multiple exposed administrative API endpoints and retrieve sensitive configuration data such as plaintext Wi-Fi Direct credentials, unique device identity information, and other administrative security state details. When accessed through the web interface, these setting pages explicitly require administrator credentials before sensitive information is displayed.	7.5	More Details
CVE-2026-25038	Gitea 1.26.2 allows unauthorized users to access labels of private organizations.	7.5	More Details
CVE-2026-25712	Gitea versions before 1.25.5 have insufficient visibility checks in organization permission APIs for hidden members and private organizations.	7.5	More Details
CVE-2026-40140	BeyondTrust Remote Support and Privileged Remote Access contain a high-severity pre-authentication vulnerability in the network communication subsystem. Insufficient validation of client-supplied input may allow an unauthenticated remote attacker to trigger a denial-of-service condition affecting appliance availability.	7.5	More Details
CVE-2026-27657	Gitea versions before 1.25.5 allow a user to change another user's primary email address.	7.5	More Details
CVE-2026-14327	The AR for WordPress plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 8.40 via the 'file' parameter parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. Exploitation requires an attacker to first obtain a valid nonce and secure nonce via the publicly accessible ar_get_fresh_nonce and ar_process_user_image nopriv AJAX handlers, and to reproduce the encryption key locally — both steps are fully achievable by an unauthenticated attacker on any default free or unlicensed installation where ar_licence_key is unset.	7.5	More Details
CVE-2026-27660	Gitea versions before 1.25.5 allow draft release data or attachments to be accessed without the required write permission.	7.5	More Details
CVE-2026-1239	The Ninja Forms – The Contact Form Builder That Grows With You plugin for WordPress is vulnerable to unauthorized access of data due to a missing authorization check on the 'ninja-forms-views/token/refresh' REST callback in all versions up to, and including, 3.14.1. This makes it possible for unauthenticated attackers to view form submissions, which could potentially contain sensitive information.	7.5	More Details
CVE-2026-27779	Gitea versions before 1.25.5 accept malformed or injected forwarded-proto values when detecting public URLs, allowing spoofed canonical URL generation.	7.5	More Details
CVE-			

2026-14193	DVP80ES300T with Improper Validation of Array Index Vulnerability	7.5	More Details
CVE-2026-20213	A vulnerability in the PE file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in PE files during scanning, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted file that contains PE content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	7.5	More Details
CVE-2026-24264	NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker can cause improper handling of highly compressed data. A successful exploit of this vulnerability might lead to denial of service.	7.5	More Details
CVE-2026-57975	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-55994	Improper Input Validation, Exposure of Sensitive Information to an Unauthorized Actor, Server-Side Request Forgery (SSRF) vulnerability in Apache Camel in Iggy component. The camel-iggy consumer mapped the user-headers of inbound Iggy messages into the Camel Exchange header map without applying any HeaderFilterStrategy (IggyFetchRecords copied the message user-headers straight into the Exchange). Because nothing blocked the Camel header namespace, an actor able to publish to the consumed Iggy stream/topic could set Camel-internal control headers - including CamelHttpUri (Exchange.HTTP_URI) - simply by supplying them as message user-headers. In a route where the Iggy consumer feeds a downstream HTTP producer, the injected CamelHttpUri redirects the server-side HTTP request to an attacker-chosen destination (server-side request forgery - for example to an internal service or a cloud metadata endpoint). In addition, the HTTP producer resolves Camel property placeholders on the resulting (attacker-controlled) URI, so placeholders embedded in the injected value - such as an environment-variable reference, an application property, or a vault reference - are resolved to their real values and sent to the attacker, disclosing environment variables, application properties and vault secrets. This issue affects Apache Camel: from 4.17.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix adds a dedicated IggyHeaderFilterStrategy (and a headerFilterStrategy endpoint option) that filters the Camel header namespace case-insensitively on inbound mapping, so externally-supplied Camel* / camel* headers are no longer copied into the Exchange. For deployments that cannot upgrade immediately, strip the Camel control headers from the inbound message before they reach any downstream producer (for example removeHeaders('Camel*') and removeHeaders('camel*') at the start of the route), restrict who can publish to the consumed Iggy stream/topic, and avoid bridging an untrusted consumer directly into an HTTP producer whose target URI can be driven from message headers.	7.5	More Details
CVE-2026-55993	Improper Input Validation, Exposure of Sensitive Information to an Unauthorized Actor, Server-Side Request Forgery (SSRF) vulnerability in Apache Camel in Atmosphere Websocket Component. The camel-atmosphere-websocket consumer mapped inbound WebSocket query parameters into the Camel Exchange header map without applying any HeaderFilterStrategy (WebsocketConsumer.sendEventNotification() iterates the query-string map collected in WebsocketConsumer.service() and copies each entry into the Exchange). Because nothing blocked the Camel header namespace, a client connecting to the WebSocket endpoint could set Camel-internal control headers - including CamelHttpUri (Exchange.HTTP_URI) - simply by supplying them as query parameters. In a route where the WebSocket consumer feeds a downstream HTTP producer, the injected CamelHttpUri redirects the server-side HTTP request to an attacker-chosen destination (server-side request forgery - for example to an internal service or a cloud metadata endpoint). In addition, the HTTP producer resolves Camel property placeholders on the resulting (attacker-controlled) URI, so placeholders embedded in the injected value - such as an environment-variable reference, an application property, or a vault reference - are resolved to their real values and sent to the attacker, disclosing environment variables, application properties and vault secrets. When the WebSocket endpoint is exposed without authentication, this is reachable by an unauthenticated remote attacker. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix makes the consumer apply the HeaderFilterStrategy it already inherits from the HTTP/servlet stack, filtering the Camel header namespace case-insensitively on inbound mapping, so externally-supplied Camel* / camel* headers are no longer copied into the Exchange. For deployments that cannot upgrade immediately, strip the Camel control headers from the inbound message before they reach any downstream producer (for example removeHeaders('Camel*') and removeHeaders('camel*') at the start of the route), require authentication on the WebSocket endpoint, and avoid bridging an untrusted consumer directly into an HTTP producer whose target URI can be driven from message headers.	7.5	More Details
	Improper Input Validation, Exposure of Sensitive Information to an Unauthorized Actor, Server-Side Request Forgery (SSRF) vulnerability in Apache Camel in Vertx Websocket component. The camel-vertx-websocket consumer mapped inbound WebSocket query and path parameters into the Camel Exchange header map		

CVE-2026-46726	without applying any HeaderFilterStrategy (VertxWebsocketConsumer.populateExchangeHeaders()). Because nothing blocked the Camel header namespace, a client connecting to the WebSocket endpoint could set Camel-internal control headers - including CamelHttpUri (Exchange.HTTP_URI) - simply by supplying them as query parameters. In a route where the WebSocket consumer feeds a downstream HTTP producer, the injected CamelHttpUri redirects the server-side HTTP request to an attacker-chosen destination (server-side request forgery - for example to an internal service or a cloud metadata endpoint). In addition, the HTTP producer resolves Camel property placeholders on the resulting (attacker-controlled) URI, so placeholders embedded in the injected value - such as an environment-variable reference, an application property, or a vault reference - are resolved to their real values and sent to the attacker, disclosing environment variables, application properties and vault secrets. When the WebSocket endpoint is exposed without authentication, this is reachable by an unauthenticated remote attacker. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix makes the affected consumers apply a HeaderFilterStrategy that filters the Camel header namespace case-insensitively on inbound mapping, so externally-supplied Camel* / camel* headers are no longer copied into the Exchange. For deployments that cannot upgrade immediately, strip the Camel control headers from the inbound message before they reach any downstream producer (for example removeHeaders('Camel*') and removeHeaders('camel*') at the start of the route), require authentication on the WebSocket endpoint, and avoid bridging an untrusted consumer directly into an HTTP producer whose target URI can be driven from message headers.	7.5	More Details
CVE-2026-46592	Improper Input Validation, Unintended Proxy or Intermediary ('Confused Deputy') vulnerability in Apache Camel CXF SOAP component. The camel-cxf producer selects which SOAP operation to invoke on the backend service from the operationName (and operationNamespace) Exchange header, whose constant values (CxfConstants.OPERATION_NAME / OPERATION_NAMESPACE) were the plain strings operationName / operationNamespace. Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that bridges an HTTP consumer (for example platform-http) into a cxf: producer, any HTTP client could therefore set the operationName header and have CxfProducer resolve and invoke a different WSDL operation than the route intended - for example replacing a read operation with a destructive one - against the backend SOAP service (a confused-deputy redirection). The constant is defined in the shared camel-cxf-common module, so the same non-prefixed names also applied to camel-cxfrs. No credentials are required when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, the operation-selection headers are named CamelCxfOperationName / CamelCxfOperationNamespace and are filtered at transport boundaries; see the 4.21 upgrade guide for the cross-transport carrier-header pattern. For deployments that cannot upgrade immediately, do not select the CXF operation from untrusted input: strip the operationName and operationNamespace headers from any untrusted ingress before the cxf: producer and set the operation from a trusted source in the route.	7.5	More Details
CVE-2026-52190	Buffer Overflow vulnerability in UTT nv518G nv518GV3v3.2.7-210919-161313 allows a remote attacker to cause a denial of service via the gohead/sub_448384 component	7.5	More Details
CVE-2026-46585	Improper Input Validation, Authorization Bypass Through User-Controlled Key vulnerability in Apache Camel Lucene Component. The camel-lucene producer reads the search phrase from an Exchange header (LuceneConstants.HEADER_QUERY) whose value was the plain string QUERY (and RETURN_LUCENE_DOCS for HEADER_RETURN_LUCENE_DOCS). Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that exposes a Lucene query operation behind an HTTP consumer (for example platform-http), any HTTP client could therefore set the QUERY header and have its value executed against the full-text index, overriding the query the route intended to run. Depending on what is indexed, this allows reading documents the request should not have access to (for example a match-all query returns the entire index, or the route's intended per-user filter can be replaced), and expensive regular-expression queries can consume significant CPU. No credentials are required when the HTTP consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that set the query via the raw header name must use CamelLuceneQuery (and CamelLuceneReturnLuceneDocs) instead of QUERY / RETURN_LUCENE_DOCS. For deployments that cannot upgrade immediately, strip the attacker-controllable headers before the Lucene producer and set the query from a trusted source (for example removeHeader('QUERY') and removeHeader('RETURN_LUCENE_DOCS'), then setHeader('QUERY', constant(...)) at the start of the route).	7.5	More Details
	Improper Input Validation vulnerability in Apache Camel NATS component. The camel-nats component maps		

CVE-2026-46457	inbound NATS message headers into the Camel Exchange but defaulted its headerFilterStrategy to a bare new DefaultHeaderFilterStrategy() with no inbound rules configured (NatsConfiguration). With no inFilter, inFilterPattern or inFilterStartsWith set, DefaultHeaderFilterStrategy.applyFilterToExternalHeaders returns not filtered for every header name, so NatsConsumer copies every NATS message header - including Camel-internal control headers such as CamelHttpUri, CamelFileName or CamelSqlQuery - unmodified onto the Camel message. A client able to publish to the consumed NATS subject can therefore inject arbitrary Camel control headers that influence the behaviour of downstream producers in the route (for example redirecting an HTTP producer, changing a file name, or overriding a query); the injected headers also persist across internal direct, seda and vm hops. The concrete downstream impact depends on which producers the route uses. NATS message headers require NATS 2.2 or later, and the issue is reachable without credentials when the NATS server is configured without authentication (the NATS server default). This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix makes camel-nats default to a dedicated NatsHeaderFilterStrategy that filters the Camel header namespace case-insensitively on inbound mapping, so client-supplied Camel* / camel* headers are no longer copied into the Exchange. For deployments that cannot upgrade immediately, strip the Camel control headers from inbound NATS messages before they reach any downstream producer (for example removeHeaders('Camel*') and removeHeaders('camel*') at the start of the route), and enable authentication on the NATS server so that only trusted clients can publish to the consumed subject.	7.5	More Details
CVE-2026-24690	Gitea versions before 1.25.5 have insufficient permission checks for updating or rebasing pull request branches.	7.5	More Details
CVE-2026-54059	Pillow is a Python imaging library. Prior to 12.3.0, PIL/PcfFontFile.py _load_bitmaps() read glyph dimensions from the PCF METRICS section and passed them directly to Image.frombytes() without calling Image._decompression_bomb_check(), allowing crafted PCF font data to cause excessive memory allocation. This issue is fixed in version 12.3.0.	7.5	More Details
CVE-2026-54060	Pillow is a Python imaging library. Prior to 12.3.0, PIL/FontFile.py FontFile.compile() assembled per-glyph images into a combined bitmap with Image.new("1", (xsize, ysize)) without calling Image._decompression_bomb_check(), allowing a font to trigger excessive allocation during conversion or saving. This issue is fixed in version 12.3.0.	7.5	More Details
CVE-2026-55379	Pillow is a Python imaging library. Prior to 12.3.0, PIL/BdfFontFile.py bdf_char() read the BBX width and height field from a BDF font file and passed attacker-controlled dimensions to Image.new() without calling Image._decompression_bomb_check(), bypassing Pillow's documented decompression bomb protection and allowing excessive memory allocation. This issue is fixed in version 12.3.0.	7.5	More Details
CVE-2026-54592	Oj (Optimized JSON) is a JSON parser and Object marshaller packaged as a Ruby gem. In versions prior to 3.17.3, Oj::Doc#each_child, when invoked recursively over a deeply nested JSON document, overflows a fixed-size stack buffer and aborts the process, leading to DoS. In a two-step chain in ext/oj/fast.c, doc_each_child increments doc->where past the where_path[MAX_STACK = 100] array with no bounds check and never restores it (the doc->where-- is missing), so calling each_child recursively from inside the yield block drives doc->where beyond the array. On the next entry the function copies the path into the 800-byte stack-local buffer save_path[MAX_STACK] using wlen = doc->where - doc->where_path, so when the previous recursive call left doc->where past where_path[100] the wlen exceeds MAX_STACK and the memcpy overflows save_path on the C stack; because the Oj::Doc parser imposes no JSON nesting-depth limit (relying on a C-stack pressure check), deeply nested attacker input reaches this path. This issue has been fixed in version 3.17.3.	7.5	More Details
CVE-2026-9546	A vulnerability in libcurl caused the HTTP `Referer:` header to persist even when explicitly cleared. While the documentation states that passing NULL to `CURLOPT_REFERER` suppresses the header, the option failed to clear the internal state. As a result the previous referrer string was erroneously reused and sent in subsequent requests, potentially leaking sensitive information to unintended servers.	7.5	More Details
CVE-2026-9545	In this scenario, libcurl first uses a proper HTTP/3 server for the initial transfers, and when it makes a second transfer to the same site it has been replaced by the attacker's impostor machine - without a valid certificate. When libcurl returns to the hostname the second time with a cached SSL session (`CURLOPT_SSL_SESSIONID_CACHE` is not disabled) and early data enabled (the `CURLSSLOPT_EARLYDATA` bit is set in `CURLOPT_SSL_OPTIONS`), libcurl might send off the second request's bytes on that new connection *before* enforcing the certificate verification failure. Potentially leaking sensitive information.	7.5	More Details
CVE-2026-5730	Authorization bypass through User-Controlled key vulnerability in Idvlabs Software and Consulting Services Inc. Ontime allows Exploitation of Trusted Identifiers. This issue affects Ontime: through 04052026.	7.5	More Details
CVE-2026-5799	Authorization bypass through User-Controlled key vulnerability in Idvlabs Software and Consulting Services Inc. Ontime allows Exploitation of Trusted Identifiers. This issue affects Ontime: through 04052026.	7.5	More Details

CVE-2026-8932	libcurl would reuse a previously created connection even when some mTLS config related option had been changed that should have prohibited reuse. libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse if one of them matches the setup. However, some TLS settings related to client certificates were left out from the configuration match checks, making them match too easily. In particular options related to the private key.	7.5	More Details
CVE-2026-38976	mrubyc through 3.4.1 was found to contain a NULL pointer dereference in src/vm.c in op_super() / OP_SUPER due to a missing runtime guard for top-level super.	7.5	More Details
CVE-2026-12576	DVP80ES3 with Improper Enforcement of Message Integrity During Transmission in a Communication Channel vulnerability.	7.5	More Details
CVE-2026-12575	DVP80ES3 with Improper Resource Shutdown or Release vulnerability.	7.5	More Details
CVE-2026-4967	In IMS, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed.	7.5	More Details
CVE-2026-12064	When a user invokes curl using a schemeless URL combined with `--proto-default` sftp (or scp), a disconnect occurs between the tool layer and libcurl. The tool layer incorrectly infers the URL scheme, which erroneously bypasses the initialization of critical SSH security options like CURLOPT_SSH_HOST_PUBLIC_KEY_SHA256 and CURLOPT_SSH_KNOWNHOSTS. Conversely, the libcurl runtime successfully honors CURLOPT_DEFAULT_PROTOCOL and establishes the connection via SFTP/SCP as specified. Because the tool layer skipped the security configuration, these SSH host verification options are silently omitted, causing curl to connect to an unverified SSH remote host without throwing an error.	7.5	More Details
CVE-2026-55727	A flaw in the authentication mechanism for video stream requests in Genetec Security Center 5.14.0.0 prior to build 5.14.178.18 may allow an unauthenticated attacker to access live video streams.	7.5	More Details
CVE-2026-55574	vLLM is a high-throughput and memory-efficient inference and serving engine for LLMs. Prior to 0.24.0, the structured_outputs.regex API parameter passes a user-supplied regular expression string directly to the grammar compiler backends with no compilation timeout; in the xgrammar backend the string reaches the regex compiler with no guard, and in the outlines backend the validation step blocks structural issues such as lookarounds and backreferences but performs no complexity analysis, so a pattern with nested quantifiers passes all checks and causes exponential state-space expansion, allowing a single request containing an adversarial regex to hang an inference worker indefinitely and deny service. This issue is fixed in version 0.24.0.	7.5	More Details
CVE-2026-11586	By default, curl automatically responds to WebSocket PING frames. Because curl lacks an upper bound on memory allocation for unacknowledged frames, a malicious server can exhaust all available memory by flooding curl with rapid, sequential PING messages.	7.5	More Details
CVE-2026-54234	vLLM is a high-throughput and memory-efficient inference and serving engine for LLMs. Prior to 0.24.0, a frontend-legal multi-request speculative decoding workload can cause the rejection sampler to produce a recovered token equal to the model vocabulary size boundary value, which is then converted to negative one when the engine selects the next live token for a request and is written back into the drafter's input ids; that out-of-vocabulary value is later consumed by the model's embedding and attention path and crashes the engine worker with a GPU device-side assertion. The same triggering request sequence is reachable through the public gRPC Generate and Abort endpoints, so a remote client that can send generation requests can crash the shared engine worker, aborting concurrent requests and causing a service-wide denial of service for other clients of the deployment until the worker is restarted. This issue is fixed in version 0.24.0.	7.5	More Details
CVE-2026-11352	An issue in curl’s QUIC UDP receive function allows a malicious HTTP/3 server to trigger a remote denial of service against a curl or libcurl client. Because the helper function discards zero-length UDP datagrams before counting them toward the per-call packet budget, a connected QUIC peer can continuously stream empty datagrams to indefinitely stall the client.	7.5	More Details
CVE-2026-14352	The AR for WooCommerce plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 8.40 via the 'file' parameter parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. The three intended access controls all fail: valid nonces are freely minted by unauthenticated callers via the nopriv ar_get_fresh_nonce and ar_process_user_image AJAX handlers; the AES-256-CBC encryption key is derived from get_option('ar_licence_key'), which returns false on default free installations and yields a predictable key attackers can use to encrypt their own path payloads; and the Referer check is trivially bypassed because the Referer header is attacker-controlled.	7.5	More Details
CVE-			

2026-24451	Gitea 1.26.2 allows fork synchronization to continue after a parent repository changes from public to private, exposing data to a fork that should no longer be authorized.	7.5	More Details
CVE-2026-55380	Pillow is a Python imaging library. Prior to 12.3.0, PIL/GdImageFile.py GdImageFile._open() read image dimensions from the GD 2.x header and stored them in self._size without calling Image._decompression_bomb_check(), allowing a crafted .gd file to trigger excessive C-heap allocation when loaded. This issue is fixed in version 12.3.0.	7.5	More Details
CVE-2026-20191	A vulnerability in Cisco Catalyst Center could allow an unauthenticated, remote attacker to read arbitrary files from a restricted container. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to read arbitrary files from a restricted container of the affected device.	7.5	More Details
CVE-2026-38969	ruby webrick through v1.9.2 WEBrick reparses trailer Content-Length into canonical request state, enabling request smuggling.	7.5	More Details
CVE-2026-20214	A vulnerability in the FSG file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in FSG files during scanning, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted file that contains portable executable content compressed with FSG to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	7.5	More Details
CVE-2026-52192	An issue in UTT nv518G nv518GV3v3.2.7-210919-161313 allows a remote attacker to cause a denial of service via the gohead/sub_445C5C component	7.5	More Details
CVE-2024-6228	The Notifications for Forms & WordPress Actions WordPress plugin before 2.6 does not validate a user-supplied value before using it to build a server-side file inclusion path, allowing authenticated users with subscriber-level access and above to include and execute arbitrary local PHP files on the server.	7.5	More Details
CVE-2026-52189	Buffer Overflow vulnerability in UTT nv518G nv518GV3v3.2.7-210919-161313 allows a remote attacker to cause a denial of service via the gohead/sub_487330 component	7.5	More Details
CVE-2026-38970	pdfcpu through v0.11.1 contains an uncontrolled-recursion denial-of-service issue in pkg/pdfcpu/model/parse.go. The parser descends recursively through nested PDF objects, including arrays, via ParseObjectContext() and parseArray() without enforcing a maximum nesting depth.	7.5	More Details
CVE-2026-8441	The WP Review Slider Pro plugin for WordPress is vulnerable to SQL Injection via the 'notinstring' parameter of the wprp_load_more_revs AJAX action in versions up to, and including, 12.7.2. The parameter is read via $_POST['notinstring'] and passed through sanitize_text_field() — which strips HTML and whitespace but does not provide SQL safety. The value is then concatenated directly into a numeric/unquoted `AND id NOT IN (...)` clause and executed via $wpdb->get_results() without $wpdb->prepare() or intval() casting. Because the value sits in an unquoted numeric context, WordPress's wp_magic_quotes protection (which only escapes embedded quotes) is ineffective. The AJAX hook is registered via wp_ajax_nopriv_wprp_load_more_revs, and the required check_ajax_referer nonce is publicly available via wp_localize_script on any frontend page that renders the plugin shortcode, so an unauthenticated attacker who can reach a public page hosting the plugin can extract arbitrary data from the database via blind/time-based injection.	7.5	More Details
CVE-2026-49119	Gradio before 6.16.0 contain a path traversal vulnerability in the FileExplorer component's preprocess() method that allows unauthenticated attackers to escape the configured root directory by supplying path segments containing directory traversal sequences or absolute paths. Attackers can provide crafted path segments that cause os.path.join to discard the root_dir prefix entirely, resulting in arbitrary file read or exposure of sensitive files outside the intended directory.	7.5	More Details
CVE-2026-59096	Dapr Sentry's OIDC discovery endpoint derives the issuer and jwks_uri of the /.well-known/openid-configuration document from the request Host, honoring an attacker-controlled X-Forwarded-Host header without validation when no allowed-hosts list is configured (the default), and serves the document with a one-hour public cache lifetime. A remote unauthenticated attacker can poison the discovery document so relying parties performing dynamic (unpinned) discovery fetch the JWKS from an attacker-controlled server, causing attacker-signed JWTs to be accepted. Exploitation requires the OIDC server enabled without a configured jwt-issuer or oidc-allowed-hosts.	7.5	More Details
CVE-2026-59094	Pathway through 0.31.1, fixed in commit d09722e, document store applies a caller-supplied glob pattern to indexed document paths using a hand-written recursive matcher that branches two ways on each ** token without memoization, giving exponential worst-case complexity. The filepath_globpattern value is taken from the body of the unauthenticated HTTP endpoints /v1/retrieve, /v1/inputs and /v2/answer and compiled into a filter evaluated once per indexed document, with no length or **-count limit. A remote unauthenticated attacker can submit a short pattern containing many ** tokens to consume CPU for tens of seconds per	7.5	More Details

	request, and a small number of requests denies service.		
CVE-2026-58467	Cockpit CMS before release 364 contains a path traversal and local file inclusion vulnerability that allows unauthenticated attackers to read arbitrary files or execute PHP files by including unvalidated PATH_INFO derived from REQUEST_URI in filesystem path construction without containment checks. Attackers can inject dot-dot sequences into the URL to traverse outside the designated spaces directory, and when the resolved path ends with a .php extension, the application passes it to include(), enabling local file inclusion on deployments using the PHP built-in server or certain non-default Nginx configurations.	7.5	More Details
CVE-2026-14265	Deserialization of untrusted data in the RemoteQueryCachePlugin in Amazon Web Services AWS Advanced JDBC Wrapper 3.3.0 through 4.0.0 might allow an actor with write access to the shared cache infrastructure to execute arbitrary code on application servers that read cached query results via a crafted serialized Java object. The RemoteQueryCachePlugin uses ObjectInputStream without class filtering when deserializing cached query results from Redis or Valkey, enabling gadget chain execution when cache entries are poisoned. We recommend upgrading to AWS Advanced JDBC Wrapper version 4.0.1 or later.	7.5	More Details
CVE-2026-52187	Buffer Overflow vulnerability in UTT nv518G nv518GV3v3.2.7-210919-161313 allows a remote attacker to cause a denial of service via the gohead/sub_483ba0 component	7.5	More Details
CVE-2026-11568	The Product Configurator for WooCommerce WordPress plugin before 1.7.3 does not perform any authorisation or post-status check before returning WooCommerce product data through a public AJAX action, allowing unauthenticated users to retrieve the data (title, price, weight, stock status, and configurator option pricing/SKUs) of private and draft, non-public products by supplying the product ID. WordPress post-visibility controls are bypassed.	7.5	More Details
CVE-2026-58593	NodeBB does not bind the claimed author of an inbound ActivityPub object to the authenticated remote actor. The inbound middleware verifies the HTTP-signature actor and checks the origin of object.id, but never validates that attributedTo corresponds to the sender. In the object mock, attributedTo is used directly as a uid, and actors.assert silently ignores numeric identifiers (filtering them out without re-deriving the uid), so a federated remote actor can set attributedTo to a bare numeric value such as 1 and have the resulting post or private message created with that local uid as author, including the administrator account. This lets a remote attacker forge posts and direct messages attributed to arbitrary local users. Requires the ActivityPub/federation feature to be enabled.	7.5	More Details
CVE-2026-58290	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-58465	Eclipse Wakaama before snapshot/2026-05-26 contains an unbounded memory allocation vulnerability in the CoAP Block1 handler within coap/block.c that allows unauthenticated remote attackers to exhaust server memory by sending a sequence of Block1 PUT requests with incrementing block numbers. Attackers can target the registration endpoint over UDP without authentication, causing the server to repeatedly reallocate a growing accumulation buffer by appending each block payload without enforcing any maximum total size limit, resulting in denial of service through memory exhaustion.	7.5	More Details
CVE-2026-58292	Improper input validation in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-55952	The Erlang/OTP ssl application does not validate that the PSK identity list and binder list carried in a TLS 1.3 ClientHello pre-shared key extension have equal length before passing them to the session ticket handler. In tls_handshake_1_3:handle_pre_shared_key/3, an OfferedPreSharedKeys record with a mismatched number of identities and binders is forwarded directly to tls_server_session_ticket:use/4, which crashes the session ticket handler process. An unauthenticated remote attacker can send a single crafted ClientHello to a TLS 1.3 server with session tickets enabled (stateful or stateless mode) and permanently disrupt session ticket handling on that listener. New TLS 1.3 handshakes complete but subsequently crash when the server attempts to issue a session ticket, effectively making TLS 1.3 unusable on the affected listener until the ssl application is restarted. TLS 1.2 connections are not affected. This issue affects OTP from 22.2 before 29.0.3, 28.5.0.3 and 27.3.4.14 corresponding to ssl from 9.5 before 11.7.3, 11.6.0.3 and 11.2.12.10.	7.5	More Details
CVE-2026-58294	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-58299	Time-of-check time-of-use (toctou) race condition in Microsoft Edge for Android allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2024-	Landray OA contains an unauthenticated HQL injection vulnerability that allows unauthenticated attackers to query arbitrary Hibernate entity classes by injecting malicious HQL syntax into the uid POST parameter of the wechatLoginHelper.do endpoint. Attackers can exploit the lack of input sanitization in the string-concatenated filter expression passed to the Hibernate findList() call to extract sensitive data such as	7.5	More

58352	administrator password hashes and, with sufficient database privileges, perform file-write operations enabling remote code execution. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-03-11 (UTC).		Details
CVE-2026-36912	A NULL pointer dereference in the AP4_AtomSampleTable::GetSample() function of Aleksoid1978 MPC-BE before commit 4341cb3 allows attackers to cause a Denial of Service (DoS) via a crafted MP4 file.	7.5	More Details
CVE-2026-38891	An improper input validation in the gazebo_ros_diff_drive.cpp component of gazebo_plugins v3.9.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted geometry_msgs::Twist message.	7.5	More Details
CVE-2026-20215	A vulnerability in the 7z file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in 7z files during scanning, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted file that contains 7z content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	7.5	More Details
CVE-2026-52191	Buffer Overflow vulnerability in UTT nv518G nv518GV3v3.2.7-210919-161313 allows a remote attacker to cause a denial of service via the gohead/sub_444C8C component	7.5	More Details
CVE-2026-58276	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-24012	Uncontrolled Resource Consumption vulnerability in Apache IoTDB. Some interface fails to impose reasonable limits on the time span and aggregation interval of the query. An attacker can construct a request with extreme parameters (e.g., a very large time range combined with a minimal interval). This forces the DataNode to build an enormous result set in memory, which exhausts the Java heap and causes the DataNode process to crash. This issue affects Apache IoTDB: from 1.3.3 before 2.0.8. Users are recommended to upgrade to version 2.0.8, which fixes the issue.	7.5	More Details
CVE-2026-57986	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-20244	A vulnerability in the DMG file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in DMG files during scanning, which may result in an integer overflow on 32-bit platforms only. An attacker could exploit this vulnerability by submitting a crafted file that contains DMG content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	7.5	More Details
CVE-2026-20243	A vulnerability in the ALZ file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in ALZ files during scanning, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted file that contains ALZ content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	7.5	More Details
CVE-2026-20217	A vulnerability in the PESpin file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in PESpin files during scanning, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted file that contains PESpin content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	7.5	More Details
CVE-2026-14809	Prog Management System developed by PROG MIS has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read database contents.	7.5	More Details
CVE-2026-57992	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-	Uncontrolled Resource Consumption vulnerability in the HTTP/1.1 message parser in Apache HttpComponents		

2026-54399	Core (5.4.2 and earlier, 5.5-beta1 and earlier) allows an remote attacker to cause a denial of service through memory exhaustion by sending messages with excessive number of headers / excessive header length	7.5	More Details
CVE-2026-20216	A vulnerability in the InstallShield file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to improper handling of temporary resources during file scanning. An attacker could exploit this vulnerability by submitting a crafted InstallShield file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to terminate the ClamAV scanning process and temporarily consume available system resources, resulting in a DoS condition on the affected software.	7.5	More Details
CVE-2026-11823	The BookingPress Appointment Booking Pro plugin for WordPress is vulnerable to SQL Injection via the 'store_service_date' parameter of the bpa_assign_staffmember_to_slots() function in versions up to and including 5.7.1. This is due to the explicit use of stripslashes_deep() on user-supplied POST data before it is interpolated verbatim into a SQL LIKE clause without use of $wpdb->prepare() or any parameterization. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-58454	JAIOTlink C492A-W6 Wi-Fi IP cameras running firmware 4.8.30.57701411 contain a remote code execution vulnerability that allows authenticated attackers to execute arbitrary shell scripts by writing to the writable persistent JFFS2 storage path and triggering execution through the authenticated HTTP endpoint. Attackers can stage a malicious script in the writable persistent storage and request the config endpoint to invoke it via popen(), achieving persistent remote code execution that survives device reboots.	7.5	More Details
CVE-2026-12413	An invalidly formatted IKEv2 fragment causes the Libreswan pluto daemon to crash and restart. Continued exploitation would cause a denial of service. The function reassemble_v2_incoming_fragments() would ignore unknown outer payloads but still store these in a fixed size array msg_digest.digest[PAYLIMIT]. An off-by-one error in the assertion PASSERT(logger, md->digest_roof < elemsof(md->digest)) causes the daemon to abort. No remote code execution is possible. Any configuration that allows IKEv2 connections that do not set fragmentation=no are vulnerable. IKEv1 is not affected.	7.5	More Details
CVE-2026-54428	Allocation of resources without limits or throttling in the HTTP/2 HPACK decoder in Apache HttpComponents Core (5.4.2 and earlier, 5.5-beta1 and earlier) allows an remote attacker to cause a denial of service through memory exhaustion by sending oversized compressed header blocks before the HTTP/2 SETTINGS acknowledgement causes the configured header list size limit to be applied.	7.5	More Details
CVE-2026-9547	When a libcurl-based application performs transfers via `SCP://` or `SFTP://` and utilizes the `CURLOPT_SSH_KEYFUNCTION` callback, it may silently accept an untrusted server. This vulnerability occurs when a server presents a host key type that does not match the specific key type already recorded for that host in the `known_hosts` file. Instead of rejecting the mismatch, the callback mechanism fails to properly enforce the restriction, allowing the connection to succeed without warning and risking a potential man-in-the-middle attack.	7.4	More Details
CVE-2026-13341	A vulnerability exists in the Kong Konnect Model Context Protocol (MCP) server prior to version 1.0.0, which could allow a remote attacker to perform an indirect prompt injection attack and execute unintended API requests.	7.4	More Details
CVE-2026-7830	UltraVNC through 1.8.2.2 uses inadequate cryptography in the MS-Logon II authentication scheme (rfbUltraVNC_MsLogonIIAuth). In rfb/dh.cpp the Diffie-Hellman key exchange is performed with parameters that fit in an unsigned 64-bit integer (DH_MAX_BITS controls the prime size). A 64-bit DH key can be broken by Pollard's rho algorithm in under one second on current hardware. Additionally, the private exponent is generated by the rng() function, which multiplies three libc rand() values seeded from time(NULL). With approximately 31 bits of internal state and a time-based seed, the private exponent is recoverable in under a minute by a passive observer. A network attacker who can observe the MS-Logon II handshake (via sniffing, recording, or man-in-the-middle) can derive the shared DH key and decrypt the encapsulated username and password, resulting in full credential disclosure. This affects legacy MS-Logon II connections; MS-Logon III (X25519 + AES-256-GCM) is unaffected.	7.4	More Details
CVE-2026-12579	AS228T with Authentication Bypass Vulnerability	7.4	More Details
CVE-2026-55075	Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, two flaws in Coder's OIDC login chained into account takeover. Email-based user matching fell back to linking by email without checking for an existing link to a different IdP subject and the `email_verified` claim was only enforced when present as a boolean `false` so an absent or non-boolean claim was treated as verified. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 restricts the email fallback to first-time and legacy linking and defaults `email_verified` to false when the claim is absent or of an unexpected type. As a workaround, configure the OIDC provider to disallow self-registration or to require email verification before issuing tokens.	7.4	More Details
CVE-	Insertion of Sensitive Information Into Sent Data vulnerability in HubSpot allows Retrieve Embedded Sensitive		More

2026-57736	Data. This issue affects HubSpot: from n/a through 11.3.51.	7.4	Details
CVE-2026-6900	Improper certificate validation vulnerability in B&R Industrial Automation GmbH APROL. This issue affects APROL: before R 4.4-01P5.	7.4	More Details
CVE-2026-57991	Improper link resolution before file access ('link following') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	7.4	More Details
CVE-2026-57993	Server-side request forgery (ssrf) in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	7.4	More Details
CVE-2026-55076	Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, Coder's OIDC callback checked `email_verified` with a direct Go `bool` type assertion. When an IdP returned the claim as a non-boolean (for example the string `"false"`) or omitted it, the assertion failed open and the email was treated as verified. Combined with an unconditional email-based account fallback, this enabled account takeover. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 coerces `email_verified` across bool, string and numeric types (fail-closed) and blocks the email fallback when the matched user already has a different linked IdP subject. As a workaround, ensure the IdP returns `email_verified` as a native JSON boolean. The email-fallback linking issue has no configuration workaround; upgrading is required.	7.4	More Details
CVE-2026-57723	Cross-Site Request Forgery (CSRF) vulnerability in e4jvikwp VikBooking Hotel Booking Engine & PMS allows Path Traversal. This issue affects VikBooking Hotel Booking Engine & PMS: from n/a through 1.8.12.	7.4	More Details
CVE-2026-9080	Calling `curl_easy_pause()` within the event-based `CURLMOPT_SOCKETFUNCTION` callback triggers a use-after-free vulnerability, where libcurl attempts to store a flag using a dangling struct pointer immediately after that pointer's memory has been freed.	7.3	More Details
CVE-2026-58379	A flaw was found in GIMP's Paint Shop Pro (PSP) file format parser. This heap buffer overflow vulnerability allows a remote attacker to cause arbitrary code execution or a denial of service (DoS) by tricking a user into opening a specially crafted PSP image file. The vulnerability occurs because the software incorrectly calculates buffer sizes when processing low bit-depth images, leading to an overwrite of adjacent memory.	7.3	More Details
CVE-2026-8079	In Progress Flowmon versions prior to 12.5.9 and 13.0.11, a vulnerability exists whereby an authenticated low-privileged user may craft a request during the PDF generation process that results in operations being performed with the privileges of another user, potentially leading to unauthorized access to sensitive data and unintended modifications to system configuration.	7.3	More Details
CVE-2026-14649	A vulnerability was detected in code-projects Online Voting System 1.0. Impacted is the function test_input of the file /saveVote.php. Performing a manipulation of the argument voterName/voterEmail/voterID/selectedCandidate results in sql injection. The attack can be initiated remotely.	7.3	More Details
CVE-2026-14802	A vulnerability was detected in react create-react-app up to 5.0.1 on macOS. This affects the function startBrowserProcess of the file openBrowser.js of the component react-dev-utils. Performing a manipulation results in os command injection. Remote exploitation of the attack is possible. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-14747	A vulnerability was detected in code-projects Real State Services 1.0. Affected by this vulnerability is an unknown functionality of the file /addprojectsale.php. The manipulation of the argument amen results in sql injection. The attack can be launched remotely.	7.3	More Details
CVE-2026-14754	A flaw has been found in code-projects Hotel and Tourism Reservation 1.0. Affected is an unknown function of the file /admin/add_room.php. Executing a manipulation of the argument delete_image/edit/description/number/price/rooms/type can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-14722	A vulnerability was found in tiddly-gittly TidGi-Desktop up to 0.13.0. This impacts an unknown function of the file src/services/wiki/wikiWorker/loadWikiTiddlersWithSubWikis.ts of the component Git Repository Import. The manipulation results in code injection. The attack may be performed from remote. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-14753	A vulnerability was detected in mjperpinosa stumasy up to 327d1b0f2915ba79d7ef8ebb74553e987609d9be. This impacts an unknown function of the file /PHP/objects/notes of the component Note Handler/Assignment Handler. Performing a manipulation of the argument assignment_item_id results in authorization bypass. The attack can be initiated remotely. The exploit is now public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	7.3	More Details

	The project was informed of the problem early through an issue report but has not responded yet.		
CVE-2026-14750	A security flaw has been discovered in mjperpinosa stumasy up to 327d1b0f2915ba79d7ef8ebb74553e987609d9be. The affected element is the function Notes_controller::accessing_dictionary_authorization of the file application/PHP/objects/notes/accessing_dictionary_authorization.php. The manipulation of the argument Password results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-14749	A vulnerability was identified in mjperpinosa stumasy up to 327d1b0f2915ba79d7ef8ebb74553e987609d9be. Impacted is the function eval of the file application/pages/imba_calculator/calculate.php. The manipulation of the argument mathematical_sentence leads to code injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-14732	A security vulnerability has been detected in SourceCodester Class and Exam Timetabling System 1.0. This vulnerability affects unknown code of the file /edit_exam.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-43825	Untrusted Java Deserialization in Apache OpenNLP SvmDoccatModel Versions Affected: before 3.0.0-M4 (libsvm document categorization module; introduced in OPENNLP-1808 and only present on the 3.x line) Description: SvmDoccatModel.deserialize(InputStream) reads an attacker-controlled stream with java.io.ObjectInputStream and calls readObject() without an ObjectInputFilter installed. ObjectInputStream materialises every class referenced in the stream before the resulting object is cast to SvmDoccatModel, so the cast that follows readObject() executes only after the foreign object graph has already been deserialised in full. If a Java deserialization gadget chain is available on the consumer's classpath, a crafted payload supplied to deserialize() executes arbitrary code in the JVM that loads it. Apache OpenNLP itself does not ship a known gadget chain, so the realistic risk is to downstream applications that embed the libsvm module alongside vulnerable transitive dependencies. The method is public and static, so any caller can pass an untrusted stream to it directly. The practical impact is remote code execution against processes that load SvmDoccatModel instances from untrusted or semi-trusted origins. Mitigation: 3.x users should upgrade to 3.0.0-M4. Users who cannot upgrade immediately should treat all serialized SvmDoccatModel streams as untrusted input unless their provenance is verified, and should avoid invoking SvmDoccatModel.deserialize() on streams supplied by end users or fetched from third-party sources without integrity checks.	7.3	More Details
CVE-2026-14713	A security flaw has been discovered in SourceCodester Pizzafy E-Commerce System 1.0. This vulnerability affects unknown code of the file /admin/ajax.php?action=confirm_order. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-14660	A vulnerability was found in code-projects Online Job Portal 1.0. The affected element is an unknown function of the file login.php. Performing a manipulation of the argument txtUser/txtPass results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-14705	A vulnerability was determined in code-projects Online Examination 1.0. Affected by this issue is some unknown functionality of the file head.php. Executing a manipulation of the argument uname/password can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-14700	A security vulnerability has been detected in code-projects Internship Management System 1.0. The impacted element is an unknown function of the file employer/login.php of the component Employer Login Endpoint. The manipulation of the argument email/password leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-14695	A vulnerability was found in SourceCodester Multi-Vendor Online Grocery Management System 1.0. This affects the function save_client of the file classes/Users.php of the component Registration Handler. The manipulation of the argument Name results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-14746	A security vulnerability has been detected in code-projects Real State Services 1.0. Affected is an unknown function of the file /addprojectrent.php. The manipulation of the argument amen leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-14756	A vulnerability was found in code-projects Hotel and Tourism Reservation 1.0. Affected by this issue is some unknown functionality of the file /admin/add_tour.php of the component Tour Management Page. The manipulation of the argument delete_image results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	7.3	More Details
	A weakness has been identified in code-projects Real State Services 1.0. This impacts an unknown function of		

CVE-2026-14745	the file /single-list_rent.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-14744	A security flaw has been discovered in code-projects Real State Services 1.0. This affects an unknown function of the file /normalHomeRent.php. Performing a manipulation of the argument loc results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-14743	A vulnerability was identified in code-projects Real State Services 1.0. The impacted element is an unknown function of the file /normalHomeSale.php. Such manipulation of the argument loc leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-14737	A vulnerability was identified in Hanwang e-Face General Management Platform 6.3.5.4. This impacts an unknown function of the file /sysAuthStr/querySysAuthStr.do. The manipulation of the argument order leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-54263	Wagtail is an open source content management system built on Django. In versions prior to 7.0.8, 7.3.3 and 7.4.2, reflected cross-site scripting (XSS) vulnerability exists on the dynamic image URL generator view within the Wagtail admin interface. A user with a limited-permission editor account for the Wagtail admin could craft a URL that, when viewed by a user with higher privileges, could perform actions with that user's credentials. The vulnerability is present for all sites, even if they do not enable the dynamic image serve view. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. This issue has been fixed in versions 7.0.8, 7.3.3, and 7.4.2.	7.3	More Details
CVE-2026-49042	Improper Input Validation vulnerability in Apache Camel. This issue affects Apache Camel: from 4.8.0 through 4.18.2, from 4.19.0 through 4.20.0. Users are recommended to upgrade to version 4.18.3, 4.21.0, which fixes the issue.	7.3	More Details
CVE-2026-14690	A weakness has been identified in SourceCodester Multi-Vendor Online Grocery Management System 1.0. This affects the function save_users of the file classes/Users.php. This manipulation causes improper authorization. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-14736	A vulnerability was found in Ruijie RG-UAC up to 1.0-R1.8.2.p5. The impacted element is an unknown function of the file user_auth_commit.php. Performing a manipulation of the argument upload_image results in unrestricted upload. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-14735	A vulnerability has been found in code-projects Smart Parking System 1.0. The affected element is an unknown function of the file /parkings/parkings.php. Such manipulation of the argument street/city/status leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-14734	A flaw has been found in SourceCodester Class and Exam Timetabling System 1.0. Impacted is an unknown function of the file /edit_product.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	7.3	More Details
CVE-2026-14733	A vulnerability was detected in SourceCodester Class and Exam Timetabling System 1.0. This issue affects some unknown processing of the file /edit_coursea.php. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-58380	A flaw was found in GIMP's PNM file format parser. When parsing a specially crafted PNM file, the pnmscanner_gettoken() function writes a null terminator one byte past the end of a stack-allocated buffer due to an off-by-one error in the loop boundary check. This could lead to memory corruption, potentially resulting in denial of service or arbitrary code execution.	7.3	More Details
CVE-2026-58384	A flaw was found in GIMP's PSD parser. An integer overflow in read_RLE_channel() can cause an undersized heap allocation for the RLE row-length table, after which subsequent per-row writes corrupt heap memory. This could lead to memory corruption, potentially resulting in denial of service or arbitrary code execution.	7.3	More Details
CVE-2026-14755	A vulnerability has been found in code-projects Hotel and Tourism Reservation 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/reservations.php of the component Reservations Management Page. The manipulation of the argument delete leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-14762	A vulnerability was detected in code-projects Hotel and Tourism Reservation 1.0. The impacted element is an unknown function of the file /admin/rooms.php of the component Room Management Page. The manipulation of the argument delete results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	7.3	More Details
CVE-	A vulnerability was detected in SourceCodester Class and Exam Timetabling System 1.0. Impacted is an		

2026-14770	unknown function of the file /edit_room.php. Performing a manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-14622	A vulnerability was found in jairiidriss restaurant-website-php-mysql up to 521428b5b612449df0cf4a5d15ee40cba67f3d35. This vulnerability affects unknown code of the file /admin/ajax_files of the component AJAX Endpoint. Performing a manipulation results in missing authentication. The attack is possible to be carried out remotely. The exploit has been made public and could be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-14635	A security flaw has been discovered in kirilkirkov Ecommerce-CodeIgniter-Bootstrap up to 222ff31c06687b1c6d0e1ab63953f82c3674c52b. This issue affects some unknown processing of the file application/modules/vendor/controllers/AddProduct.php of the component Vendor Multi-Image Endpoint. Performing a manipulation of the argument folder results in path traversal. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The patch is named 2a9497ff11f36e573ad99e1c357ff0e6ded49745. Applying a patch is the recommended action to fix this issue.	7.3	More Details
CVE-2026-14640	A vulnerability was found in CodeAstro Apartment Visitor Management System 1.0. Affected is an unknown function of the file /index.php of the component Login. Performing a manipulation of the argument Username results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-14641	A vulnerability was determined in SourceCodester Class and Exam Timetabling System 1.0. Affected by this vulnerability is an unknown functionality of the file /edit_course.php. Executing a manipulation of the argument ID can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-14642	A vulnerability was identified in SourceCodester Class and Exam Timetabling System 1.0. Affected by this issue is some unknown functionality of the file /edit_class2.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-13760	OS command injection in the NodejsFunction Docker bundling pipeline (OsCommand helper) in AWS aws-cdk-lib on all platforms might allow a actor who controls dependency version strings in a project's package.json file to execute arbitrary commands on the host running the CDK toolchain via injected shell metacharacters in the OsCommand helper. This issue requires the actor to control the content of a package.json dependency version string that is processed during Docker-based bundling with nodeModules specified. To remediate this issue, users should upgrade to v2.260.0.	7.3	More Details
CVE-2026-14648	A security vulnerability has been detected in code-projects Online Voting System up to 0.x/1.0. This issue affects the function test_input of the file /authentication.php of the component Login. Such manipulation of the argument adminUserName/adminPassword leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-41121	Dell Device Management Agent, versions prior to DDMA 26.05, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	7.3	More Details
CVE-2026-43866	Deserialization of Untrusted Data vulnerability in Apache Camel, Apache Camel JMS component. JmsBinding.extractBodyFromJms() in camel-jms - and the equivalent JmsBinding in camel-sjms - deserializes the payload of an incoming JMS ObjectMessage via jakarta.jms.ObjectMessage.getObject() whenever the mapJmsMessage option is enabled (the default) and Camel acts as a JMS consumer. The CVE-2026-40860 hardening added a post-deserialization class check that rejects classes outside the default allow-list java.**;javax.**;org.apache.camel.**;!*. However org.apache.camel.support.DefaultExchangeHolder itself lives in the allow-listed org.apache.camel.** namespace, so an ObjectMessage whose top-level object is a DefaultExchangeHolder passes the check. The receiving side then calls DefaultExchangeHolder.unmarshal() on it without requiring the transferExchange option to be enabled - an asymmetric trust boundary, since the sending side gates ObjectMessage and transferExchange handling but the receiving side did not - writing every non-null field of the holder into the Exchange: the message body, the IN and OUT headers, the exchange properties, the variables, the exchange id and the exception. An attacker who can publish an ObjectMessage to a queue or topic consumed by an affected Camel application can therefore inject arbitrary Exchange state using only universally-trusted java.lang and java.util types, with no deserialization gadget chain required, to manipulate routing and headers, exchange properties and error handling. The same handling applies to camel-sjms and camel-sjms2, and to the JMS-family components built on JmsComponent and JmsBinding: camel-amqp, camel-activemq and camel-activemq6. This is a bypass of the CVE-2026-40860 fix rather than a flaw in it. This issue affects Apache Camel: from 3.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0; Apache Camel: from 3.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are	7.3	More Details

	on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, JMS ObjectMessage handling is disabled by default in camel-jms, camel-sjms and the JMS-family components (a new objectMessageEnabled option defaults to false at the component and endpoint level), so an incoming ObjectMessage - including a DefaultExchangeHolder payload - is no longer deserialized unless the option is explicitly enabled; only set objectMessageEnabled=true when the consumed JMS destination is fed exclusively by trusted producers. For deployments that cannot upgrade immediately, restrict publish access to the queues and topics consumed by Camel to trusted producers via JMS broker authorization, and do not expose JMS consumers that map ObjectMessage bodies to untrusted networks; a JMS-provider deserialization allow-list does not mitigate this specific bypass because the crafted payload uses only universally-trusted classes.		
CVE-2026-14778	A security vulnerability has been detected in SourceCodester Onlne Examination & Learning Management System 1.0. This affects an unknown part of the file /ajax_enroll.php of the component Enrollment Management. The manipulation of the argument student_id/schedule_id/action leads to improper authorization. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The name of the affected product appears to have a typo in it.	7.3	More Details
CVE-2026-14772	A vulnerability has been found in SourceCodester Class and Exam Timetabling System 1.0/1.php. The impacted element is an unknown function of the file /edit_course1.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-14771	A flaw has been found in SourceCodester Class and Exam Timetabling System 1.0/1.php. The affected element is an unknown function of the file /edit_exam1.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-14688	A vulnerability was identified in itsourcecode Online Hotel Management System 1.0. The affected element is an unknown function of the file /admin/login.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-14652	A vulnerability was found in SourceCodester Simple and Nice Shopping Cart Script 1.0. This affects an unknown function of the file /admin/login.php of the component Admin Login. The manipulation of the argument Username results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-46588	Improper Input Validation vulnerability in Apache Camel. This issue affects Apache Camel: through 4.14.7, from 4.15.0 through 4.18.2, from 4.19.0 through 4.20.0. Users are recommended to upgrade to version 4.14.8, 4.18.3, 4.21.0, which fixes the issue.	7.3	More Details
CVE-2026-14653	A vulnerability was determined in SourceCodester Simple and Nice Shopping Cart Script 1.0. This impacts an unknown function of the file /admin/mensproductdeletequery.php. This manipulation of the argument user_id causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-14769	A security vulnerability has been detected in code-projects Real State Services 1.0. This issue affects some unknown processing of the file /pay.php. Such manipulation of the argument Bankname leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-14719	A flaw has been found in SourceCodester Onlne Examination & Learning Management System 1.0. The impacted element is an unknown function of the file register.php of the component Registration Endpoint. Executing a manipulation of the argument role can lead to improper privilege management. The attack can be executed remotely. The exploit has been published and may be used. The name of the affected product appears to have a typo in it.	7.3	More Details
CVE-2026-14768	A weakness has been identified in code-projects Real State Services 1.0. This vulnerability affects unknown code of the file /builderHome.php. This manipulation of the argument loc causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-14763	A flaw has been found in code-projects Hotel and Tourism Reservation 1.0. This affects an unknown function of the file /admin/tour_reserves.php of the component Tour Reservations Page. This manipulation of the argument tour causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-14654	A vulnerability was identified in SourceCodester Simple and Nice Shopping Cart Script 1.0. Affected is an unknown function of the file /admin/girlsproductdeletequery.php. Such manipulation of the argument user_id leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-	A vulnerability has been found in code-projects Hotel and Tourism Reservation 1.0. This impacts an unknown		

2026-14764	function of the file /admin/add_event.php of the component Event Management Page. Such manipulation of the argument fdetails leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-46587	Improper Input Validation vulnerability in Apache Camel. This issue affects Apache Camel: through 4.14.7, from 4.15.0 through 4.18.2, from 4.19.0 through 4.20.0. Users are recommended to upgrade to version 4.14.8, 4.18.3, 4.21.0, which fixes the issue.	7.3	More Details
CVE-2026-7517	The Custom Payment Gateways for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'alg_wc_cpg_input_fields' parameter in all versions up to, and including, 2.1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This vulnerability is exploitable by unauthenticated guest users submitting a crafted checkout POST request, requiring no custom input fields to be configured in the plugin.	7.2	More Details
CVE-2026-11883	The WebAuthn Provider for Two Factor WordPress plugin before 2.5.6 does not correctly validate the second-factor authentication response, allowing an attacker who already knows a user's password to bypass the two-factor authentication requirement by submitting a malformed request.	7.2	More Details
CVE-2026-13040	The NEX-Forms – Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'real_val__' parameter in all versions up to, and including, 9.2.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The submission endpoint is registered via wp_ajax_nopriv_submit_nex_form with no nonce verification, making it fully accessible to unauthenticated attackers without any CSRF token.	7.2	More Details
CVE-2026-12142	The NEX-Forms – Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via '_name[]' Array Parameter in all versions up to, and including, 9.2.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The wp_kses() output filtering pass provides no mitigation because NEXForms_allowed_tags() explicitly permits <script>, <iframe src/srcdoc>, and JS event handlers such as onClick, onBlur, and onChange in its allow-list.	7.2	More Details
CVE-2026-53479	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper neutralization of special elements used in an OS command ('OS command Injection') vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to protection mechanism bypass. This is a Critical vulnerability as it allows an attacker to invoke arbitrary command execution with root privileges; so Dell recommends customers to upgrade at the earliest opportunity.	7.2	More Details
CVE-2026-7829	UltraVNC repeater through 1.8.2.2 contains a post-authentication out-of-bounds write in the allow/deny rule parser. In repeater/webgui/settings.c:225-272, after strncpy_s copies a rule token into temp1[rule1] (25-byte destination) or temp2/temp3 (16-byte destination), the code unconditionally writes a NUL terminator at temp1[rule1][len] = 0 without clamping len to the destination size. When an authenticated administrator saves a rule with a token length equal to or greater than the destination size, the NUL byte is written one or more bytes past the end of the stack-allocated array, corrupting adjacent stack data. An attacker who has obtained admin credentials (including via CVE-2026-7839 default password) can trigger this to gain code execution on the repeater host.	7.2	More Details
CVE-2026-55077	Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, the `PUT /api/v2/users/{user}/password` endpoint authorized only `ActionUpdatePersonal` and did not prevent a `user-admin` from resetting an `owner` account's password. It also did not require the current password when an admin reset another user's password. Exploitation requires the privileged `user-admin` role so practical risk is limited to deployments that grant `user-admin` to less trusted operators. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 prevents non-owner users from resetting the password of an account that holds the `owner` role. As a workaround, restrict the `user-admin` role to trusted administrators.	7.2	More Details
CVE-2026-49814	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution.	7.2	More Details
CVE-2026-58263	Jodit Editor is a WYSIWYG editor with written in pure TypeScript file and image editing capabilities. In versions prior to 4.12.28, the built-in clean-html sanitizer can be bypassed by a MathML/<style> carrier that hides a dangerous element from the sanitizer's element walk, so a no-interaction event handler survives into the editor value, potentially causing Mutation XSS. When an application supplies attacker-influenced HTML to the editor's value-set or insertion paths, the sanitized output still contains a live <img ... onload=...> (or another non-onerror handler such as onfocus). A consumer that renders that output (element.innerHTML =	7.2	More Details

	editor.value) executes the handler with no user interaction. This issue has been fixed in version 4.12.28.		
CVE-2026-9834	The WP Database Backup – Unlimited Database & Files Backup by Backup for WP plugin for WordPress is vulnerable to OS Command Injection in all versions up to and including 7.11 via the `wp_db_exclude_table` parameter. This is due to the direct concatenation of user-supplied `$_POST['wp_db_exclude_table']` values into the `mysqldump` shell command string in the `mysqldump()` function of `includes/admin/class-wpdb-admin.php` without wrapping them in `escapeshellarg()`—every other argument in the same command (DB_USER, DB_PASSWORD, host, filename, DB_NAME) is properly escaped, making the exclude-table values the sole exception—and because the only applied filtering, `sanitize_text_field()` via `recursive_sanitize_text_field()`, strips HTML tags but leaves shell metacharacters such as `;`, `\|`, `` ` ``, and `$()` intact. This makes it possible for authenticated attackers, with administrator-level access and above, to execute arbitrary operating system commands on the server, potentially enabling full remote code execution. The injection is stored: malicious values submitted through the plugin settings form are persisted to the WordPress options table via `update_option('wp_db_exclude_table')` and later retrieved with `get_option()` and passed unsanitized to `shell_exec()` whenever a backup operation runs.	7.2	More Details
CVE-2026-23698	Vtiger CRM through 8.4.0 contains an authenticated remote code execution vulnerability in the admin module import feature that allows administrator-level attackers to upload arbitrary PHP files by submitting a crafted zip archive through the ModuleManager import function, which extracts contents directly into the modules/ directory under the web root without validating file types beyond the manifest.xml descriptor. Attackers can place executable PHP files in the modules/ directory that become directly accessible via HTTP, bypassing Vtiger's authentication and authorization layer entirely since Apache resolves the path and invokes the PHP interpreter before the application routing layer is involved, resulting in a persistent web shell independent of the originating session.	7.2	More Details
CVE-2026-58298	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	7.2	More Details
CVE-2026-53478	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper neutralization of special elements used in an OS command ('OS command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to command execution.	7.2	More Details
CVE-2026-49815	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper neutralization of special Elements used in an OS command ('OS command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to execution of arbitrary OS commands.	7.2	More Details
CVE-2026-13731	The WPBot – AI ChatBot for Live Support, Lead Generation, AI Services plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'conversation' parameter in all versions up to, and including, 8.4.9 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The AJAX nonce required to authenticate the save request is publicly emitted on every frontend page via wp_localize_script, making it freely obtainable by any anonymous visitor and removing any practical barrier to exploitation.	7.2	More Details
CVE-2026-57348	Unauthenticated Server Side Request Forgery (SSRF) in Paid Member Subscriptions <= 3.0.4 versions.	7.2	More Details
CVE-2026-9148	The Comments – wpDiscuz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the guest commenter 'Website' field in versions up to, and including, 7.6.56 This is due to insufficient output escaping in the getCommentAuthor() function, which interpolates the stored comment_author_url value directly into single-quoted HTML attributes without applying esc_url() or esc_attr(). This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-20779	Gitea versions from 1.5.0 before 1.26.3 have a TOTP single-use enforcement defect that allows a valid TOTP code to be accepted more than once across web two-factor authentication flows and the Basic Auth X-Gitea-OTP path.	7.1	More Details
CVE-2026-57988	Relative path traversal in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	7.1	More Details
CVE-2026-57977	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	7.1	More Details

CVE-2026-57761	Unauthenticated Cross Site Request Forgery (CSRF) in SEOWP <= 3.12.2 versions.	7.1	More Details
CVE-2026-55153	mchange-commons-java is a Java library of shared utility classes used by mchange projects like the c3p0 connection pool. Prior to version 0.6.0, its JNDI ObjectFactory implementation (com.mchange.v2.naming.JavaBeanObjectFactory) will construct objects of arbitrary classes and initialize "JavaBean"-style properties, which for certain classes enables JNDI injection and "deserialization gadgets." Such initialization is unsafe for some classes: for example, setting the contentType property of a Swing JEditorPane to text/html and its text property to HTML containing a stylesheet <link> will provoke an HTTP GET on an arbitrary URL, potentially from within a trusted security domain. The problem is aggravated by the library's ReferenceIndirector, through which malicious JNDI Reference objects can be smuggled in for dereferencing wherever an application reads a Java-serialized object. This has been resolved in version 0.6.0.	7.1	More Details
CVE-2026-58583	FluxInk (formerly Sunia SPB Peripheral) Color Management Driver (TcnPeripheral64.sys) 1.0.7.2 allows local privilege escalation for a standard user account via arbitrary physical memory mapping at \Device\PhysicalMemory. Fixed in version 1.0.7.6. The fixed driver is currently available in the Windows 11 25H2 HLK (Hardware Lab Kit). The fixed driver may be available through Windows Update or from Lenovo directly.	7.1	More Details
CVE-2026-59194	pnpm is a package manager. Prior to 10.34.4 and 11.7.0, a crafted patch entry could resolve outside the configured patches directory and cause pnpm patch-remove to delete an arbitrary reachable file. This vulnerability is fixed in 10.34.4 and 11.7.0.	7.1	More Details
CVE-2026-58296	Exposure of private personal information to an unauthorized actor in Microsoft Edge for Android allows an unauthorized attacker to disclose information over a network.	7.1	More Details
CVE-2026-58297	Exposure of private personal information to an unauthorized actor in Microsoft Edge for Android allows an unauthorized attacker to disclose information over a network.	7.1	More Details
CVE-2026-57757	Unauthenticated Cross Site Request Forgery (CSRF) in pCloud WP Backup <= 2.0.2 versions.	7.1	More Details
CVE-2026-28740	Gitea versions up to and including 1.26.2 allow Git LFS object reuse to authorize private source objects for users who have repository access but lack Code-unit access.	7.1	More Details
CVE-2026-59196	pnpm is a package manager. Prior to 10.34.4 and 11.7.0, a crafted lockfile alias could be joined directly under a hoisted node_modules directory. Traversal aliases could escape that directory, while reserved aliases such as .bin or .pnpm could overwrite pnpm-owned layout. This vulnerability is fixed in 10.34.4 and 11.7.0.	7.1	More Details
CVE-2026-13705	Imager versions before 1.032 for Perl have a heap out-of-bounds read in the bundled Imager::File::SGI reader via a 16-bit RLE literal run in read_rgb_16_rle. read_rgb_16_rle guards each literal run with if (count > data_left), but count is a pixel count while every 16-bit sample consumes two bytes. The copy loop reads inp[0] * 256 + inp[1] and advances two bytes per pixel, so a run with data_left / 2 < count <= data_left passes the guard yet consumes 2 * count bytes and reads past the end of the buffer. The 8-bit path is unaffected because there one pixel is one byte. Reading a crafted SGI image through Imager->read triggers the over-read before the parser rejects the malformed image, which can crash the process.	7.1	More Details
CVE-2026-57758	Unauthenticated Cross Site Request Forgery (CSRF) in Permalink Manager for WooCommerce <= 1.0.8.2 versions.	7.1	More Details
CVE-2026-59704	Cap's GET /api/video/ai endpoint fails to validate user ownership or membership before returning private video AI metadata including titles, summaries, and chapters. Authenticated attackers can supply arbitrary video IDs to read sensitive AI-generated content and trigger unauthorized AI generation that consumes the video owner's credits without consent.	7.1	More Details
CVE-2026-57358	Unauthenticated Cross Site Scripting (XSS) in Customize My Account for WooCommerce <= 4.3.9 versions.	7.1	More Details
CVE-2026-57357	Unauthenticated Cross Site Scripting (XSS) in Search Atlas SEO <= 2.6.6 versions.	7.1	More Details
CVE-2026-57345	Unauthenticated Cross Site Scripting (XSS) in Internal Links Manager <= 3.0.3 versions.	7.1	More Details

CVE-2026-57678	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemePunch Slider Revolution allows Reflected XSS. This issue affects Slider Revolution: from 7.0.0 through 7.0.16.	7.1	More Details
CVE-2026-57675	Unauthenticated Cross Site Scripting (XSS) in WP Photo Album Plus <= 9.2.02.004 versions.	7.1	More Details
CVE-2026-57674	Unauthenticated Cross Site Scripting (XSS) in Timetics <= 1.0.58 versions.	7.1	More Details
CVE-2026-57673	Unauthenticated Cross Site Scripting (XSS) in Optimole <= 4.2.7 versions.	7.1	More Details
CVE-2026-57349	Unauthenticated Cross Site Scripting (XSS) in WPeMatico RSS Feed Fetcher <= 2.8.17 versions.	7.1	More Details
CVE-2026-57672	Unauthenticated Cross Site Scripting (XSS) in wpDataTables <= 6.5.1.1 versions.	7.1	More Details
CVE-2026-57671	Unauthenticated Cross Site Scripting (XSS) in perfmatters <= 2.6.4 versions.	7.1	More Details
CVE-2026-57670	Unauthenticated Cross Site Scripting (XSS) in Google Maps CP <= 1.2.5 versions.	7.1	More Details
CVE-2026-57350	Unauthenticated Cross Site Scripting (XSS) in WP Debugging <= 2.12.2 versions.	7.1	More Details
CVE-2026-57426	Unauthenticated Cross Site Scripting (XSS) in Modula - PRO <= 2.10.8 versions.	7.1	More Details
CVE-2026-57366	Unauthenticated Cross Site Scripting (XSS) in WPAdverts <= 2.3.1 versions.	7.1	More Details
CVE-2026-57362	Unauthenticated Cross Site Scripting (XSS) in ChatBot <= 8.3.2 versions.	7.1	More Details
CVE-2026-57351	Unauthenticated Cross Site Scripting (XSS) in HandL UTM Grabber <= 2.9.2 versions.	7.1	More Details
CVE-2026-57361	Unauthenticated Cross Site Scripting (XSS) in Survey Maker <= 5.2.2.5 versions.	7.1	More Details
CVE-2026-57360	Unauthenticated Cross Site Scripting (XSS) in eCommerce Product Catalog <= 3.5.4 versions.	7.1	More Details
CVE-2026-57359	Unauthenticated Cross Site Scripting (XSS) in ReviewX <= 2.3.10 versions.	7.1	More Details
CVE-2026-57344	Unauthenticated Cross Site Scripting (XSS) in Classified Listing <= 5.4.2 versions.	7.1	More Details
CVE-2026-57343	Unauthenticated Cross Site Scripting (XSS) in Real Estate 7 <= 3.5.9 versions.	7.1	More Details
CVE-			More

2026-57682	Unauthenticated Cross Site Scripting (XSS) in Simple Link Directory <= 15.0.5 versions.	7.1	Details
CVE-2026-27402	Unauthenticated Cross Site Scripting (XSS) in Kids Life | Children School WordPress <= 5.2 versions.	7.1	More Details
CVE-2026-21383	Cryptographic Issue when using a static initialization vector for AES-GCM key wrapping, which requires a unique value for each call to ensure security.	7.1	More Details
CVE-2026-53904	MCO is vulnerable to Account Denial of Service due to improper implementation of password reset functionality. Each password reset request invalidates previously set password as well as previously issued temporary passwords, furthermore, password resets are not limited in any way. An attacker who provides victim's email and answer to their security question, can successfully initiate the reset process and continuously invalidate credentials, effectively locking the victim out of their account. Answering security questions has a limited number of tries which lowers the risk of this vulnerability. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 25.3.3.1 but may also affect other versions.	7.1	More Details
CVE-2025-69152	Unauthenticated Cross Site Scripting (XSS) in Artale | Wedding Photography WordPress <= 2.2.2 versions.	7.1	More Details
CVE-2025-69153	Unauthenticated Cross Site Scripting (XSS) in Trendy Travel <= 6.7 versions.	7.1	More Details
CVE-2025-69154	Unauthenticated Cross Site Scripting (XSS) in SpaLab | Beauty Salon WordPress Theme <= 6.7 versions.	7.1	More Details
CVE-2025-69155	Unauthenticated Cross Site Scripting (XSS) in Fitness Zone WordPress Theme <= 5.7 versions.	7.1	More Details
CVE-2025-69156	Unauthenticated Cross Site Scripting (XSS) in Kids Zone - Children WordPress Theme <= 5.4 versions.	7.1	More Details
CVE-2026-27404	Unauthenticated Cross Site Scripting (XSS) in LMS <= 9.7 versions.	7.1	More Details
CVE-2026-53905	MCO does not properly enforce authorization checks in the /customer/servlet/mco/webapi/admin-view-hierarchy/get-acl-tree-structure endpoint. An authenticated, low-privileged user can retrieve administrator access control structures without proper authorization checks. This may expose sensitive permission mappings and internal configuration details. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 25.3.3.1 but may also affect other versions.	7.1	More Details
CVE-2026-27408	Unauthenticated Cross Site Scripting (XSS) in NativeChurch <= 4.8.8.2 versions.	7.1	More Details
CVE-2026-7017	HTTP::Tiny versions before 0.095 for Perl forward credential headers to cross-origin redirect targets. When the server returns a 3xx redirect, `_maybe_redirect` follows the `Location:` header and `_prepare_headers_and_cb` re-merges the caller's `headers` argument into the new request, without checking whether the redirect target shares an origin with the original URL. Caller-supplied `Authorization`, `Cookie` and `Proxy-Authorization` headers are therefore re-sent to whatever host the redirect names, across scheme, host or port boundaries, and including `https` to `http` downgrades that expose them in plaintext on the wire. The HTTP::Tiny POD note that "Authorization headers will not be included in a redirected request" applied only to the URL-userinfo Basic-auth path, not to headers passed explicitly by the caller.	7.1	More Details
CVE-2026-57746	Subscriber Broken Access Control in Booked <= 3.0.0 versions.	7.1	More Details
CVE-2026-27425	Unauthenticated Cross Site Scripting (XSS) in Automotive Listings <= 18.6 versions.	7.1	More Details
CVE-			

2026-27426	Unauthenticated Cross Site Scripting (XSS) in Automotive Car Dealership Business <= 13.3.3 versions.	7.1	More Details
CVE-2026-57686	Unauthenticated Cross Site Scripting (XSS) in WowAddons <= 1.6.14 versions.	7.1	More Details
CVE-2026-27430	Unauthenticated Cross Site Scripting (XSS) in TheFox <= 3.9.76 versions.	7.1	More Details
CVE-2026-57356	Unauthenticated Cross Site Scripting (XSS) in MC Woocommerce Wishlist <= 1.9.19 versions.	7.1	More Details
CVE-2026-53935	Cilium is a networking, observability, and security solution. Prior to 1.17.16, from 1.18.2 to 1.18.9, and from 1.19.0 to 1.19.3, users with the ability to create CiliumLocalRedirectPolicies can specify arbitrary ClusterIPs via addressMatcher, enabling hijacking traffic to Services in any namespace and bypassing namespace scoping enforced by serviceMatcher; deleting such a policy can also corrupt Cilium internal service state and stop service translation for the affected Service. This issue is fixed in versions 1.17.16, 1.18.10, and 1.19.4.	6.9	More Details
CVE-2026-58522	Relative path traversal in Microsoft Edge for Android allows an unauthorized attacker to disclose information locally.	6.8	More Details
CVE-2026-14440	Description: To issue and renew TLS certificates on behalf of customers, Cloudflare's Universal SSL feature automatically manages the CAA RRset for the customer's zone. This auto-managed RRset is permissive by design (e.g. 'issue "letsencrypt.org"' without parameters). On Universal SSL zones, Cloudflare's authoritative DNS serves this auto-managed RRset at query time, superseding any customer-configured CAA records on the zone. When a customer publishes a stricter CAA record using the RFC 8657 accounturi or validationmethods parameters, the Certificate Authority does not observe those parameters when evaluating the served RRset under RFC 8659. As a result, the RFC 8657 account-binding and validation-method-binding protections are not enforced end-to-end on Universal SSL zones. Successful exploitation could result in issuance of a browser-trusted TLS certificate to an attacker, enabling MITM against the affected domain. Exploitation is non-trivial in practice: an attacker would need to hold an ACME account at one of the Certificate Authorities in the served CAA RRset and to simultaneously satisfy domain control validation across the multiple geographically distinct Network Perspectives the CA relies on for Multi-Perspective Issuance Corroboration. Cloudflare prefixes are anycast-announced from hundreds of locations globally, raising the bar against single-vantage-point BGP hijacks. Any resulting misissuance of a browser-trusted certificate is subject to Certificate Transparency logging required by major browsers, and would be visible to CT monitoring. Mitigation: Customers requiring strict RFC 8657 enforcement need to disable Universal SSL on the affected zone. Universal SSL's automatic CAA management and customer-set RFC 8657 accounturi and validationmethods enforcement are mutually exclusive by the nature of the issue, so there is no in-product workaround that preserves both. Certificate Transparency monitoring is recommended for all customers as a general detection control. Credits: David Osipov (ORCID: https://orcid.org/0009-0005-2713-9242), independent researcher	6.8	More Details
CVE-2026-10077	The yootheme WordPress theme before 5.0.35 does not prevent its bundled front-end framework from treating certain HTML attributes, which are permitted by wp_kses_post(), as markup, allowing users with the Author role to perform Stored Cross-Site Scripting attacks that execute in the browser of any user who views the affected post.	6.8	More Details
CVE-2026-54483	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper neutralization of special elements used in an OS command ('OS command Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution.	6.7	More Details
CVE-2026-20462	In Telephony, there is a possible memory corruption due to a heap buffer overflow. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11006447; Issue ID: MSV-7871.	6.7	More Details
CVE-2026-20463	In Modem, there is a possible escalation of privilege due to a permissions bypass. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: MOLY01716533; Issue ID: MSV-6309.	6.7	More Details
CVE-2026-49813	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper neutralization of special elements used in an OS command ('OS command Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution.	6.7	More Details

CVE-2025-59617	Memory Corruption when processing multiple IOCTL calls with the same buffer file descriptor input.	6.6	More Details
CVE-2025-59615	Memory Corruption when invoking device input/output control operations for mapping and unmapping persistent memory buffers due to improper synchronization.	6.6	More Details
CVE-2025-59616	Memory Corruption when processing multiple IOCTL calls with the same buffer file descriptor input due to accessing already freed memory.	6.6	More Details
CVE-2026-56151	Improper Input Validation (CWE-20) in Kibana can lead to a denial of service via Input Data Manipulation (CAPEC-153). An authenticated user can submit a specially crafted Fleet policy input that is not correctly validated, which can render Fleet agent, server, and policy management functionality unavailable.	6.5	More Details
CVE-2026-49097	Improper Input Validation, Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in Apache Camel IRC component. The camel-irc producer chooses the destination of an outgoing IRC message from the irc.sendTo Exchange header (the constant IrcConstants.IRC_SEND_TO, value irc.sendTo); when that header is present it overrides the channel list configured on the endpoint, and the message is sent only to the specified destination. This and the component's other control headers (irc.target, irc.messageType, irc.user.*, irc.num, irc.value) used plain, non-Camel-prefixed values. Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that bridges an HTTP consumer (for example platform-http) into an irc: producer, any HTTP client could therefore set the irc.sendTo header and redirect a message that the route intended for a configured channel to an arbitrary IRC channel or user - exfiltrating the message content to an attacker-chosen nickname, leaking it into a public channel, or delivering messages that appear to come from the bot. No credentials are required when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that set IRC headers via the raw header names must use the CamelIrc* names (for example CamelIrcSendTo) instead of the old irc.* values. For deployments that cannot upgrade immediately, strip the irc.* headers from any untrusted ingress before the irc: producer (for example removeHeaders('irc.*') at the start of the route), and set the IRC destination from a trusted source.	6.5	More Details
CVE-2026-49086	Improper Input Validation, Unintended Proxy or Intermediary ('Confused Deputy') vulnerability in Apache Camel DAPR component. The camel-dapr Dapr Pub/Sub consumer (DaprPubSubConsumer) copied two fields from each inbound CloudEvent - its Pub/Sub component name and its topic - into the CamelDaprPubSubName and CamelDaprTopic Exchange headers. These two headers are producer-direction routing headers: when the route republishes through a Dapr producer, DaprConfigurationOptionsProxy reads them back and prefers them over the destination configured on the endpoint. As a result, in a route that consumes from one Dapr Pub/Sub topic and republishes to another (for example from('dapr-pubsub:p:t').to('dapr-pubsub:p:other')), an actor able to publish a message to the subscribed topic could set the CloudEvent's pub/sub-name and topic to values of their choosing and cause the re-published message to be delivered to an arbitrary Dapr Pub/Sub component and topic instead of the configured destination - redirecting or exfiltrating the message and bypassing the route's intended routing and any topic-level access controls in the underlying broker. Exploitation requires the ability to publish to the topic the route subscribes to; no other authentication or user interaction is needed. This issue affects Apache Camel: from 4.12.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. For deployments that cannot upgrade immediately, remove the CamelDaprPubSubName and CamelDaprTopic headers from the Exchange between the Dapr consumer and any Dapr producer in the route (for example removeHeaders('CamelDaprPubSubName', 'CamelDaprTopic')), and restrict who can publish to the subscribed Dapr Pub/Sub topic so that only trusted producers can send to it.	6.5	More Details
CVE-2026-8458	libcurl might in some circumstances reuse the wrong connection when asked to do Negotiate-authenticated ones, even when they are set to use different 'services'. libcurl features a pool of recent connections so that subsequent requests can reuse an existing connection to avoid overhead. When reusing a connection a range of criteria must be met. Due to a logical error in the code, a request that was issued by an application could wrongfully reuse an existing connection to the same server that was authenticated using different services.	6.5	More Details
CVE-2026-48828	The Bulk Variables API in Apache Airflow called the redactor without passing the variable's key, so the key-based `should_hide_value_for_key` check (which triggers on secret-suffixed key names like `*_password` / `*_token` / `*_secret`) could not fire for JSON-decodable variable values. An authenticated UI/API user with bulk Variable read permission could retrieve plaintext values from JSON variables whose key would otherwise trigger redaction. Affects deployments that store sensitive values in JSON-typed Airflow Variables under secret-suffixed key names. Users are advised to upgrade to `apache-airflow` 3.3.0 or later (the fix landed on	6.5	More Details

	`main` after 3.2.2; no 3.2.x backport).		
CVE-2026-56150	Allocation of Resources Without Limits or Throttling (CWE-770) in Fleet Server can lead to a denial of service via Excessive Allocation (CAPEC-130). An attacker can submit a specially crafted request to an upload endpoint that causes excessive memory consumption, which may render Fleet Server unavailable.	6.5	More Details
CVE-2026-34050	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the Settings/Updates Livewire component does not check isInstanceAdmin in its mount method, allowing non-admin users to access the Updates settings page and potentially modify auto-update settings or trigger update checks. This issue is fixed in version 4.0.0-beta.471.	6.5	More Details
CVE-2026-56148	Uncontrolled Recursion (CWE-674) in Elasticsearch can lead to a denial of service via Excessive Allocation (CAPEC-130). An authenticated user can submit a specially crafted query that causes excessive resource consumption while the request is processed, which may render the affected node unavailable.	6.5	More Details
CVE-2026-57987	Server-side request forgery (ssrf) in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2026-26355	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper neutralization of special Elements used in an OS command ('OS command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to command execution.	6.5	More Details
CVE-2026-32718	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.466, mutating API validation endpoints are guarded by read ability, allowing read-scoped API tokens to perform state-changing operations such as validating cloud tokens and servers. This issue is fixed in version 4.0.0-beta.466.	6.5	More Details
CVE-2026-49087	Allocation of Resources Without Limits or Throttling (CWE-770) in Kibana can lead to a denial of service via Excessive Allocation (CAPEC-130). An authenticated user can submit a specially crafted bulk deletion request that causes excessive resource consumption, which may render Kibana unavailable.	6.5	More Details
CVE-2026-55490	OpenWrt is a Linux operating system targeting embedded devices. Before v25.12.5, an integer underflow in handle_send_a() of the Emergency Access Daemon allows any unauthenticated attacker on the local network to crash the daemon by sending a single crafted UDP packet. The message length underflows before a bounds check and is then passed to memcpy as a very large size. This issue is fixed v25.12.5.	6.5	More Details
CVE-2026-55646	vLLM is an inference and serving engine for large language models. From 0.22.0 to 0.23.0, the /v1/audio/transcriptions and /v1/audio/translations routes call request.file.read() to fully materialize an uploaded audio file into memory before vLLM checks the documented VLLM_MAX_AUDIO_CLIP_FILESIZE_MB compressed upload size limit (default 25 MB) later in the speech-to-text preprocessing step, so an API caller who can reach those routes can submit an oversized multipart upload and cause vLLM to allocate memory proportional to the uploaded file size before the request is rejected as too large, creating memory pressure or terminating the process depending on deployment resource limits. This issue is fixed in version 0.24.0.	6.5	More Details
CVE-2026-41899	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, POST /api/feedback has no authentication, no rate limiting, and no input validation, allowing arbitrary content to be forwarded directly to a Discord webhook and enabling spam, content injection, and webhook abuse. This issue is fixed in version 4.0.0-beta.474.	6.5	More Details
CVE-2026-14898	The OpenAI Codex desktop app for macOS rendered remote images from Markdown in model responses. An attacker who could place an indirect prompt injection in content processed by Codex, such as a connected-tool result or another untrusted source, could induce the model to construct a remote image URL containing sensitive data. The app automatically fetched that URL when rendering the response, sending the embedded data to an attacker-controlled server without a separate user click. Successful exploitation could exfiltrate secrets and other information accessible in the Codex session, including API keys, source code, and data returned by connected tools. No direct integrity or availability impact was demonstrated, and there is no known exploitation in the wild.	6.5	More Details
CVE-2026-14324	RAOP module accepts unbounded Content-Length values and does not check the pw_array_add() return.	6.5	More Details
CVE-2026-13454	The MotoPress Appointment Booking plugin for WordPress is vulnerable to generic SQL Injection via the 's' parameter in all versions up to, and including, 2.4.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with custom-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires the mpa_appointment_employee custom role, meaning any user assigned this role can perform the attack.	6.5	More Details

CVE-2026-5135	A flaw was found in Foreman. This broken access control vulnerability allows an authenticated user with host-edit permissions to retarget an existing lookup value override to a different host. This is achieved by modifying the match field through nested host attributes, effectively bypassing authorisation checks. The consequence is the potential for unauthorised modification of managed host configurations across different organisational and location boundaries.	6.5	More Details
CVE-2026-46463	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an integer overflow or wraparound vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to denial of service.	6.5	More Details
CVE-2026-56646	Exposure of sensitive information to an unauthorized actor in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2026-53909	MCO does not correctly validate types of uploaded files. File upload validation functionality relies only on client-side checks, which can be bypassed. An authorized, low-privileged attacker can upload files with arbitrary types to the server. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 25.3.3.1 but may also affect other versions.	6.5	More Details
CVE-2026-55078	Coder allows organizations to provision remote development environments via Terraform. Starting in version 2.17.0 and prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, `POST /api/v2/files` converts zip uploads to tar in memory via `CreateTarFromZip`, which enforced a per-entry size limit but no aggregate limit on total decompressed output, writing to an unbounded in-memory buffer. Exploitation requires authenticated file-upload access and the impact is limited to availability (denial of service). The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 adds a metadata preflight check that sums projected entry sizes and a streaming writer that enforces the aggregate limit during decompression. As a workaround, restrict file-upload permissions to trusted users or place a reverse proxy with request-body size limits in front of `coderd`.	6.5	More Details
CVE-2026-5142	A flaw was found in foreman. Authenticated users with 'view_keypairs' permission can bypass taxonomy scoping, allowing them to download private SSH (Secure Shell) keys from other organizations by directly querying key pair IDs. This vulnerability leads to cross-tenant data exposure in multi-tenant deployments, potentially compromising sensitive information.	6.5	More Details
CVE-2026-58266	Anki is a program for creating and reviewing flashcards. Prior to 25.09.4, Anki's webview-based pages communicate with the Rust backend using an internal localhost API, and user scripts included via iframes in the editor can access this API despite protections intended to block reviewer and editor scripts. A malicious imported card package with an embedded iframe can use exposed API methods such as getImageForOcclusion to read arbitrary files accessible to the Anki process and exfiltrate them over the network. This issue is fixed in version 25.09.4.	6.5	More Details
CVE-2026-14258	A flaw was found in dhcpcd's IPv6 Neighbor Discovery Router Advertisement processing. A specially crafted IPv6 Router Advertisement containing a zero-length Neighbor Discovery option can bypass validation during packet storage and later be reparsed without adequate validation, causing the parser to enter a non-advancing loop. Successful exploitation may result in excessive CPU consumption, leading to a denial of service.	6.5	More Details
CVE-2026-45489	Microsoft Edge (Chromium-based) Spoofing Vulnerability	6.5	More Details
CVE-2026-55514	vLLM is a library for LLM inference and serving. From 0.12.0 to before 0.24.0, sending a pure prompt embeds payload in a /v1/completions request with a model using M-RoPE causes EngineCore to fail an assertion and fatally crash, shutting down the entire server application. Any remote user who is authorized to make a /v1/completions request can make such a request and induce a crash. This issue is fixed in version 0.24.0.	6.5	More Details
CVE-2026-14029	The Groundhogg — CRM, Newsletters, and Marketing Automation plugin for WordPress is vulnerable to generic SQL Injection via the 'select' parameter in all versions up to, and including, 4.5.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with custom-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires the attacker to hold a Groundhogg custom role with the view_contacts capability, which is granted by default to several built-in Groundhogg roles above the base subscriber level.	6.5	More Details
CVE-2026-48892	The Config API in Apache Airflow surfaced per-key secrets-backend overrides (environment variables like `AIRFLOW__SECRETS__BACKEND_KWARG__SECRET_ID` and `AIRFLOW__WORKERS__SECRETS_BACKEND_KWARG__SECRET_ID`) as synthetic config options whose option names were not in `sensitive_config_values`, so the masker did not redact them. An authenticated UI/API user with Config read permission could retrieve plaintext secrets-backend credentials (Vault `role_id` / `secret_id`, etc.) from the Config API output. Affects deployments that configure secrets backends via per-key environment overrides. Users are advised to upgrade to `apache-airflow` 3.3.0 or later.	6.5	More Details

CVE-2026-49090	Uncontrolled Resource Consumption (CWE-400) in Elasticsearch can lead to a denial of service via Excessive Allocation (CAPEC-130). An authenticated user can submit a specially crafted bulk request that causes sustained high CPU consumption, which can render the affected node unable to process requests.	6.5	More Details
CVE-2026-11988	The LearnPress – WordPress LMS Plugin for Create and Sell Online Courses plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.3.9.1 via the 'userId' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to view the course enrollment progress and completion data belonging to any instructor or administrator account on the site. This IDOR does not apply when the target user is a regular subscriber, as the guard correctly blocks cross-subscriber access; exploitation is limited to cases where the victim user holds the LP_TEACHER_ROLE or administrator role.	6.5	More Details
CVE-2026-12090	The Taskbuilder – Project Management & Task Management Tool With Kanban Board plugin for WordPress is vulnerable to generic SQL Injection via the 'wppm_proj_filter' parameter in all versions up to, and including, 5.0.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. No nonce verification is performed on the wp_ajax_wppm_view_project_tasks handler, meaning any authenticated session — including subscriber-level — can reach the vulnerable code path without any additional preconditions.	6.5	More Details
CVE-2026-57764	Contributor Cross Site Scripting (XSS) in Surbma | Yoast SEO Breadcrumb Shortcode <= 1.2 versions.	6.5	More Details
CVE-2026-57763	Contributor Cross Site Scripting (XSS) in Structured Content <= 1.7.0 versions.	6.5	More Details
CVE-2026-12110	The Taskbuilder – Project Management & Task Management Tool With Kanban Board plugin for WordPress is vulnerable to generic SQL Injection via the 'task_search' parameter in all versions up to, and including, 5.0.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The wppm_get_task_list AJAX handler performs no capability check and no nonce verification, meaning any authenticated user including those with Subscriber-level access can invoke it directly.	6.5	More Details
CVE-2026-57755	Contributor Cross Site Scripting (XSS) in Mosaic Gallery – Advanced Gallery <= 1.2.0 versions.	6.5	More Details
CVE-2026-57754	Contributor Cross Site Scripting (XSS) in Livemesh Addons for WPBakery Page Builder <= 3.9.4 versions.	6.5	More Details
CVE-2026-14421	Uninitialized Use in Dawn in Google Chrome on ChromeOS prior to 150.0.7871.46 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2025-12799	A flaw was found in Jastow. Jastow is vulnerable to Cross-Site Scripting (XSS) attack. If using a set of combined configuration to allow unescaped characters in URL with embedded Undertow and Jastow, a server might be vulnerable to improper input handling.	6.5	More Details
CVE-2026-14904	AWS Research and Engineering Studio (RES) is an open-source solution that enables researchers and engineers to create and manage secure virtual desktops and computing resources on AWS. Improper link resolution before file access issue (CWE-59) in the Auth.GetUserPrivateKey API. An authenticated remote user could read arbitrary files on the cluster-manager EC2 instance by replacing their SSH private key file (~/.ssh/id_rsa) with a symbolic link targeting any file on the host. Because the cluster-manager process runs as root, any file readable by root is exposed, including other users' SSH private keys and application configuration secrets. It's recommended to upgrade to RES version 2026.06.	6.5	More Details
CVE-2026-14714	A weakness has been identified in zhayujie chatgpt-on-wechat CowAgent 2.1.0. This issue affects the function verify_server of the file channel/wechatmp/common.py of the component wx Endpoint. This manipulation of the argument wechatmp_token causes missing authentication. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 2.1.1 is capable of addressing this issue. Patch name: 3d7c68bac6ee74fad63f43cf99e45c62e202ed55. It is suggested to upgrade the affected component. The project confirms: "We've added an explicit non-empty check for wechatmp_token in verify_server() so that the /wx endpoint now fails closed with 403 Forbidden whenever the token is missing or left at the default empty value, instead of relying on a signature check that silently degenerates to a predictable hash."	6.5	More Details
CVE-			

2026-57747	Unauthenticated Cross Site Request Forgery (CSRF) in Booked <= 3.0.0 versions.	6.5	More Details
CVE-2026-57731	Contributor Broken Access Control in Flatsome <= 3.20.5 versions.	6.5	More Details
CVE-2026-57684	Contributor Cross Site Scripting (XSS) in TheFox <= 3.9.70 versions.	6.5	More Details
CVE-2026-57680	Unauthenticated Insecure Direct Object References (IDOR) in Kirki <= 6.0.11 versions.	6.5	More Details
CVE-2026-57669	Subscriber Broken Access Control in Advanced Contact form 7 DB <= 2.0.9 versions.	6.5	More Details
CVE-2026-57355	Subscriber Broken Access Control in Classified Listing <= 5.4.2 versions.	6.5	More Details
CVE-2026-57354	Subscriber Cross Site Scripting (XSS) in JetReviews <= 3.0.0.1 versions.	6.5	More Details
CVE-2026-57353	Subscriber Broken Access Control in Link Whisper Premium <= 2.9.0 versions.	6.5	More Details
CVE-2026-57347	Subscriber Sensitive Data Exposure in Hotel Booking Lite <= 6.0.3 versions.	6.5	More Details
CVE-2026-57342	Subscriber Cross Site Scripting (XSS) in ShortPixel Adaptive Images <= 3.11.3 versions.	6.5	More Details
CVE-2026-44877	An unauthenticated remote disclosure vulnerability has been identified in HPE Networking Instant On 1830, 1930, and 1960 Switches. Successful exploitation of this vulnerability could allow an unauthenticated remote threat actor to access sensitive cryptographic secrets on a vulnerable system.	6.5	More Details
CVE-2026-49779	Customer Path Traversal in Tax Exempt for WooCommerce <= 1.9.3 versions.	6.5	More Details
CVE-2026-27433	Unauthenticated Broken Access Control in Motors <= 5.6.80 versions.	6.5	More Details
CVE-2026-53902	MCO does not properly enforce authorization checks in the /customer/servlet/mco/webapi/profile-sections/group-membership endpoint. An authenticated user can modify their group membership without proper authorization checks, allowing privilege escalation. An attacker can add themselves to arbitrary groups by supplying a valid group ID, which can be obtained via other application functionalities (e.g. /customer/servlet/mco/webapi/group/picker/groups), provided he has necessary permissions, or potentially inferred through brute-force techniques. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 25.3.3.1 but may also affect other versions.	6.5	More Details
CVE-2026-11965	The User Registration & Membership WordPress plugin before 5.2.0 does not enforce payment completion before activating a paid membership subscription, allowing unauthenticated users (after self-registering an account through the open registration flow) to obtain an active subscription on any paid plan without paying and access the gated content.	6.5	More Details
CVE-2025-69132	Subscriber Sensitive Data Exposure in Corpkit <= 1.0.5 versions.	6.5	More Details
CVE-2026-58523	Improper access control in Microsoft Edge for Android allows an unauthorized attacker to bypass a security feature over a network.	6.5	More Details

CVE-2026-14408	Uninitialized Use in Dawn in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-55434	Coder allows organizations to provision remote development environments via Terraform. Starting in version 2.33.0 and prior to versions 2.33.8 and 2.34.2, AI Bridge provider handlers read request bodies with `io.ReadAll` without a maximum size so an authenticated user with AI Bridge access could send an arbitrarily large body and exhaust memory. Exploitation requires authenticated access to the AI Bridge endpoints and the impact is limited to availability (denial of service). Versions 2.33.8 and 2.34.2 patch the issue. No known workarounds are available.	6.5	More Details
CVE-2026-54164	API Platform Core is a system to create hypermedia-driven REST and GraphQL APIs. In versions prior to 4.1.30, 4.2.26 and 4.3.12, the serializer's AbstractItemNormalizer does not validate the resource type returned when resolving relation IRIs, allowing type confusion where a resource of an unintended type can be silently assigned to a relation property. An attacker who can submit write requests (POST/PUT/PATCH) to an API Platform endpoint with writable relations can supply a relation IRI pointing to a resource of a different type than the relation's declared class. Because getResourceFromIri() does not pass an $operation to IriConverter::getResourceFromIri(), the is_a type guard at IriConverter.php:86 is skipped. For untyped relation properties (legacy @var-only style), the wrong-typed object is silently assigned, corrupting invariants and potentially feeding downstream logic that assumes the declared type (CWE-843). For typed properties (modern PHP 8.x), the substitution is blocked by Symfony's PropertyAccessor with an InvalidTypeException. This issue has been fixed in versions 4.1.30, 4.2.26 and 4.3.12.	6.5	More Details
CVE-2026-51946	SQL Injection vulnerability in GoAdminGroup GoAdmin (last release v1.2.26) allows a remote attacker to execute arbitrary code and obtain sensitive information via the the __sort_type URL parameter on all /admin/info/{table} endpoints	6.5	More Details
CVE-2026-57737	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Averta LTD Shortcodes and extra features for Phlox theme allows DOM-Based XSS. This issue affects Shortcodes and extra features for Phlox theme: from n/a through 2.17.16.	6.5	More Details
CVE-2026-49296	Before apache-airflow 3.3.0, a user authorized to read one Dag could disclose the source of other Dags co-located in the same source file. `GET /api/v2/dagSources/{dag_id}` — and the equivalent Dag-source view in the UI — returned the entire source file without redacting Dags the caller was not authorized to read, bypassing per-DAG read authorization. Deployments that co-locate multiple Dags in a single file and rely on per-DAG access control to limit source visibility are affected; single-Dag-per-file deployments are not. Upgrade to apache-airflow 3.3.0 or later.	6.5	More Details
CVE-2026-14792	A security vulnerability has been detected in Formbricks 5.0.0. This impacts an unknown function of the file apps/web/modules/survey/link/actions.ts of the component Survey Handler. The manipulation leads to improper access controls. Remote exploitation of the attack is possible. Upgrading to version 5.1.0-rc.1 will fix this issue. The identifier of the patch is af6023b5ac3b030ffcea24fac799f76f3e3512c6. You should upgrade the affected component.	6.5	More Details
CVE-2026-52188	Buffer Overflow vulnerability in UTT nv518G nv518GV3v3.2.7-210919-161313 allows a remote attacker to cause a denial of service via the gohead//sub_497498 component	6.5	More Details
CVE-2026-38142	An unauthenticated command injection vulnerability in the /goform/fast_setting_internet_set endpoint of Tenda AC18 v15.03.05.05 allows attackers to execute arbitrary commands via a crafted payload injected into the mac parameter.	6.5	More Details
CVE-2026-14803	Mojo::JSON versions before 9.47 for Perl allow memory exhaustion via unbounded recursion in the pure-Perl decoder. The pure-Perl decode path (`_decode_value` dispatching to `_decode_array` and `_decode_object`) recurses with no depth limit, so a small deeply nested JSON document can consume excessive memory. This path is the default when Cpanel::JSON::XS is not installed or `MOJO_NO_JSON_XS=1` is set; the Cpanel::JSON::XS fast path is not affected. Any caller that decodes an untrusted JSON body, for example `Mojo::Message::json` reached through `$c->req->json`, can exhaust process memory and cause denial of service.	6.5	More Details
CVE-2026-53466	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-51 and 7.1.2-26, an integer overflow in the XCF decoder can result in an out of bounds read when a crafted image is read, potentially resulting in a crash. This issue has been fixed in versions 6.9.13-51 and 7.1.2-26.	6.5	More Details
CVE-2026-53489	containerd is an open-source container runtime. Versions prior to 2.3.2, 2.2.5 and 2.1.9 contain a bug where the CRI plugin restores container.log from a checkpoint image without validating a symlinked path. This could result in reading an arbitrary file on the host via kubectl logs. This issue has been fixed in versions 2.3.2, 2.2.5 and 2.1.9.	6.5	More Details
CVE-	LobeChat through 2.2.9 contains a broken access control vulnerability in the retrieval-augmented-generation semantic search functionality that allows authenticated attackers to access other users' data by exploiting		More

2026-59098	missing user-identifier predicates in the chunk model semanticSearch method. Attackers can supply arbitrary victim file or knowledge-base identifiers through the chunk retrieval and chat knowledge-base paths to retrieve text content, file names, and metadata belonging to other users.	6.5	Details
CVE-2026-57963	An attacker who can send HTML chat messages (via Matrix or XMPP) can inject arbitrary styled content, phishing links, and CSS that manipulates the chat UI. This vulnerability was fixed in Thunderbird 152.0.1 and Thunderbird 140.12.1.	6.5	More Details
CVE-2026-58451	Horde IMP before 7.0.1 contains a path traversal vulnerability in lib/Compose.php that allows authenticated attackers to read arbitrary files from the server filesystem by embedding traversal sequences after a CKEditor path prefix in img src URLs. Attackers can bypass the stripos() prefix validation by appending sequences such as traversal segments after the matching prefix, causing file_get_contents() to read sensitive files whose contents are then exfiltrated as MIME parts in outgoing email; unauthenticated exploitation is also achievable via CSRF against an active authenticated session.	6.5	More Details
CVE-2026-58578	LobeChat before version 2.2.10-canary.15 contains a regular expression denial of service (ReDoS) vulnerability that allows authenticated attackers to block the Node.js event loop by supplying a catastrophic-backtracking pattern in a GitHub repository URL path during skill import. Attackers can craft a malicious basePath value containing unescaped regex metacharacters such as catastrophic-backtracking patterns, which are injected into a dynamically constructed regular expression in the findSkillMd function and executed synchronously against archive entries, denying service to all concurrent users for tens of seconds per request.	6.5	More Details
CVE-2026-58418	SSRF via HTTP Redirect in Repository Migration	6.5	More Details
CVE-2026-54261	Wagtail is an open source content management system built on Django. In versions prior to 7.0.8, 7.3.3 and 7.4.2, due to a missing permission check on the image preview endpoint, a user with access to the Wagtail admin can preview any image. The existing data of the image object itself is not exposed. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. This issue has been fixed in versions 7.0.8, 7.3.3, and 7.4.2.	6.5	More Details
CVE-2026-54704	OpenTelemetry Java Instrumentation provides OpenTelemetry auto-instrumentation and instrumentation libraries for Java. In versions prior to 2.28.0, the JDBC auto-instrumentation may fail to sanitize passwords in SQL CONNECT statements when the password is double-quoted. As a result, clear-text database passwords can be added to trace span attributes and exported to observability backends. This issue has been fixed in version 2.28.0.	6.5	More Details
CVE-2026-45796	Coder allows organizations to provision remote development environments via Terraform. Versions prior tp 2.24.5, 2.29.13, 2.30.8, 2.31.12, 2.32.2, and 2.33.3 are vulnerable to unauthenticated semi-blind Server-Side Request Forgery (SSRF) via the Azure instance identity endpoint (`POST /api/v2/workspaceagents/azure-instance-identity`). An external attacker can force the Coder server to issue HTTP GET requests to arbitrary internal or external hosts by submitting a crafted PKCS#7 signature. The server does not return the target's response body, but error messages in the API response reveal whether the target is reachable and what type of failure occurred. Versions 2.24.5, 2.29.13, 2.30.8, 2.31.12, 2.32.2, and 2.33.3 patch the issue. As a workaround, if the Azure identity-auth mechanism is not being used then restrict access to the corresponding endpoint (`/api/v2/workspaceagents/azure-instance-identity`) using ingress firewall and/or proxy ACLs.	6.5	More Details
CVE-2026-9145	The Database for Contact Form 7, WPforms, Elementor forms plugin for WordPress is vulnerable to Arbitrary File Copy via the create_entry_el() function in versions up to, and including, 1.5.1. The function reads raw_value from Elementor Pro's Form_Record object for upload-type fields and passes it directly to PHP's copy() without validating that the value corresponds to a legitimately uploaded file — when no file is present in $_FILES, raw_value reflects the attacker-controlled POST string. copy() accepts both local filesystem paths and URL sources, so the attacker can target any file readable by the PHP process or supply an attacker-controlled remote URL. Elementor Pro is a prerequisite for triggering the code path (it owns the elementor_pro/forms/new_record hook and populates the Form_Record object), but the bug itself is entirely in Contact Form Entries' handler. This could allow unauthenticated attackers to disclose arbitrary files on the affected site's server. The file is copied to a directory unknown to the attacker; the hashed directory name provides defense-in-depth but is generated from non-cryptographic sources (uniqid() + rand()) and should not be relied upon as the primary mitigation.	6.5	More Details
CVE-2026-49487	In Apache Airflow before 3.3.0, the REST API task-instance detail and list endpoints returned a deferred task's trigger kwargs without masking. When a deferred operator passed a secret (for example a provider API key) into its trigger, any authenticated user with DAG-scoped task-instance read access for that DAG could read that secret in clear text while the task was deferred. Users should upgrade to apache-airflow 3.3.0 or later, which masks sensitive values in trigger kwargs returned by the API.	6.5	More Details
CVE-2026-14384	Out of bounds read in ANGLE in Google Chrome on Windows prior to 150.0.7871.46 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details

CVE-2026-14386	Out of bounds read in ANGLE in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-14388	Out of bounds read in ANGLE in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-14396	Out of bounds read in ANGLE in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-14399	Uninitialized Use in Dawn in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-14402	Uninitialized Use in ANGLE in Google Chrome on Windows prior to 150.0.7871.46 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-14404	Inappropriate implementation in PDFium in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to perform UI spoofing via a crafted PDF file. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-14381	Incorrect security UI in WebAppInstalls in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-12154	The Reviews Widgets for Google, Yelp & TripAdvisor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'page_id' shortcode attribute of the [fbrev] shortcode in versions up to and including 2.7.3. This is due to insufficient input sanitization and output escaping in the Feed_Shortcode::fbrev() method, which passes the raw shortcode attribute through Feed_Old::get_feed() into the View::render() method, where it is echoed directly into the data-id HTML attribute without esc_attr(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-11328	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the post title parameter in all versions up to, and including, 2.7.9.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-9756	The GenerateBlocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Headline Block 'linkMetaFieldType' Dynamic Link Attribute in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. A contributor-level attacker can store a JavaScript payload in their own profile description (allowlisted by get_safe_user_meta_keys()) and prepend 'javascript:' via the linkMetaFieldType attribute, creating a fully attacker-controlled href that executes when any user, including an administrator, clicks the rendered headline link.	6.4	More Details
CVE-2026-9626	The JSON API User plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'content' parameter of the post_comment API endpoint in versions up to, and including, 4.1.0 This is due to insufficient input sanitization in the post_comment() function, which passes the attacker-controlled comment_content value directly to wp_insert_comment() without applying any HTML sanitization, and additionally allows the caller to set comment_approved=1 to self-approve the comment and bypass moderation. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-13252	The RSS Aggregator by Feedzy – Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'aspectRatio' Attribute in all versions up to, and including, 5.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8489	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'about_me' parameter in all versions up to, and including, 2.11.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
	The CM Business Directory – Optimise and showcase local business plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Business Address Meta Fields in all versions up to, and including, 1.5.7 due to		

CVE-2026-8892	insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Because the malicious payload is stored in post meta rather than post_content, WordPress's unfiltered_html capability restriction does not apply, meaning contributors who lack that capability can still inject executable HTML via the address meta fields such as cmbd_address, cmbd_cityTown, cmbd_stateCounty, cmbd_postalcode, cmbd_region, and cmbd_country.	6.4	More Details
CVE-2026-10089	The Insert Pages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via post custom field keys (meta key names) in all versions up to, and including, 3.11.4. This is due to insufficient output escaping in the the_meta() function: while the custom field VALUE is sanitized with wp_kses_post(), the custom field KEY ($key) is interpolated into the rendered HTML (lines 1786-1791) and echoed (line 1806) without any escaping when an inserted page is rendered with the [insert page='ID' display='all'] shortcode. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-13733	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'no_data_msg' Shortcode Attribute in all versions up to, and including, 3.3.60 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Although wp_kses_post is applied to post content on save, it only strips HTML tokens and does not neutralize C-style escape sequences embedded within shortcode attribute values, meaning contributors can craft a payload that survives the kses filter and is silently reconstructed into a raw script tag at render time.	6.4	More Details
CVE-2026-11380	The JetWidgets For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to and including 1.0.21. This is due to insufficient output escaping and missing server-side validation of the Animated Box widget's animation_effect setting before it is rendered inside an HTML class attribute. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-57681	Subscriber Server Side Request Forgery (SSRF) in GeoDirectory <= 2.8.161 versions.	6.4	More Details
CVE-2026-9107	The Kali Forms — Contact Form & Drag-and-Drop Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'meta[kaliforms_field_components]' parameter in all versions up to, and including, 2.4.13 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-13246	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'block_id' (and other) shortcode attributes of the 'givewp_campaign_comments' shortcode in versions up to, and including, 4.16.0. This is due to insufficient input sanitization and output escaping on user supplied attributes in CampaignCommentsShortcode::parseAttributes() and BlockRenderController::render(), where the blockId value is interpolated directly into a single-quoted HTML attribute without esc_attr(). This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-13704	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'sequoia[introduction][image]' parameter in all versions up to, and including, 4.16.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Give Worker-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-13443	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Lesson Attachment Title in all versions up to, and including, 3.9.13 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-2387	The Event Organiser plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 3.12.9. This is due to the 'eo_events' shortcode accepting attacker-controlled 'no_events' content and rendering it in event list templates without output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5220	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in DivvyDrive Information Technologies Inc. DivvyDrive allows Stored XSS. This issue affects DivvyDrive: from 4.8.2.23 before v.4.8.3.1.	6.4	More Details
	The LearnPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class_wrapper_form' shortcode attribute in versions up to, and including, 4.4.0. This is due to insufficient input sanitization and		

CVE-2026-12732	output escaping in the FilterCourseTemplate::sections() method at line 98, where the attacker-controlled attribute is inserted into an HTML class attribute via sprintf('<form class="%s">', $class_wrapper_form) without esc_attr() escaping. The FilterCourseShortcode::render() handler does not apply shortcode_atts() filtering, so raw user attributes flow directly through do_action('learn-press/filter-courses/layout', $data) into the template. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-12734	The weDocs: AI Powered Knowledge Base, Docs, Documentation, Wiki & AI Chatbot plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'connectorWidth' Block Attribute in all versions up to, and including, 2.3.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-12731	The weDocs: AI Powered Knowledge Base, Docs, Documentation, Wiki & AI Chatbot plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'sectionTitleTag' and 'articleTitleTag' Block Attributes in all versions up to, and including, 2.3.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-10095	The WP Photo Album Plus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'subtext' parameter in all versions up to, and including, 9.1.13.005 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. A contributor-level attacker can embed the malicious [photo] shortcode in a post submitted for review, causing the stored payload to execute when an administrator or any other user views the post.	6.4	More Details
CVE-2026-4804	The Zakra theme for WordPress is vulnerable to Stored Cross-Site Scripting via post meta values in all versions up to, and including, 4.2.0. This is due to the theme registering three post meta fields (zakra_menu_item_color, zakra_menu_item_hover_color, and zakra_menu_item_active_color) with 'show_in_rest' => true and 'auth_callback' => '__return_true', but without any sanitize_callback parameter in the register_post_meta() calls. While the classic editor save path applies sanitize_hex_color() sanitization, the REST API path completely bypasses this protection. The unsanitized meta values are then retrieved via get_post_meta() and concatenated directly into CSS strings that are output through wp_add_inline_style() without any escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the injected page.	6.4	More Details
CVE-2026-12135	The FV Flowplayer Video Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'video_player' shortcode 'align' attribute in all versions up to, and including, 7.5.51.7212 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8351	The RTMKit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Advanced Heading widget's 'Background Text' parameter in versions up to, and including, 2.0.7 This is due to insufficient output escaping on the 'background_text_heading' setting in the render() function, which concatenates the value directly into an HTML attribute without applying esc_attr(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-14689	A security flaw has been discovered in CodeAstro Apartment Visitor Management System 1.0. The impacted element is an unknown function of the file /apartment-visitor/add-apartment.php. The manipulation of the argument apartmentno results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-14798	A vulnerability was identified in CodeAstro Apartment Visitor Management System 1.0. This issue affects some unknown processing of the file /apartment-visitor/visitor-entry.php. The manipulation of the argument visname leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-14784	A vulnerability was identified in vxcontrol PentAGI up to 2.1.0. This affects an unknown function of the file backend/pkg/docker/client.go of the component Docker API. The manipulation leads to sandbox issue. The attack may be initiated remotely. The pull request to fix this issue awaits acceptance.	6.3	More Details
CVE-2026-14694	A vulnerability has been found in SourceCodester Multi-Vendor Online Grocery Management System 1.0. Affected by this issue is the function cancel_order of the file classes/Master.php of the component POST Parameter Handler. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-14799	A security flaw has been discovered in CodeAstro Ecommerce Website 1.0. Impacted is an unknown function of the file /customer/my_account.php?my_wishlist. The manipulation of the argument delete_wishlist results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be	6.3	More Details

	used for attacks.		
CVE-2026-14797	A vulnerability was determined in CodeAstro Apartment Visitor Management System 1.0. This vulnerability affects unknown code of the file /apartment-visitor/edit-apartment.php. Executing a manipulation of the argument editid can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-14691	A security vulnerability has been detected in SourceCodester Multi-Vendor Online Grocery Management System 1.0. This impacts the function update_settings_info of the file classes/SystemSettings.php of the component Setting Handler. Such manipulation of the argument content[] leads to code injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-14659	A vulnerability has been found in itsourcecode Hospital Management System 1.0. Impacted is an unknown function of the file /patientappointment.php. Such manipulation of the argument patiente leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-14731	A weakness has been identified in itsourcecode Hospital Management System 1.0. This affects an unknown part of the file /patientreport.php. Executing a manipulation of the argument editid can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-14730	A security flaw has been discovered in itsourcecode Hospital Management System 1.0. Affected by this issue is some unknown functionality of the file /patientprofile.php. Performing a manipulation of the argument patientname results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-14725	A vulnerability was identified in SourceCodester Online Boat Reservation System 1.0. Affected by this vulnerability is an unknown functionality. Such manipulation leads to session expiration. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-14717	A vulnerability was detected in itsourcecode Hospital Management System 1.0. The affected element is an unknown function of the file /patientlogin.php. Performing a manipulation of the argument loginid results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	6.3	More Details
CVE-2026-14796	A vulnerability was found in CodeAstro Apartment Visitor Management System 1.0. This affects an unknown part of the file /apartment-visitor/report.php. Performing a manipulation of the argument fromdate results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-14706	A vulnerability was identified in code-projects Online Examination 1.0. This affects an unknown part of the file /update.php?q=addquiz of the component Quiz Creation Feature. The manipulation of the argument name/total/right/wrong/time/tag/desc leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-14604	A vulnerability was determined in Open Asset Import Library Assimp up to 6.0.4. Affected is the function Assimp::Exporter::ExportToBlob of the file code/AssetLib/Ply/PlyLoader.cpp of the component PLY Model Handler. This manipulation causes double free. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report.	6.3	More Details
CVE-2026-14658	A vulnerability was detected in code-projects Assessment Management 1.0. This vulnerability affects unknown code of the file /lecturer/marking-scheme.php. The manipulation of the argument smarksrange[] results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-14751	A weakness has been identified in mjperpinosa stumasy up to 327d1b0f2915ba79d7ef8ebb74553e987609d9be. The impacted element is the function Notes_controller::search_scratch_data of the file application/PHP/objects/notes/search_scratch_data.php. This manipulation of the argument field_name causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-54601	FastGPT is an open source AI knowledge base platform. From 4.14.17 to before 4.15.0-beta4, FastGPT allows an authenticated tenant user to call POST /api/core/dataset/collection/create/reTrainingCollection in a way that persists a server-owned datasetId value from another tenant. This creates mixed dataset objects and downstream dataset, collection, and training endpoints then make authorization decisions from inconsistent ownership anchors, allowing cross-tenant read, update, and delete access when mixed object ids are known. This issue is fixed in version 4.15.0-beta4.	6.3	More Details
	A vulnerability was identified in CodeAstro Apartment Visitor Management System 1.0. Affected by this issue		

CVE-2026-14766	is some unknown functionality of the file /apartment-visitor/search-result.php of the component POST Parameter Handler. The manipulation of the argument searchdata leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-14767	A security flaw has been discovered in CodeAstro Ecommerce Website 1.0. This affects an unknown part of the file /ecommerce-website-php/customer/confirm.php of the component POST Parameter Handler. The manipulation of the argument invoice_no results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-14698	A security flaw has been discovered in SourceCodester Syllabus-Aligned Learning Management and Examination System 1.0. Impacted is an unknown function of the file upload_files.php. Performing a manipulation results in unrestricted upload. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-14701	A vulnerability was detected in code-projects Internship Management System 1.0. This affects an unknown function of the file employer/details/change_password.php of the component Password Change Endpoint. The manipulation of the argument Current results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-14625	A security flaw has been discovered in NousResearch hermes-agent up to 0.15.2. The affected element is the function shell.exec of the file tui_gateway/server.py. The manipulation results in protection mechanism failure. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-14619	A flaw has been found in itsourcecode Hospital Management System 1.0. Affected by this issue is some unknown functionality of the file /medicine.php. This manipulation of the argument editid causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	6.3	More Details
CVE-2026-14638	A flaw has been found in itsourcecode Hospital Management System 1.0. This affects an unknown function of the file /patient.php. This manipulation of the argument editid causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-14639	A vulnerability has been found in CodeAstro Ecommerce Website 1.0. This impacts an unknown function of the file /ecommerce-website-php/customer/my_account.php?edit_account. Such manipulation of the argument c_name leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-14657	A flaw has been found in code-projects Assessment Management 1.0. This issue affects some unknown processing of the file /lecturer/marking-scheme.php of the component Database Query Handler. This manipulation of the argument squestions[] causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-14692	A vulnerability was detected in SourceCodester Multi-Vendor Online Grocery Management System 1.0/5.7.26. Affected is the function save_shop_type of the file classes/Master.php of the component POST Parameter Handler. Performing a manipulation results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-14703	A vulnerability has been found in itsourcecode Hospital Management System 1.0. Affected is an unknown function of the file /patientorder.php. Such manipulation of the argument editid leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-14773	A vulnerability was found in itsourcecode Hospital Management System 1.0. This affects an unknown function of the file /payment.php. The manipulation of the argument patientid results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-14774	A vulnerability was determined in itsourcecode Hospital Management System 1.0. This impacts an unknown function of the file /paymentdischarge.php. This manipulation of the argument patientid causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-14748	A flaw has been found in AIAnytime Awesome-MCP-Server up to a884bb51bcd99e08e14fd712c749d55d9d9a13ab. Affected by this issue is some unknown functionality of the file mcp-wiki/src/mcp_wiki/server.py of the component mcp-wiki/wiki-summary. This manipulation of the argument url causes server-side request forgery. The attack may be initiated remotely. The exploit has been published and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-13356	A malicious webpage could interrupt a pending navigation by enqueuing a synchronous JavaScript dialog, causing the browser UI to display the destination origin in the address bar while continuing to render attacker-controlled content. This vulnerability was fixed in Firefox for iOS 152.3.	6.3	More Details
CVE-	A vulnerability was identified in SourceCodester Onlne Examination & Learning Management System 1.0. Affected is an unknown function of the file /process_lesson.php. Such manipulation of the argument user_id		More

2026-14775	leads to unrestricted upload. The attack may be launched remotely. The exploit is publicly available and might be used. The name of the affected product appears to have a typo in it.	6.3	Details
CVE-2026-14776	A security flaw has been discovered in SourceCodester Onlne Examination & Learning Management System 1.0. Affected by this vulnerability is the function pathinfo of the file /upload_files.php of the component Filename Extension. Performing a manipulation results in unrestricted upload. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The name of the affected product appears to have a typo in it.	6.3	More Details
CVE-2026-14777	A weakness has been identified in SourceCodester Onlne Examination & Learning Management System 1.0. Affected by this issue is some unknown functionality of the file /announcements.php. Executing a manipulation can lead to unrestricted upload. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. The name of the affected product appears to have a typo in it.	6.3	More Details
CVE-2026-14795	A vulnerability has been found in CodeAstro Apartment Visitor Management System 1.0. Affected by this issue is some unknown functionality of the file /apartment-visitor/action-visitor.php. Such manipulation of the argument remark leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-14716	A security vulnerability has been detected in nextlevelbuilder GoClaw up to 3.13.0-beta.2. Impacted is the function MethodRouter.Handle of the file internal/gateway/router.go of the component WebSocket RPC Handler. Such manipulation leads to incorrect authorization. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report.	6.3	More Details
CVE-2026-36909	A NULL pointer dereference in the AP4_TkhdAtom::GetTrackId() function of Aleksoid1978 MPC-BE before commit 4341cb3 allows attackers to cause a Denial of Service (DoS) via a crafted MP4 file.	6.2	More Details
CVE-2026-58300	Absolute path traversal in Microsoft Edge for Android allows an unauthorized attacker to disclose information locally.	6.2	More Details
CVE-2026-58381	A flaw was found in GIMP's PSP file format parser. A double-free condition occurs in the read_layer_block() function when processing a specially crafted PSP file. This could allow an attacker to cause memory corruption, potentially leading to denial of service or arbitrary code execution.	6.1	More Details
CVE-2026-7380	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in Armiya Information Technologies Ltd. Co. Access Control System (GKS) allows XSS Targeting HTML Attributes. This issue affects Access Control System (GKS): before Version 2.	6.1	More Details
CVE-2025-71385	Netdata before 2.3.1 reflects the user-supplied love query parameter of the api/v2/ilove.svg and api/v3/ilove.svg endpoints verbatim into the generated SVG document (into a text element) without HTML or XML escaping, and serves the response with Content-Type image/svg+xml. An attacker can craft a URL such as /api/v2/ilove.svg?love=<script>...</script>; when a victim navigates to it the injected script executes in the victim browser in the origin of the Netdata instance (reflected cross-site scripting). These endpoints are registered with HTTP_ACL_NOCHECK and anonymous access and, because bearer-token protection is disabled by default, are reachable without authentication on a default Netdata agent. The issue was resolved by removing the ilove endpoint.	6.1	More Details
CVE-2026-4322	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Raera - Ankara Web Design and Digital Advertising Agency Destekz allows Reflected XSS. This issue affects Destekz: through 02062026. NOTE: The vendor was contacted and it was learned that the product is not supported.	6.1	More Details
CVE-2026-53878	An issue was discovered in Django 6.0 before 6.0.7 and 5.2 before 5.2.16. `DomainNameValidator` does not prohibit newlines in domain names (unless used via a form field, since `CharField` strips newlines). If an application uses values with newlines in an HTTP response, header injection can occur. Django itself is unaffected because `HttpResponse` prohibits newlines in HTTP headers. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Bence Nagy for reporting this issue.	6.1	More Details
CVE-2026-58291	Operation on a resource after expiration or release in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	6.1	More Details
CVE-2026-25779	Gitea versions up to and including 1.25.4 allow redirect bypasses through raw or percent-encoded backslashes in redirect_to values.	6.1	More Details
	The Wp Google Places Review Slider plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'place' parameter in versions up to, and including, 18.1. This is due to insufficient input sanitization and		

CVE-2026-13015	output escaping in admin/partials/googlecrawl_dfs.php, where the $_GET['place'] value is URL-decoded, stripslashes()'d, and echoed directly into an HTML value attribute with no esc_attr() call when the supplied place is not already a stored key in the wprev_google_crawls option. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a specially crafted link.	6.1	More Details
CVE-2026-12754	The VikBooking Hotel Booking Engine & PMS plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'layoutstyle' parameter in all versions up to, and including, 1.8.12 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. Exploitation requires the targeted page to render the [vikbooking view="roomslist"] shortcode, as the vulnerable layoutstyle parameter is only processed in that view context.	6.1	More Details
CVE-2026-59710	showdown contains a stored cross-site scripting vulnerability in the parseHeaders function of src/subParsers/makehtml/tables.js that fails to properly escape table header ID attributes. Attackers can inject arbitrary HTML and script-executing SVG elements through double-quote characters in markdown table headers, achieving stored XSS when untrusted markdown is rendered with the default github flavor configuration.	6.1	More Details
CVE-2026-59711	showdown contains a cross-site scripting vulnerability in metadata title handling that allows attackers to inject arbitrary HTML and JavaScript. When completeHTMLDocument option is enabled, unescaped less-than and greater-than characters in markdown frontmatter metadata are inserted directly into HTML title tags, enabling attackers to break out of the title context and execute malicious scripts in the rendered page.	6.1	More Details
CVE-2025-8591	The software accepts user-supplied input via a URL parameter without adequate output encoding before reflecting it back to the user's browser. This condition allows an attacker to inject malicious script content into pages served by the application. By leveraging this weakness, an attacker can cause the user's browser to redirect to a malicious website, modify the UI of the webpage, or retrieve information from the browser. However, the impact is mitigated by the use of httpOnly flags on session-related cookies, preventing session hijacking.	6.1	More Details
CVE-2026-6685	FatFs R0.16 and earlier exhibits a stale dirty-cache skip via unsigned-subtraction wrap in f_read() / f_write() (fp->sect - sect < cc) during interleaved read/write on fragmented filesystems. This maps to CWE-191 (Integer Underflow). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H (6.1, Medium). The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Total.	6.1	More Details
CVE-2026-8306	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Armiya Information Technologies Ltd. Co. Access Control System (GKS) allows Stored XSS. This issue affects Access Control System (GKS): before Version 2.	6.1	More Details
CVE-2026-58580	LobeChat through 2.2.9 server-database deployments are vulnerable to broken object-level authorization in MessageModel. The updateMessagePlugin, updatePluginState, updatePluginError, updateTTS and updateTranslate methods filter target rows by message id alone, omitting the userId scope that sibling methods apply, and findMessagePlugin reads back by id alone. Reachable via the corresponding tRPC message procedures, an authenticated user who knows another user's message identifier can overwrite that victim's plugin tool-call metadata, plugin state/error, text-to-speech and translation records on the same instance, and the tampered content is served back to the victim. Exploitation requires knowledge of the victim's non-enumerable message identifier.	5.9	More Details
CVE-2026-55950	Time-of-check Time-of-use (TOCTOU) race condition vulnerability in Erlang/OTP ssl (dtls_packet_demux module) allows an unauthenticated remote attacker to crash all active DTLS sessions on a listener. A DTLS server listener uses a single shared dtls_packet_demux gen_server process to route incoming UDP datagrams to the correct connection handler. When a DTLS client reconnects rapidly from the same source address and port (sending multiple ClientHello messages in quick succession), a race condition in the demux's internal gb_trees key-value store causes a {key_exists, {old, Client}} crash, terminating the demux process. Because the demux is shared across all DTLS associations on that listener, its crash immediately kills every active DTLS session, not just the attacker's. The attack is pre-authentication: the attacker only needs to send UDP datagrams containing valid ClientHello messages from the same source IP and port before the intermediate DOWN monitor message is processed by the gen_server. No credentials, no completed handshake, and no special configuration are required, and the crash can be repeated indefinitely to create a persistent denial of service for all clients of that listener. This vulnerability is associated with program file lib/ssl/src/dtls_packet_demux.erl. This issue affects OTP from OTP 25.3 before 29.0.3, 28.5.0.3, and 27.3.4.14 corresponding to ssl from 10.9 before 11.7.3, 11.6.0.3, and 11.2.12.10.	5.9	More Details
CVE-2026-56016	CGI::Session::ID::md5 versions before 4.49 for Perl generate predictable session ids from low-entropy sources. The generate_id method builds the session id from a MD5 digest of the process id, the epoch time, and the built-in rand() function. All three are predictable, low-entropy sources: the PID is drawn from a small range, the epoch time can be guessed or read from the HTTP Date header, and Perl's rand() is unsuitable for security purposes because it is predictable and reversible. An attacker who predicts a session id can impersonate the corresponding session and bypass authentication.	5.9	More Details
CVE-			More

2026-57762	Author Cross Site Scripting (XSS) in Simple URLs <= 151 versions.	5.9	Details
CVE-2026-24266	NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker can cause a use-after-free issue. A successful exploit of this vulnerability might lead to denial of service.	5.9	More Details
CVE-2026-49858	API Platform Core is a system to create hypermedia-driven REST and GraphQL APIs. In versions from 2.6.0 prior to 4.1.29, 4.2.26, and 4.3.12, a missing isCacheKeySafe gate in the JSON:API and HAL item normalizers causes a cross-user attribute leak. #[ApiProperty(security: ...)] is evaluated per request to decide whether a property is exposed. The componentsCache arrays in ApiPlatform\JsonApi\Serializer\ItemNormalizer and ApiPlatform\Hal\Serializer\ItemNormalizer are keyed on $context['cache_key'], which is set unconditionally before delegating to the parent normalizer. The component structure (attributes, relationships, links) computed for one request can therefore be reused for a subsequent request whose user has a different set of accessible properties. A user with lower privileges may end up seeing the structure of properties that the security predicate would otherwise have hidden for them. This issue has been fixed in versions 4.1.29, 4.2.26, and 4.3.12.	5.9	More Details
CVE-2026-57722	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ShortPixel Enable Media Replace allows Stored XSS. This issue affects Enable Media Replace: from n/a through 4.2.1.	5.9	More Details
CVE-2026-12352	This vulnerability allows an unauthenticated actor to bypass authentication and gain access to restricted resources on the device.	5.9	More Details
CVE-2026-55577	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-51 and 7.1.2-26, a heap buffer overflow occurs in the MVG decoder that could result in an out of bounds write when processing a crafted image. This issue has been fixed in versions 6.9.13-51 and 7.1.2-26.	5.9	More Details
CVE-2026-58472	GNU Wget through 1.25.0, fixed in commit dd692d9, contains a heap buffer overflow vulnerability in the html_quote_string() function in src/convert.c that allows a remote attacker to trigger memory corruption by supplying a crafted HTML attribute with a large number of characters requiring entity encoding. A server-supplied HTML attribute causes a signed integer counter to overflow during output size accumulation, resulting in an undersized heap allocation and subsequent heap buffer overflow during the copy phase.	5.9	More Details
CVE-2026-58471	GNU Wget through 1.25.0, fixed in commit c2640fe, contains a heap buffer overflow vulnerability in the convert_fname() function within src/url.c that allows remote attackers to trigger memory corruption through a server-supplied filename requiring character set conversion. When the output buffer is too small during iconv E2BIG reallocation, the reallocation logic miscalculates the remaining space, leading to a heap buffer overflow that can be exploited via a maliciously crafted server response.	5.9	More Details
CVE-2026-14406	Out of bounds read in V8 in Google Chrome prior to 150.0.7871.46 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory via a crafted Chrome Extension. (Chromium security severity: Medium)	5.9	More Details
CVE-2026-46467	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an insertion of sensitive information into log file vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to information exposure.	5.8	More Details
CVE-2026-59101	AutoBangumi before 3.2.8 contains a server-side request forgery (SSRF) vulnerability that allows unauthenticated remote attackers to probe internal network services by supplying arbitrary host values to an unprotected setup endpoint. Attackers can send requests to the POST /api/v1/setup/test-downloader endpoint during the initial setup window, causing the server to issue HTTP GET requests to internal or reserved addresses and leak information through echoed connection-error messages.	5.8	More Details
CVE-2026-14355	In PHP versions 8.2.* before 8.2.32, 8.3.* before 8.3.32, 8.4.* before 8.4.23, 8.5.* before 8.5.8, the AES-WRAP-PAD algorithm implementation in OpenSSL extension contains a buffer allocation flaw. The output buffer for the AES key-wrap-with-padding operation is sized from the plaintext length without accounting for RFC 5649 expansion. This may cause OpenSSL to write beyond allocated memory, corrupting heap metadata and triggering application abort.	5.6	More Details
CVE-2026-14609	A vulnerability was detected in SourceCodester CET Automated Grading System with AI Predictive Analytics 1.0. This issue affects some unknown processing. The manipulation results in session fixiation. The attack can be executed remotely. The attack requires a high level of complexity. The exploitability is assessed as difficult. The exploit is now public and may be used.	5.6	More Details
CVE-2026-	A security vulnerability has been detected in NousResearch hermes-agent up to 0.15.2. This affects the function DiscordAdapter._is_allowed_user of the file gateway/platforms/discord.py of the component Discord Platform Integration. Such manipulation leads to improper authentication. The attack can be launched remotely. This attack is characterized by high complexity. The exploitability is reported as difficult. The	5.6	More Details

14627	exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-10540	The Control-M/Enterprise Manager uses weak protections for stored hashes of account passwords, potentially allowing offline password recovery attacks if credential data is obtained by an attacker. This vulnerability affects Control-M/Enterprise Manager unsupported versions 9.0.20.x and potentially earlier unsupported versions	5.6	More Details
CVE-2026-36910	An access violation in the BaseSplitterFile::Read function of Aleksoid1978 MPC-BE before commit 4341cb3 allows attackers to cause a Denial of Service (DoS) via a crafted MP4 file.	5.5	More Details
CVE-2026-47262	containerd is an open-source container runtime. Versions prior to 1.7.33, 2.0.10, 2.1.9, 2.2.5 and 2.3.2, contain a vulnerability that allows a maliciously crafted image to cause a Denial of Service (DoS) condition. When creating a container from this image, memory exhaustion occurs, leading to an Out Of Memory (OOM) kill of the containerd process. This renders the container runtime API unavailable and can disrupt clients such as the Docker Engine or Kubernetes control-plane components. This issue has been fixed in versions 1.7.33, 2.0.10, 2.1.9, 2.2.5 and 2.3.2.	5.5	More Details
CVE-2026-14607	A weakness has been identified in RT-Thread up to 5.0.2. This affects the function sys_getaddrinfo of the file components/lwp/lwp_syscall.c. Executing a manipulation of the argument ai_addr can lead to memory corruption. The attack can only be executed locally. The exploit has been made available to the public and could be used for attacks. The pull request to fix this issue awaits acceptance.	5.5	More Details
CVE-2026-12166	A NULL pointer dereference vulnerability for driver `GFAC_Sys_x64.sys` in Little Orbit GFAC allows a local attacker to cause a denial of service via crafted requests that trigger a system crash.	5.5	More Details
CVE-2026-46465	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an use of externally-controlled format string vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure and denial of service.	5.5	More Details
CVE-2026-55510	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-51 and 7.1.2-26, when identifying an image with a crafted 8BIM profile with a specific format string a use-after-free will occur. This issue has been fixed in versions 6.9.13-51 and 7.1.2-26.	5.5	More Details
CVE-2026-59089	A flaw was found in GIMP. The PlayStation TIM loader, responsible for handling PlayStation image files, incorrectly calculates the size of the Color Look-Up Table (CLUT) due to an integer overflow. This occurs when multiplying num_colors and num_cluts, both 16-bit unsigned short integers, resulting in a value exceeding the maximum integer limit. An attacker could exploit this by providing a specially crafted image file, leading to undefined behavior and causing the GIMP plug-in to abort, effectively resulting in a denial of service.	5.5	More Details
CVE-2026-36911	A division-by-zero vulnerability in the CStreamSwitcherOutputPin::DecideBufferSize function of Aleksoid1978 MPC-BE before commit 4341cb3 allows attackers to cause a Denial of Service (DoS) via a crafted MP4 file.	5.5	More Details
CVE-2026-44362	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 3.20.0 and prior to version 4.11.0, a vulnerability in OP-TEE's subkey rollback protection allows the use of revoked or older subkey versions because the system fails to propagate versioning data during the Trusted Application (TA) loading process. In `core/crypto/signed_hdr.c`, the function `shdr_load_pub_key()` parses subkey headers but does not assign the `subkey_version` to the runtime `shdr_pub_key` structure. As a result, the `key->version` field remains at zero regardless of the version specified in the header. When `ree_fs_ta_open()` in `core/kernel/ree_fs_ta.c` calls `check_update_version()`, it passes this zeroed version to the rollback database. Because the database never receives a non-zero version to record, it never advances, effectively bypassing the rollback check and allowing TAs signed with downgraded subkey chains to load successfully. This impacts OP-TEE mainline configurations that utilize subkey-based signing chains for Trusted Application (TA) authentication. Version 4.11.0 contains a patch. No known workarounds are available.	5.5	More Details
CVE-2026-58468	NocoBase through 2.1.20 contains a server-side request forgery vulnerability in the serverRequest wrapper that allows authenticated administrators to issue arbitrary outbound HTTP requests by supplying malicious URLs to workflow request nodes, custom request action buttons, or the AI plugin. Attackers can target loopback addresses, RFC-1918 private ranges, and cloud instance metadata endpoints to perform internal network port enumeration, host discovery, and retrieval of IAM role credentials from the instance metadata service. v2.1.18 added a warning message for when SERVER_REQUEST_WHITELIST is not configured.	5.5	More Details
CVE-2026-48267	DNG SDK versions 1.7.1 2536 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE-2026-14330	Multiple unbounded alloca() calls in the PulseAudio protocol server.	5.5	More Details
CVE-2026-40257	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 3.21.0 and prior to version 4.11.0, the ARM Crypto Extensions accelerated SHA-3 implementation has an off-by-one error that can cause a massive heap overflow that corrupts all TEE kernel memory following the hash state. This affects all platforms built with `CFG_CRYPTO_WITH_CE82=y` (ARMv8.2+ with SHA3 Crypto Extensions). Version 4.11.0 contains a patch. As a workaround, disable SHA3 Crypto Extensions with `CFG_CRYPTO_WITH_CE82=n`.	5.5	More Details
CVE-2026-11397	The WP Import Export Lite plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to and including 3.9.30 via the wpie_import_upload_file_from_url AJAX action. The plugin's URL downloader first calls wp_safe_remote_get() (which correctly blocks private/reserved IP ranges), but when that call returns a WP_Error — the exact outcome for any blocked internal host — the Download::download_file() method falls back to GuzzleHttp\Client::request() with the original attacker-supplied URL and no SSRF protection (and with TLS verification disabled). This makes it possible for authenticated attackers, with administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services such as the cloud metadata endpoint at 169.	5.5	More Details
CVE-2026-13769	Overly permissive file permissions in AWS CLI before 1.44.78 (v1) and 2.34.29 (v2) on Unix-like systems where the umask has not been configured to restrict file permissions (the default on most systems) may allow other local users on the same host to read credentials written by certain CLI subcommands (aws codeartifact login, aws iam create-virtual-mfa-device, aws deploy register). To remediate this issue, users should upgrade to AWS CLI 1.44.78 (v1) or 2.34.29 (v2) or later.	5.5	More Details
CVE-2026-55597	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to version 7.1.2-26, an incorrect handling of arguments can cause a heap buffer over-write in the JP2 encoder. This issue has been fixed in version7.1.2-26.	5.5	More Details
CVE-2026-55628	In versions prior to 7.1.2-26he, the `-concatenate` operation is missing policy checks, potentially resulting in both reading and writing to paths disallowed by the security policy. This issue has been fixed in version 7.1.2-26.	5.5	More Details
CVE-2026-45488	User interface (ui) misrepresentation of critical information in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	5.4	More Details
CVE-2026-58579	RAGFlow before 0.26.3 stores an agent pipeline (DSL) node name without sanitization: the agent update endpoint normalizes the submitted DSL via normalize_dsl, which only performs JSON serialization validation and preserves the node name verbatim. The dataflow-result web UI then renders that name into the "Rerun from current step" confirmation modal via dangerouslySetInnerHTML, and the i18next configuration sets escapeValue:false, so the value is inserted into the DOM without HTML encoding. An authenticated workspace user who can create or edit an agent can inject arbitrary JavaScript that executes in the session of another workspace member who opens the dataflow result and clicks rerun, enabling session/token theft and account takeover across the user trust boundary.	5.4	More Details
CVE-2026-58278	Server-side request forgery (ssrf) in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	5.4	More Details
CVE-2026-14693	A flaw has been found in SourceCodester Multi-Vendor Online Grocery Management System 1.0. Affected by this vulnerability is the function cancel_order of the file classes/Master.php. Executing a manipulation can lead to improper authorization. The attack may be performed from remote. The exploit has been published and may be used.	5.4	More Details
CVE-2026-14636	A weakness has been identified in kirilkirkov Ecommerce-CodeIgniter-Bootstrap up to 23105f25dadf57b4314fc015a63a7c6e910c89df. Impacted is the function do_upload_others_images of the file application/modules/vendor/controllers/AddProduct.php of the component Vendor Image Manager. Executing a manipulation of the argument folder can lead to path traversal. It is possible to launch the attack remotely. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. This patch is called de1c9e73ccf3bd032d9a0525c4752290d959dd8b. It is best practice to apply a patch to resolve this issue.	5.4	More Details
CVE-2026-6283	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in DivvyDrive Information Technologies Inc. DivvyDrive allows Stored XSS. This issue affects DivvyDrive: from v.4.8.2.23 before v.4.8.3.1.	5.4	More Details
CVE-2026-	Silverstripe Framework is a PHP framework which powers the Silverstripe CMS. In versions prior to 6.2.2, the "Insert media from web" functionality in the CMS is vulnerable to XSS from a specially crafted embed. This	5.4	More

54720	issue was fixed in version 6.2.2/		Details
CVE-2026-11778	The The CURCY – Multi Currency for WooCommerce – Smoothly on WooCommerce 9.x plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.2.14. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	5.4	More Details
CVE-2026-58524	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	5.4	More Details
CVE-2026-53907	MCO is vulnerable to Stored Cross-Site Scripting (XSS) via the application logo upload functionality. An attacker with the ability to change the application logo can upload a crafted SVG file containing malicious JavaScript code that is executed when the logo is rendered or opened. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 25.3.3.1 but may also affect other versions.	5.4	More Details
CVE-2026-8309	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Armiya Information Technologies Ltd. Co. Access Control System (GKS) allows Reflected XSS. This issue affects Access Control System (GKS): before Version 2.	5.4	More Details
CVE-2026-58519	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in The Wikimedia Foundation Mediawiki - Cargo Extension allows Stored XSS. This issue affects Mediawiki - Cargo Extension: from * before 3.9.1.	5.4	More Details
CVE-2026-55435	Coder allows organizations to provision remote development environments via Terraform. Starting in version 2.30.0 and prior to versions 2.32.7, 2.33.8, and 2.34.2, AI Bridge proxy endpoints authenticate via `Server.IsAuthorized` in `coderd/aibridgedserver`, which validates key format, expiry, secret and deleted or system users but does not check whether the account is suspended. Because suspension does not revoke existing API keys, a suspended user's unexpired token keeps working. Practical impact is limited to already-issued API keys of suspended users until those keys are deleted. Versions 2.32.7, 2.33.8, and 2.34.2 patch the issue. As a workaround, on suspension, delete the user's API keys via `DELETE /api/v2/users/{user}/keys`.	5.4	More Details
CVE-2026-4772	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in TR7 Cyber Defense Inc. WAF-ASP allows Stored XSS. This issue affects WAF-ASP: from v1.0.324.900 before v1.4.0.117.	5.4	More Details
CVE-2026-59102	Forgejo before 15.0.3 contains a stored cross-site scripting vulnerability that allows authenticated attackers to execute arbitrary JavaScript in other users' browsers by setting a full name containing an HTML payload and triggering an Actions run. When the DEFAULT_SHOW_FULL_NAME option is enabled, the run description is assembled server-side with the user's display name interpolated into an HTML string via a translation function that does not escape its arguments, and the frontend renders the result using a Vue v-html binding, causing script execution for any user who views the affected Actions run page.	5.4	More Details
CVE-2026-54477	The admin panel lacks standard security headers, enabling clickjacking and cross-site scripting attacks.	5.4	More Details
CVE-2026-14614	A flaw was found in the ClientResource component of Keycloak's admin services when Fine-Grained Admin Permissions (FGAP) v2 is enabled. This issue allows a delegated administrator, who should only have limited control over specific clients, to attach or remove hidden client scopes that they are not authorized to see or manage. As a result, an attacker could inject unauthorized data or permissions into the security tokens issued to end-users, potentially tricking other applications into granting higher levels of access than intended.	5.4	More Details
CVE-2026-14723	A vulnerability was determined in AD-Security AD_Miner 1.9.0. Affected is the function request_a of the file ad_miner/scripts/analyse_cache.py of the component Cache Handler. This manipulation of the argument sys.argv[1] causes deserialization. The attack can only be executed locally. The pull request to fix this issue awaits acceptance.	5.3	More Details
CVE-2026-14414	Insufficient validation of untrusted input in Skia in Google Chrome prior to 150.0.7871.46 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	5.3	More Details
CVE-2026-11896	The My Calendar – Accessible Event Manager plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.7.14 via the 'vcal' parameter due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to enumerate occurrence IDs and access the full iCalendar export of non-public, draft, trashed, and personal calendar events, disclosing sensitive event metadata including titles, descriptions, dates, locations, organizer and host details, permalinks, and related calendar metadata.	5.3	More Details
CVE-	A vulnerability was determined in radareorg radare2 up to 6.1.6. This affects the function core_anal_bytes of		

2026-14757	the file libr/core/cmd_anal.inc. This manipulation causes integer overflow. The attack needs to be launched locally. The exploit has been publicly disclosed and may be utilized. It is suggested to install a patch to address this issue.	5.3	More Details
CVE-2026-55594	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-51 and 7.1.2-26, a missing depth check in the MVG decoder will result in a stack overflow when a crafted image is provided. This issue has been fixed in versions 6.9.13-51 and 7.1.2-26.	5.3	More Details
CVE-2026-57721	Missing Authorization vulnerability in WP Reloaded ApplyOnline allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects ApplyOnline: from n/a through 2.6.7.6.	5.3	More Details
CVE-2026-12122	The Kirki – Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 6.0.11 via the get_single_symbol. This makes it possible for unauthenticated attackers to extract the full builder metadata and rendered HTML of any kirki_symbol post — including unpublished drafts — by supplying a sequential WordPress post ID.	5.3	More Details
CVE-2026-12472	The Kirki – Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 6.0.11. 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 send arbitrary HTML-injected emails — including phishing messages embedding a real, valid WordPress password-reset URL for the targeted user — to any registered user via the site's own mail server, abusing its SPF/DKIM reputation. The attacker-controlled emailSubject parameter is passed to wp_mail() with only sanitize_text_field() applied, while emailBody 'text' items are concatenated raw into the HTML email body with no escaping, and 'chip' items can include the genuine WordPress password-reset link for the targeted account.	5.3	More Details
CVE-2026-14391	Integer overflow in ANGLE in Google Chrome on Windows prior to 150.0.7871.46 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	5.3	More Details
CVE-2026-46453	Improper Input Validation, Authorization Bypass Through User-Controlled Key vulnerability in Apache Camel ElasticSearch Rest Client. The camel-elasticsearch-rest-client component reads several Exchange headers to control its behaviour - SEARCH_QUERY (an advanced query body), OPERATION (which Elasticsearch operation to run), INDEX_NAME, INDEX_SETTINGS and ID. The string values of these header constants, defined in ElasticSearchRestClientConstant, are plain unprefixed names ('SEARCH_QUERY', 'OPERATION', 'INDEX_NAME', 'INDEX_SETTINGS', 'ID') rather than the 'Camel'-prefixed names used by every other Camel component (for example CamelSqlQuery, CamelMongoDbCriteria, CamelCqlQuery). Camel's inbound HTTP header filter, HttpHeaderFilterStrategy, blocks only header names that begin with 'Camel' or 'camel'. Because the Elasticsearch header names do not carry that prefix, they pass through the inbound filter unchanged. When a Camel route exposes an HTTP entry point (for example platform-http) in front of an elasticsearch-rest-client producer, an untrusted HTTP client can set these headers directly on its request and override the query and operation that the route author configured: reading every document in the index (SEARCH_QUERY with a match_all query), deleting documents (OPERATION set to Delete together with ID), or exfiltrating selected fields. No credentials are required and the producer reads the headers unconditionally. This issue affects Apache Camel: from 4.3.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix renames the camel-elasticsearch-rest-client Exchange header constant string values (ID, SEARCH_QUERY, INDEX_SETTINGS, INDEX_NAME, OPERATION) to carry the Camel prefix (CamelElasticsearchId, CamelElasticsearchSearchQuery, CamelElasticsearchIndexSettings, CamelElasticsearchIndexName, CamelElasticsearchOperation) so that they are blocked by the inbound HttpHeaderFilterStrategy; the Java field names are unchanged. For deployments that cannot upgrade immediately, strip the affected headers from untrusted inbound messages before they reach the producer (for example removeHeader('SEARCH_QUERY'), removeHeader('OPERATION'), removeHeader('INDEX_NAME'), removeHeader('INDEX_SETTINGS') and removeHeader('ID') in front of the elasticsearch-rest-client endpoint), or apply a custom HeaderFilterStrategy that blocks these names.	5.3	More Details
CVE-2026-56139	Generation of Error Message Containing Sensitive Information vulnerability in Apache Camel Undertow Component. The camel-undertow HTTP server consumer exposes a muteException option that controls what is returned to the client when a route processing error occurs. This option defaulted to false, whereas the other Camel HTTP server components (camel-http / camel-jetty / camel-servlet and camel-platform-http) default it to true. With muteException=false, when a request triggers an exception during route processing the consumer writes the full Throwable stack trace into the HTTP response body as text/plain instead of returning an empty body. Any unauthenticated client that can reach the endpoint and cause a processing error - for example by sending a malformed request body, an invalid parameter, or otherwise triggering a route-internal failure - therefore receives a complete Java stack trace. Such a stack trace can disclose sensitive internal information, including credentials embedded in exception messages, internal host names and IP addresses, filesystem paths, dependency and version details, database and class names, and the application's internal structure, which an attacker can use to plan further attacks. In addition, for Rest DSL consumers the muteException option was not honoured at all: the RestUndertowHttpBinding was created	5.3	More Details

	with a hard-coded false, so the stack trace was returned even when muteException=true had been configured. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. For deployments that cannot upgrade immediately, set muteException=true explicitly on the camel-undertow consumer (for example undertow: http://0.0.0.0:8080/api?muteException=true , or globally via the camel.component.undertow.mute-exception=true property), so that processing errors no longer return the stack trace to the client; note that on affected releases this workaround does not cover Rest DSL consumers, whose binding ignores the option until the fix is applied.		
CVE-2026-14628	A vulnerability was detected in NousResearch hermes-agent up to 2026.5.16. This impacts the function extract_media of the file gateway/platforms/base.py of the component Live Webhook Endpoint. Performing a manipulation results in path traversal. The attack may be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-14687	A vulnerability was determined in 666ghj BettaFish up to 1.2.1. Impacted is the function _deduplicate_results of the file InsightEngine/agent.py of the component InsightEngine search-result Deduplication. Executing a manipulation can lead to partial string comparison. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The pull request to fix this issue awaits acceptance.	5.3	More Details
CVE-2026-56152	Incorrect Authorization (CWE-863) in Elastic Defend can lead to unauthorized information disclosure via Accessing Functionality Not Properly Constrained by ACLs (CAPEC-1). Under certain conditions, a low-privileged authenticated user can access response action data that they are not authorized to view.	5.3	More Details
CVE-2026-59511	Insertion of Sensitive Information Into Sent Data vulnerability in Tim Strifler Exclusive Addons Elementor allows Retrieve Embedded Sensitive Data. This issue affects Exclusive Addons Elementor: from n/a through 2.7.9.9.	5.3	More Details
CVE-2026-54712	OpenTelemetry Java Instrumentation provides OpenTelemetry auto-instrumentation and instrumentation libraries for Java. In versions prior to 2.27.0, the RMI context propagation payload reader limits the number of context entries but does not limit the aggregate size of the strings read from the stream. An attacker who can reach an RMI endpoint on an instrumented JVM can send an oversized context propagation payload. This can cause excessive memory allocation while the JVM reads the payload, potentially leading to denial of service. The issue affects only deployments where RMI instrumentation is enabled and an RMI endpoint is network-reachable. This issue has been fixed in version 2.27.0.	5.3	More Details
CVE-2026-5348	The Academy LMS – WordPress LMS Plugin for Complete eLearning Solution plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 3.8.1. This is due to the '/topics' REST API endpoint being registered with a permission callback set to '__return_true', allowing unauthenticated access to course curriculum data without verifying the course's post status or user enrollment. This makes it possible for unauthenticated attackers to access detailed curriculum information for private, draft, scheduled, or password-protected courses by enumerating course IDs.	5.3	More Details
CVE-2026-49365	Generation of Error Message Containing Sensitive Information vulnerability in Apache Camel Netty HTTP component. The camel-netty-http HTTP server consumer exposes a muteException option that controls what is returned to the client when a route processing error occurs. This option defaulted to false because the backing field was an uninitialised primitive boolean (Java's default of false), whereas the other Camel HTTP server components (camel-http / camel-jetty / camel-servlet and camel-platform-http) default it to true. With muteException=false, when a request triggers an exception during route processing the consumer writes the full Throwable stack trace into the HTTP response body as text/plain (via DefaultNettyHttpBinding) instead of returning an empty body. Any unauthenticated client that can reach the endpoint and cause a processing error - for example by sending a malformed request body, an invalid parameter, or otherwise triggering a route-internal failure - therefore receives a complete Java stack trace. Such a stack trace can disclose sensitive internal information, including credentials embedded in exception messages, internal host names and IP addresses, filesystem paths, dependency and version details, database and class names, and the application's internal structure, which an attacker can use to plan further attacks. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. For deployments that cannot upgrade immediately, set muteException=true explicitly on the camel-netty-http consumer (for example netty-http: http://0.0.0.0:8080/api?muteException=true , or globally via the camel.component.netty-http.configuration.mute-exception=true property), so that processing errors no longer return the stack trace to the client.	5.3	More Details
CVE-2026-59519	Insertion of Sensitive Information Into Sent Data vulnerability in Softaculous FormLayer allows Retrieve Embedded Sensitive Data. This issue affects FormLayer: from n/a through 1.0.6.	5.3	More Details
	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Authorization Bypass Through User-Controlled Key vulnerability in Apache Camel Salesforce Component. The		

CVE-2026-49099	camel-salesforce producer resolves its operation parameters - the SOQL query, the SOSL search, the target SObject name and id, the Apex REST URL and method, and the Apex query parameters - from Exchange message headers, reading the header in preference to the value configured on the endpoint (AbstractSalesforceProcessor.getParameter() reads the header first and uses the endpoint configuration only as a fallback). The control-header constants in SalesforceEndpointConfig (for example SOBJECT_QUERY = sObjectQuery, SOBJECT_SEARCH = sObjectSearch, SOBJECT_NAME = sObjectName, SOBJECT_ID = sObjectId, APEX_URL = apexUrl, APEX_METHOD = apexMethod, and the apexQueryParam. prefix) used plain, non-Camel-prefixed values. Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that bridges an HTTP consumer (for example platform-http) into a salesforce: producer, any HTTP client could therefore set these headers and override what the route intended - supplying its own SOQL query or SOSL search to read data from any SObject the connected Salesforce user can access, overriding the target SObject name and id for CRUD operations, or redirecting an Apex REST call to a different endpoint and HTTP method (including destructive methods) with injected query parameters. All such operations run with the full permissions of the Salesforce connected (integration) user, which is typically broad. No credentials are required from the attacker when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that set Salesforce operation parameters via the raw header names must use the CamelSalesforce* names (for example CamelSalesforceSObjectQuery and CamelSalesforceApexUrl) instead of the old sObject* / apex* values; the endpoint-option spelling is unchanged. For deployments that cannot upgrade immediately, strip the Salesforce control headers from any untrusted ingress before the salesforce: producer (for example removeHeaders('sObject*') and removeHeaders('apex*') at the start of the route), and set the query, SObject and Apex parameters from a trusted source.	5.3	More Details
CVE-2026-53467	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-51 and 7.1.2-26, the MNG decoder contains a possible heap information disclosure vulnerability because part of the pixels are left unchanged. This issue has been fixed in versions 6.9.13-51 and 7.1.2-26.	5.3	More Details
CVE-2026-49098	Improper Input Validation, Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in Apache Camel Kafka Component. The camel-kafka producer can override its configured target topic at runtime from the kafka.OVERRIDE_TOPIC Exchange header: KafkaProducer.evaluateTopic() returns the header value in preference to the topic configured on the endpoint. The control-header constants in KafkaConstants (for example OVERRIDE_TOPIC = kafka.OVERRIDE_TOPIC, OVERRIDE_TIMESTAMP = kafka.OVERRIDE_TIMESTAMP, PARTITION_KEY = kafka.PARTITION_KEY) used plain, non-Camel-prefixed values. camel-kafka's own KafkaHeaderFilterStrategy does filter the kafka.* namespace, but only on the Kafka-to-Exchange serialization boundary (reading Kafka record headers into the Exchange, and writing Exchange headers into a Kafka record); it does not apply to headers that arrive from an upstream consumer in a multi-component route. The upstream HTTP consumer uses HttpHeaderFilterStrategy, which blocks only the Camel / camel namespace, so a kafka.* header passes through unfiltered. As a result, in a route that bridges an HTTP consumer (for example platform-http) into a kafka: producer, any HTTP client could set the kafka.OVERRIDE_TOPIC header and cause the message to be published to an arbitrary Kafka topic instead of the configured one - redirecting it to a sensitive internal topic, or injecting attacker-crafted messages into a topic consumed by a critical downstream service. The related kafka.OVERRIDE_TIMESTAMP and kafka.PARTITION_KEY headers could likewise be injected to backdate messages or target specific partitions. No credentials are required when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that set or read Kafka headers via the raw header names must use the CamelKafka* names (for example CamelKafkaOverrideTopic and CamelKafkaTopic) instead of the old kafka.* values. For deployments that cannot upgrade immediately, strip the kafka.* headers from any untrusted ingress before the kafka: producer (for example removeHeaders('kafka.*') at the start of the route), and set the target topic from a trusted source.	5.3	More Details
CVE-2026-48206	Improper Input Validation, Authorization Bypass Through User-Controlled Key vulnerability in Apache Camel JIRA component. The camel-jira producers read their operation parameters - the issue key, project key, transition id, summary, type, assignee, components, watchers, link type, work-log minutes and others - from Exchange message headers. The header constants defined in JiraConstants (for example ISSUE_KEY = IssueKey, ISSUE_PROJECT_KEY = ProjectKey, ISSUE_TRANSITION_ID = IssueTransitionId, LINK_TYPE = linkType) used plain, non-Camel-prefixed values. Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that bridges an HTTP consumer (for example platform-http) into a jira: producer, any HTTP client could therefore supply these headers and override the values the route intended, driving JIRA operations against the configured JIRA instance with the endpoint's configured service-account credentials - for example deleting or transitioning an arbitrary issue (via IssueKey / IssueTransitionId), creating an issue in a different project (via ProjectKey), modifying issue fields, adding or removing watchers, or logging work. The operations are bounded by what	5.3	More Details

	the configured service account is permitted to do. No credentials are required from the attacker when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that drive JIRA operations via the raw header names must use the CamelJira* names (for example CamelJiraIssueKey) instead of the old values. For deployments that cannot upgrade immediately, strip the camel-jira control headers from any untrusted ingress before the jira: producer (for example removing the IssueKey, ProjectKey, IssueTransitionId and related headers at the start of the route), and set the required JIRA operation parameters from a trusted source.		
CVE-2026-27409	Missing Authorization vulnerability in Webba Plugins Webba Booking allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Webba Booking: from n/a through 6.4.13.	5.3	More Details
CVE-2026-54500	Oj (Optimized JSON) is a JSON parser and Object marshaller packaged as a Ruby gem. In versions prior to 3.17.3, Oj.load in :object mode reads uninitialized stack memory (and, for long keys, reads out of bounds) when parsing a JSON object whose key is 254 bytes or longer. The interned bytes can surface to the caller, disclosing process stack memory. In ext/oj/intern.c, form_attr() handles the long-key path by allocating a heap buffer, `b`, populating it with the attribute name, and then freeing it — but it passed the uninitialized stack buffer buf (not b) to rb_intern3(). rb_intern3 therefore reads len + 1 bytes of uninitialized stack memory. When the key length is >= 256, it also reads out of bounds past the 256-byte buf. The resulting bytes are interned and can reach the caller via the produced Symbol or via the EncodingError message raised on invalid UTF-8, leaking process stack contents. This issue has been fixed in version 3.17.3.	5.3	More Details
CVE-2025-66076	Unauthenticated Broken Access Control in Woostify Sites Library <= 1.6.2 versions.	5.3	More Details
CVE-2026-14631	webpack-dev-server versions 5.2.5 and earlier terminate the whole Node.js process when an unauthenticated peer sends either a normal HTTP request with a malformed Host header or a WebSocket upgrade to the default /ws endpoint with a malformed Origin header. The malformed value causes an uncaught exception in the host-validation path and crashes the dev server. Impact is limited to availability of the development server, no data disclosure, no code execution. Patches: upgrade to webpack-dev-server 5.2.6. Workarounds: keep the dev server bound to localhost (the default) and do not expose it to untrusted networks.	5.3	More Details
CVE-2026-57760	Missing Authorization vulnerability in Sendcloud Sendcloud Shipping allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Sendcloud Shipping: from n/a through 1.0.29.	5.3	More Details
CVE-2026-20461	In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01267281 / MOLY01318201; Issue ID: MSV-6486.	5.3	More Details
CVE-2026-35159	Dell Client Platform BIOS contains an Authentication Bypass by Primary Weakness vulnerability. An unauthenticated attacker with physical access could potentially exploit this vulnerability, leading to Information Disclosure.	5.3	More Details
CVE-2026-11398	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.6.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to modify the personally identifiable information (first name, last name, phone number, and notes) of any existing customer record, including those linked to administrator accounts, by submitting the booking form with a known customer's email address. Exploitation requires the plugin to be configured with guest bookings enabled (is_customer_auth_disabled() returning true), which is necessary for the vulnerable unauthenticated code path in process_step_customer() to be reached.	5.3	More Details
CVE-2026-34198	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the TrustProxies middleware trusts all proxies ($proxies = '*'), accepting X-Forwarded-Host from any source. The TrustHosts middleware, intended to prevent host header attacks, has a circular caching dependency that prevents it from ever validating hosts. When a password reset is requested, the ResetPassword notification generates the reset URL using url(route(..., false)), which derives the host from the (spoofable) request. An unauthenticated attacker can trigger a password reset email containing a link pointing to an attacker-controlled domain, enabling token theft and account takeover. This issue is fixed in version 4.0.0-beta.471.	5.3	More Details
CVE-2026-27435	Missing Authorization vulnerability in WofficeIO Woffice allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Woffice: from n/a before 5.4.33.	5.3	More Details
	The WPForms – Easy Form Builder for WordPress – Contact Forms, Payment Forms, Surveys, & More plugin for		

CVE-2026-12127	WordPress is vulnerable to Improper Neutralization of CRLF Sequences ('CRLF Injection') in all versions up to, and including, 1.10.2 This is due to `get_reply_to_address()` processing the Reply-To display name through smart-tag expansion with context `'notification'` instead of `'notification-reply-to'`, which bypasses email-address validation while `wpforms_sanitize_textarea_field()` intentionally preserves CR/LF characters that are never stripped before the display name is concatenated into the raw `Reply-To:` mail header string. This makes it possible for unauthenticated attackers to inject arbitrary additional email headers — such as `Bcc:` — into outgoing notification emails, silently blind-copying all notification email copies to an attacker-controlled address. Exploitation requires that a form notification is configured to use a Paragraph Text (textarea) field as the Reply-To display name via a Smart Tag.	5.3	More Details
CVE-2026-26053	An Incorrect Privilege Assignment (CWE-266) vulnerability in the Command Centre Server allows an authenticated operator with limited privileges to perform some operations that they would not normally be authorized to perform. Version of Command Centre affected: 9.50 prior to vEL9.50.1587(MR1), 9.40 prior to vEL9.40.3130(MR3), 9.30 prior to vEL9.30.3983(MR5), 9.20 prior to vEL9.20.4349(MR7), all versions of 9.10.	5.3	More Details
CVE-2026-59097	Taiga before 6.10.2 contains a missing authorization vulnerability that allows unauthenticated remote attackers to create default due-date records in any project by exploiting unprotected POST endpoints on the user-story, task, and issue due-date API viewsets. Attackers can supply an arbitrary project identifier to these endpoints, which bypass permission checks and apply the AllowAny default, to pre-empt project administrators from initializing due dates by creating records before they can do so themselves.	5.3	More Details
CVE-2026-9180	The MotoPress Appointment Booking plugin for WordPress is vulnerable to Authorization Bypass Through User-Controlled Key in all versions up to, and including, 2.4.4. This is due to the `POST /motopress/appointment/v1/bookings` REST endpoint being registered with `'permission_callback' => '__return_true'`, allowing unauthenticated access, while the `createBooking` handler in `BookingsRestController.php` accepts an attacker-supplied `payment_details.booking_id` value and loads the referenced booking via `findById()` without verifying that the caller owns or has any rights to that booking. This makes it possible for unauthenticated attackers to overwrite the customer name, email address, phone number, and `customer_id` of any non-confirmed victim booking by submitting a request with no reservation items, causing `BookingService::createBooking()` to load the existing victim booking object and persist it with attacker-controlled customer data. Victim booking IDs can be harvested prior to exploitation without authentication by querying the also-publicly-accessible `GET /motopress/appointment/v1/bookings/reservations` endpoint with a guessable `service_id` and date range, and only bookings whose status is not `STATUS_CONFIRMED` (e.g., pending or auto-draft) are valid targets.	5.3	More Details
CVE-2026-57750	Unauthenticated Broken Access Control in ez Form Calculator Premium <= 2.14.1.2 versions.	5.3	More Details
CVE-2026-14610	A flaw has been found in Open Asset Import Library Assimp up to 6.0.5. Impacted is the function Assimp::CSMImporter::InternReadFile of the file code/AssetLib/CSM/CSMLoader.cpp of the component CSM File Handler. This manipulation causes heap-based buffer overflow. The attack is restricted to local execution. The exploit has been published and may be used. Patch name: eb84eec580d3f4ba2f0fd87409b7d0744620f11e. Applying a patch is the recommended action to fix this issue.	5.3	More Details
CVE-2026-20909	Gitea versions before 1.25.5 have insufficient permission checks when listing tracked time entries.	5.3	More Details
CVE-2026-12557	The Ninja Forms - File Uploads plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.3.29. 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 read all plugin debug log entries stored in the wp_nf3_log table or permanently delete all rows from that table.	5.3	More Details
CVE-2025-15666	A security vulnerability has been detected in Open Asset Import Library Assimp up to 5.4.3. Affected by this vulnerability is the function Assimp::SceneCombiner::Copy of the file code/Common/SceneCombiner.cpp of the component Model File Handler. Such manipulation of the argument width/height leads to heap-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed publicly and may be used. This and similar defects are tracked and handled via issue #6128.	5.3	More Details
CVE-2026-7828	UltraVNC repeater through 1.8.2.2 contains an integer overflow in the HTTP request logging path. In repeater/webgui/settings.c:336, the win_log() function allocates list nodes via malloc(sizeof(struct LIST) + strlen(line)), where line is derived from HTTP request URIs. If strlen(line) is sufficiently large, the addition overflows to a value smaller than sizeof(struct LIST), causing a heap allocation smaller than required. The subsequent strcpy of the full string into the undersized allocation produces a heap buffer overflow. In the current implementation this overflow is bounded by the HTTP receive buffer size (WI_RXBUFSIZE = 153600 bytes, well below SIZE_MAX on 32-bit builds), limiting practical exploitability to a partial heap write. A remote unauthenticated attacker can trigger the theoretical overflow path by sending a maximally-sized URI in an HTTP request to the repeater HTTP port.	5.3	More Details
	A heap-buffer-overflow flaw was found in 389 Directory Server (389-ds-base). When normalizing a		

CVE-2026-14940	Distinguished Name (DN) that contains a legacy-quoted value encoding a multivalued nested Relative Distinguished Name (RDN), the server can write past the end of a heap allocation while sorting RDN attribute-value pairs. An unauthenticated remote attacker can trigger this condition by sending an LDAP operation whose DN reaches the DN normalization routine, such as a search with a crafted base DN. This can corrupt heap memory and may cause denial of service.	5.3	More Details
CVE-2026-55726	The Azure Blob Storage container used for Gardyn device logs is publicly listable without authentication. A malicious user would be able to access any device log file available in the blob storage container.	5.3	More Details
CVE-2026-28705	Gitea versions before 1.25.5 use release tag names and asset names as filesystem path components when dumping release assets, allowing specially crafted names to affect dump output paths.	5.3	More Details
CVE-2026-25782	Gitea versions before 1.25.5 look up tracked-time entries by time ID without scoping the lookup to the issue in the request URL, allowing deletion attempts to target entries from another issue.	5.3	More Details
CVE-2026-57753	Unauthenticated Sensitive Data Exposure in Kit (formerly ConvertKit) for WooCommerce <= 2.1.5 versions.	5.3	More Details
CVE-2026-58470	GNU Wget through 1.25.0, fixed in commit 43d3ba9, contains an integer overflow vulnerability in the parse_content_range() function within src/http.c that allows server-controlled values to cause signed integer arithmetic to overflow. Attackers can supply malicious Content-Range header values to trigger undefined behavior and download desynchronization in the affected client.	5.3	More Details
CVE-2026-13459	The JetFormBuilder — Dynamic Blocks Form Builder plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.6.3. 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 retrieve every distinct value stored under any arbitrary wp_postmeta key on the site — including WooCommerce billing PII such as _billing_email, _billing_phone, and _billing_address fields, order totals, attachment paths, and any third-party plugin credentials or tokens stored in post meta — provided at least one published JetFormBuilder form with a get_from_db generator field exists on the site. Exploitation requires that the target site has at least one published jet-form-builder post containing a field whose generator_function is set to get_from_db; an attacker must supply a matching form ID, field name, and generator ID in the request, but all of these can be discovered by browsing the site's public forms.	5.3	More Details
CVE-2026-58203	pydantic-settings provides settings management using Pydantic. From 2.12.0 until 2.14.2, NestedSecretsSettingsSource reads secret values from files in a configured secrets_dir. When secrets_nested_subdir=True, a directory entry inside secrets_dir that is a symbolic link pointing outside secrets_dir is followed, so files outside the configured directory are read into settings values. The same code path bypasses the documented secrets_dir_max_size protection. An attacker or lower-privileged component able to influence entries in the configured secrets directory (for example, a writable or shared secrets mount) can turn this into an unintended local file read into settings and can defeat the advertised loading-size cap. This vulnerability is fixed in 2.14.2.	5.3	More Details
CVE-2026-57962	A malicious LDAP server, which a Thunderbird user is configured to query for address-book autocomplete, can stash arbitrarily large amounts of attacker-supplied data into the Thunderbird LDAP client until it crashes due to memory exhaustion. This vulnerability was fixed in Thunderbird 152.0.1 and Thunderbird 140.12.1.	5.3	More Details
CVE-2026-20457	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01826924; Issue ID: MSV-7301.	5.3	More Details
CVE-2026-20459	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01816800; Issue ID: MSV-6842.	5.3	More Details
CVE-2026-9182	ArcGIS Server contains an unrestricted file upload vulnerability. An unauthenticated attacker could exploit this issue by uploading a crafted file to the affected endpoint. Successful exploitation could allow arbitrary file upload.	5.3	More Details
CVE-2026-12657	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.6.2 via the 'service_id' parameter due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to create approved bookings against services explicitly restricted to admins and agents, consuming restricted appointment capacity and triggering unauthorized bookings for admin/agent-only services. The bypass works via both the params[booking][service_id] parameter in steps__load_step and the presets[selected_service] parameter in steps__start, both of which are publicly accessible without authentication.	5.3	More Details

CVE-2026-21368	Memory Corruption when parsing jpeg commands due to unaccounted extra writes to the buffer during validation checks.	5.3	More Details
CVE-2026-21384	Memory Corruption when updating prepared commands with invalid port indices based on user space input exceeds supported read client limits.	5.3	More Details
CVE-2026-21369	Memory Corruption when handling flash commands due to outdated LED count values being used after userspace modification.	5.3	More Details
CVE-2026-20460	In Modem, there is a possible information disclosure due to improper input validation. This could lead to remote information disclosure, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01811421; Issue ID: MSV-6788.	5.3	More Details
CVE-2026-9188	The Appointment Bookings for Zoom GoogleMeet and more – Wappointment plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to and including 2.7.6 via the `appointmentkey` parameter due to the appointment `edit_key` — the sole authorization token consumed by `tryCancel()` — being generated as a predictable, unsalted MD5 hash of only `client_id` (a sequential integer), `start_at` (a publicly observable appointment timestamp), and `staff_id` (a small enumerable integer), with no secret salt or random component, and the unauthenticated cancellation and rescheduling REST endpoints performing no ownership or identity verification beyond matching this reconstructible key. This makes it possible for unauthenticated attackers to compute valid `edit_key` values for appointments belonging to other users and cancel or reschedule those appointments arbitrarily. Exploitation requires the `allow_cancellation` or `allow_rescheduling` setting to be enabled on the site, both of which are common configurations for active booking deployments; an attacker can obtain the inputs needed to reconstruct a victim's key by booking their own appointment to observe their sequential `client_id` and correlating publicly visible appointment times and enumerable staff identifiers.	5.3	More Details
CVE-2026-21370	Memory Corruption when validating input batch size and buffer plane count exceeds maximum allowed values.	5.3	More Details
CVE-2026-14340	An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed a user-to-server token scoped to a GitHub App installation to perform certain write operations on public repositories outside the token's intended scope. This was possible because the authorization check only verified that the installation had read permissions on the target repository rather than verifying that the token's installation was explicitly granted access to that repository. An attacker who obtained a victim's user-to-server token could create issues, issue comments, commit comments, and private vulnerability reports on any public repository, appearing as the victim user with no indication of the app involvement. This vulnerability was fixed by adding a repository scope check for user-to-server tokens issued by global apps. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.22 and was fixed in versions 3.21.2, 3.20.4, 3.19.8, 3.18.11, 3.17.17, 3.16.20. This vulnerability was reported via the GitHub Bug Bounty program.	5.0	More Details
CVE-2026-59152	LangSmith Client SDKs provide SDK's for interacting with the LangSmith platform. Prior to 0.8.18, an attacker who can send an HTTP request to a server running the LangSmith SDK's TracingMiddleware can cause that server to read an arbitrary file from its local filesystem and upload the contents to LangSmith as a trace attachment. Depending on how the distributed trace system is deployed, triggering a read may not require authentication. Retrieving the contents requires read access to the LangSmith workspace the traces are sent to. The net effect is a trust-boundary crossing: a party with workspace trace-read access (for example a low-privilege workspace member, a contractor, or a compromised teammate account) gains the ability to read files from any server running TracingMiddleware, a capability outside that workspace's intended trust boundary. This vulnerability is fixed in 0.8.18.	5.0	More Details
CVE-2026-44936	Missing filtering when the helmRepoURLRegex field isn't set on a GitRepo resource in SUSE Rancher Fleet's bundle reader in 0.15 before 0.15.2, 0.14 before 0.14.6, 0.13 before 0.13.11 and 0.12 before 0.12.15 forwards Helm authentication credentials (BasicAuth) to any URL specified in the helm.repo field of a fleet.yaml file, allowing attackers able to push to fleet monitored git repos to leak helm access credentials.	5.0	More Details
CVE-2026-59100	LobeChat through 2.2.9 contains a broken object level authorization vulnerability that allows authenticated attackers to access and modify other users' chat-group agent data by supplying arbitrary group identifiers. Attackers can invoke the getGroupAgents, updateAgentInGroup, and removeAgentsFromGroup operations without user-scoped predicates to read agent listings, modify agent roles and ordering, and remove agents from chat groups belonging to other users.	5.0	More Details
CVE-2024-	Minosoft is an open-source, multi-version Minecraft Java Edition client written in Kotlin. Starting in commit f1ae30e2b046a490026a8413b075685deb795122, the CryptManager encryption routine (CryptManager.kt) initializes its AES cipher using an initialization vector (IV) that is set equal to the secret key rather than to a sufficiently random value. Because the IV is not random and is derived directly from the key, the encryption	5.0	More Details

56141	is vulnerable to chosen-ciphertext/chosen-plaintext attacks: an attacker who can submit specific messages for encryption can recover the secret key. This affects all versions supporting Minecraft protocol 1.7 and later. No patched version is available, and no known workarounds are available.		
CVE-2026-34167	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the ActivityMonitor Livewire component exposes a public $activityId property without Livewire's #[Locked] attribute. It loads activities via Activity::find($this->activityId) with no authorization or team scoping. Activity IDs are auto-incrementing integers. Any authenticated user can enumerate activity records across all teams and read the full command output from remote SSH processes, which may include secrets, configuration files, and infrastructure details. This issue is fixed in version 4.0.0-beta.471.	5.0	More Details
CVE-2026-54786	Wasmtime is a runtime for WebAssembly. All versions prior to 24.0.10; versions 25.0.0 through those before 36.0.11; versions 37.0.0 through those before 44.0.3; and versions 45.0.0 and 45.0.1 contain a native implementation of WASIp1 which suffers from a leak in the fd_renumber function where the file descriptor being renumbered to is not properly closed. Wasmtime's implementation erroneously only updated the table of descriptors for WASIp1 and didn't update the underlying table of descriptors used by the host. This behavior means that while fd_renumber works correctly from a guest's perspective it ends up leaking resources in the host that aren't cleaned up until the corresponding Store is destroyed. In a loop, guests can use fd_renumber to cause hosts to exhaust both resources and file descriptors. This bug only affects the native implementation of WASIp1, meaning that only runtimes which load core wasm modules and expose fd_renumber are affected. Runtimes are additionally only affected if they expose the ability to acquire a file descriptor, such as opening a file. For runtimes that deny access to files they are unaffected. This issue has been fixed in versions 24.0.10, 36.0.11, 44.0.3, and 45.0.2.	5.0	More Details
CVE-2026-46464	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper link resolution before file access ('Link following') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to information disclosure.	4.9	More Details
CVE-2026-12920	The Cookie Banner for GDPR / CCPA – WPLP Cookie Consent plugin for WordPress is vulnerable to generic SQL Injection via the 's' parameter in all versions up to, and including, 4.3.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2026-13357	The Houzez Property Feed plugin for WordPress is vulnerable to SQL Injection via the 'orderby' parameter in all versions up to, and including, 2.5.46 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query in the prepare_items() method of the Houzez_Property_Feed_Admin_Logs_Export_Table (and Houzez_Property_Feed_Admin_Logs_Import_Table) class. The user-controlled $_GET['orderby'] and $_GET['order'] values are filtered only with sanitize_text_field() and then concatenated into the SQL format string before $wpdb->prepare() is called — prepare() only parameterizes the appended LIMIT/OFFSET clause and cannot retroactively secure the already-tainted ORDER BY clause. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2026-56149	Allocation of Resources Without Limits or Throttling (CWE-770) in Elasticsearch can lead to a denial of service via Excessive Allocation (CAPEC-130). A user with elevated privileges can submit a specially crafted machine learning request that causes excessive memory consumption, which may render the affected node unavailable.	4.9	More Details
CVE-2026-42147	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, S3 storage endpoint validation only checks URL format and testConnection() sends a server-side request to the configured endpoint, allowing an authenticated user with storage management permissions to make Coolify request internal or metadata-service URLs. This issue is fixed in version 4.0.0-beta.474.	4.9	More Details
CVE-2026-14781	A flaw exists in the org.keycloak.broker.oidc package where the OIDC broker incorrectly synchronizes the email_verified claim. When an OIDC identity provider is configured with trustEmail=true and the userinfo endpoint is enabled, Keycloak retrieves the email address from the userinfo response but retrieves the email_verified status exclusively from the id_token. The root cause is a lack of validation ensuring that the email_verified claim in the id_token actually refers to the email address returned by the userinfo endpoint. If these two sources return different email addresses, the id_token's email_verified=true claim is blindly applied to the userinfo email. Exploitation Conditions: The OIDC identity provider must have trustEmail set to true (non-default). The userinfo endpoint must be enabled (default). The attacker must control or have compromised the upstream OIDC provider. Concrete Impact: Mark arbitrary email addresses as verified in the Keycloak database. Bypass email-based security controls or verification workflows. Potential account takeover if the application relies solely on the email_verified flag from the IdP to link accounts.	4.8	More Details
	The silent Just-In-Time (JIT) provisioning feature in federated authentication implementations fails to properly segregate user roles during account creation when a federated user shares a username with a local user. This		

CVE-2024-1248	allows the provisioning process to overwrite existing roles of local users with roles assigned to the federated user. Exploitation requires a federated identity provider (IDP) with silent JIT provisioning enabled and an attacker's knowledge of a local user's username. When these conditions are met, a malicious individual can leverage the JIT provisioning process to modify the roles of local users. The overwritten roles are limited to those defined within the federated IDP, typically granting minimal access rights unless explicitly configured otherwise by the federated IDP administrator.	4.8	More Details
CVE-2026-53877	An issue was discovered in Django 6.0 before 6.0.7 and 5.2 before 5.2.16. `django.contrib.gis.gdal.GDALRaster` over-reads its in-memory buffer when constructed from a bytes object, which can disclose adjacent memory or cause service degradation via a potential segmentation fault when the `vsi_buffer` property is accessed. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Bence Nagy for reporting this issue.	4.8	More Details
CVE-2026-54887	Use of Default Cryptographic Key vulnerability in Erlang/OTP ssl (DTLS server) allows predictable DTLS cookie computation during the startup window, enabling source address verification bypass. On DTLS server startup, dtls_server_connection:initial_hello/3 initializes previous_cookie_secret to the empty binary (<<>>) instead of a random value. Because HMAC with an empty key is deterministic, anyone who observes the plaintext ClientHello can compute dtls_handshake:cookie(<<>>, IP, Port, Hello) and forge a valid DTLS cookie before the first rotation of the cookie secret. The DTLS cookie (RFC 6347 §4.2.1) is a denial-of-service mitigation that prevents spoofed source IPs from forcing the server to allocate state and perform expensive cryptographic operations; it is not an authentication mechanism. During the window from server startup until the first secret rotation (0 to 15 seconds), an attacker who can observe the plaintext ClientHello can bypass the source address verification, enabling DTLS handshake amplification with spoofed source addresses. This vulnerability is associated with program file lib/ssl/src/dtls_server_connection.erl and program routine dtls_server_connection:initial_hello/3. This issue affects OTP from OTP 20.0 before 29.0.3, 28.5.0.3 and 27.3.4.14 corresponding to ssl from 8.2 before 11.7.3, 11.6.0.3 and 11.2.12.10.	4.8	More Details
CVE-2026-57352	Unauthenticated Broken Authentication in ALD – Dropshipping and Fulfillment for AliExpress and WooCommerce <= 2.2.0 versions.	4.8	More Details
CVE-2026-26145	Improper access control in Azure Synapse allows an authorized attacker to elevate privileges over a network.	4.8	More Details
CVE-2026-44040	UltraVNC through 1.8.2.2 uses a cryptographically weak pseudo-random number generator to produce VNC authentication challenge bytes. In rfb/vncauth.c:119-129, the vncRandomBytes() function seeds libc rand() with time(0) + getpid() + rand() and generates a 16-byte challenge. The combined seed space is approximately 31 bits (libc rand() internal state) and is entirely determined by publicly-observable values (wall-clock time and process ID). An attacker who can observe the authentication exchange can enumerate the seed space and predict the challenge within seconds, enabling forgery or offline brute-forcing of responses. Note: on Windows, the active code path may use vncEncryptBytes2.cpp which calls CryptGenRandom; reachability on shipped Windows binaries requires compile-graph verification and is under investigation.	4.8	More Details
CVE-2026-10659	The Dhara flash translation layer disk driver (drivers/disk/ftl_dhara.c) implemented the dhara_nand_ callbacks so that, on a flash error, the error code was written unconditionally through the caller-supplied dhara_error_t err pointer (e.g. *err = DHARA_E_ECC in dhara_nand_read, and similar in dhara_nand_erase/prog/copy). The upstream Dhara library calls these callbacks with err == NULL along its journal-resume binary search: find_last_checkblock() invokes find_checkblock(j, mid, &found, NULL), which forwards the NULL pointer into dhara_nand_read(). This path runs during disk_ftl_access_init() -> dhara_map_resume() whenever the FTL disk is mounted/initialised. If a flash read error (uncorrectable ECC, bad block, controller error) occurs on one of the probed checkpoint pages, the driver dereferences and writes to NULL, faulting the kernel (denial of service). The trigger is conditioned on the NAND medium content/health, which can be influenced by media wear, induced faults, or a corrupted/crafted on-flash image. The fix routes all error assignments through the library's NULL-safe dhara_set_error() helper. Affects Zephyr v4.4.0, where the driver was introduced.	4.7	More Details
CVE-2026-55595	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-51 and 7.1.2-26, when providing invalid arguments to the connected-components option an infinite loop will occur. This issue has been fixed in versions 6.9.13-51 and 7.1.2-26.	4.7	More Details
CVE-2026-14620	webpack-dev-server versions 5.2.5 and earlier expose two internal developer endpoints, /webpack-dev-server/open-editor and /webpack-dev-server/invalidate, that perform state-changing actions on any GET request without verifying that the request originated from the dev server's own page. Any website a developer visits while the dev server is running can trigger these endpoints cross-origin with no interaction beyond the visit. An attacker can open an arbitrary existing local file in the developer's editor, including files outside the project root, and repeated requests can spawn editor processes and force recompilations that degrade the developer's machine. Patches: upgrade to webpack-dev-server 5.2.6. Workarounds: none.	4.7	More Details
	The MAX32xxx USB device controller driver (drivers/usb/udc/udc_max32.c, compatible adi_max32_usbhs) dereferenced an endpoint buffer in its OUT and IN transfer-completion handlers without checking it for NULL.		

CVE-2026-10656	udc_event_xfer_out_done() called net_buf_add(buf, ep_request->actlen) immediately after buf = udc_buf_get(ep_cfg), where udc_buf_get() returns NULL when the endpoint FIFO is empty. A transfer-completion event is queued from interrupt context and processed asynchronously by the driver thread; between queuing and processing, the endpoint FIFO can be drained by host-controlled control flow — in particular udc_setup_received() drains the EP0 OUT/IN FIFOs whenever a new SETUP packet arrives, and dequeue/disable/purge paths drain it likewise. A USB host that aborts an in-flight EP0 control transfer with a new SETUP packet (legal USB behavior) can therefore cause a stale XFER_OUT_DONE event to be processed against an empty FIFO, producing net_buf_add(NULL, ...), a near-NULL pointer dereference that faults and crashes the device. No authentication is required; the attacker is the USB host the device is connected to (physical bus access). Impact is denial of service (device crash). The defect was introduced when the MAX32 UDC driver was added and shipped in Zephyr v4.4.0. The fix adds NULL-buffer checks that return early with UDC_EVT_ERROR/-ENOBUFS in both the OUT-done and IN-done handlers.	4.6	More Details
CVE-2026-46672	Actual is a local-first personal finance app. Prior to 26.6.0, @actual-app/cli ships a hand-rolled CSV serializer in packages/cli/src/output.ts used whenever the global --format csv option is passed, whose escapeCsv helper only handles RFC 4180 delimiter, quote, and newline escaping and does not neutralize standard CSV formula-injection prefixes. Any CLI command that streams an object array containing user-controlled strings, including transactions list, accounts list, payees list, categories list, tags list, category-groups list, rules list, schedules list, and query, can emit cells that auto-evaluate when the resulting CSV is opened in Excel, LibreOffice Calc, or Google Sheets, enabling data exfiltration and arbitrary formula execution. This issue is fixed in version 26.6.0.	4.6	More Details
CVE-2026-6683	FatFs R0.16 and earlier contains a divide-by-zero in exFAT sync logic bug when crafted metadata causes n_fatent - 2 to be zero during write/sync operations. This maps to CWE-369 (Divide By Zero). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H (4.6, Medium). Network-delivered update media can make this remote in some pipelines. The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Partial.	4.6	More Details
CVE-2026-34098	Guardian language-system fails to sanitize the id GET parameter before inserting it into HTML source and form action attributes in media.php (lines 119, 129). An authenticated attacker can craft a URL that injects script tags executing in the victim's browser session.	4.6	More Details
CVE-2026-34097	Guardian language-system fails to sanitize the id GET parameter before inserting it into multiple HTML form action attributes in text_file.php (lines 94, 101, 323, 403, 826, 852). An authenticated attacker can craft a URL that injects script tags executing in the victim's browser session.	4.6	More Details
CVE-2026-6686	FatFs R0.16 and earlier contains an uninitialized cluster exposure when f_lseek() extends files beyond EOF without zero-filling newly allocated clusters. This maps to CWE-908 (Use of Uninitialized Resource). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N (4.6, Medium). The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Partial.	4.6	More Details
CVE-2026-4770	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in TR7 Cyber Defense Inc. Web Application Firewall allows DOM-Based XSS. This issue affects Web Application Firewall: from v1.0.42.239 before v1.4.0.117.	4.6	More Details
CVE-2026-6684	FatFs prior to R0.16 that use GPT scanning with 'FF_LBA64 = 1' contains an issue where an unbounded loop count derived from GPT header field GPTH_PtNum, enabling extremely long or effectively infinite mount-time scans. This maps to CWE-835 (Loop with Unreachable Exit Condition). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H (4.6, Medium). The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Partial.	4.6	More Details
CVE-2026-34096	Guardian language-system fails to sanitize the name GET parameter before outputting it into an HTML input value attribute in designer.php (line 57). An authenticated attacker can craft a URL containing script tags that execute in the victim's browser session.	4.6	More Details
CVE-2026-55798	Pillow is a Python imaging library. Prior to 12.3.0, WindowsViewer.get_command() constructed a cmd.exe shell command by directly embedding a file path into an f-string without escaping and passed the result to subprocess.Popen(..., shell=True), allowing shell metacharacters in the file path to inject arbitrary cmd.exe commands. This issue is fixed in version 12.3.0.	4.5	More Details
CVE-2026-44269	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper link resolution before file access ('link following') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to unauthorized access.	4.4	More Details
CVE-2026-46468	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper link resolution before file access ('Link following') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to information exposure.	4.4	More Details

CVE-2026-5051	HashiCorp Vault and Vault Enterprise prior to 2.0.1 audit device validation logic did not consistently apply plugin directory protections when the legacy file audit path option was used. This vulnerability (CVE-2026-5051) is fixed in 2.0.1, 1.21.6, 1.20.11, and 1.19.17.	4.4	More Details
CVE-2026-49088	Insertion of Sensitive Information into Log File (CWE-532) in Kibana can lead to information disclosure. When the optional application performance monitoring (APM) instrumentation is enabled, sensitive request header values could be recorded in application logs, where they may be accessible to operators with log access.	4.4	More Details
CVE-2026-44268	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an incorrect permission Assignment for critical resource vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to unauthorized access.	4.4	More Details
CVE-2026-10104	The Product Video Gallery for Woocommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via custom_thumbnail Parameter in all versions up to, and including, 1.5.1.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with shop manager-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Details
CVE-2026-14969	A flaw was found in 389-ds-base where the LDBM backend attribute encryption uses a hardcoded static initialization vector for AES-CBC and 3DES-CBC operations, allowing an attacker with privileged filesystem access to detect plaintext equality across encrypted entries by comparing ciphertext blocks.	4.4	More Details
CVE-2026-13211	The genucenter web interface before version 8.0p11 unnecessarily exposes sensitive SNMP authentication and encryption keys in its HTTP responses to users with the “Service” or “Admin” role.	4.3	More Details
CVE-2026-8480	A vulnerability was discovered on Stormshield Network Security 4.3.0 to 4.3.41 (included), 4.4.0 to 4.8.15 (included) , 5.0.2 EA to 5.0.5 (included) A revoked client certificate can still be used to authenticate to the captive-admin portal, allowing an attacker who possesses the revoked certificate to gain administrative access.	4.3	More Details
CVE-2026-5138	A flaw was found in Foreman. An authenticated user with host-edit permissions could exploit a cross-tenant information disclosure vulnerability. This flaw occurs because the taxonomy_scope controller method does not properly validate organization and location IDs from nested request parameters, bypassing existing authorization checks. This allows the user to leak sensitive infrastructure metadata, including subnet topology, IP ranges, gateways, DNS servers, and VLAN IDs, from organizations and locations they are not authorized to access.	4.3	More Details
CVE-2026-53908	MCO is vulnerable to User Enumeration through authentication-related functionalities. The application returns distinguishable responses for valid and invalid users during username reminder and password reset operations. An attacker can leverage these differences to enumerate valid usernames and email addresses. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 25.3.3.1 but may also affect other versions.	4.3	More Details
CVE-2026-34170	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the GithubApp api_url field is used as the base URL for server-side HTTP requests without allowlisting or private IP blocking, allowing an authenticated user to configure a GitHub App source that causes Coolify to request internal services or cloud metadata endpoints. This issue is reported as fixed in version 4.0.0-beta.471.	4.3	More Details
CVE-2026-59520	Cross-Site Request Forgery (CSRF) vulnerability in properfraction CrawlWP SEO allows Cross Site Request Forgery. This issue affects CrawlWP SEO: from n/a through 3.0.16.	4.3	More Details
CVE-2026-14793	A vulnerability was detected in Craft CMS up to 4.18.0.1. Affected is the function actionReorderSets of the file src/controllers/GlobalsController.php of the component reorder-sets Endpoint. The manipulation results in authorization bypass. The attack can be executed remotely. Upgrading to version 4.18.1 is able to address this issue. The patch is identified as 9bd05c91e6a7e6da5e949ec41a31c220c059aa04. The affected component should be upgraded.	4.3	More Details
CVE-2026-11981	The GiveWP plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.15.3 This is due to missing nonce validation on the give_set_notification_status_handler() function. This makes it possible for unauthenticated attackers to disable donation email notifications via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-44041	UltraVNC through 1.8.2.2 contains an out-of-bounds read in the wide-string to multibyte conversion helper. In rfb/dh.cpp:204, the vncWc2Mb() function passes a caller-supplied WCHAR pointer to wcslen() before any bounds check. If the caller provides a wide-character buffer that is not properly NUL-terminated, wcslen() reads past the end of the buffer until it encounters a NUL wchar, resulting in an out-of-bounds read. Under typical Win32 API usage this requires an abnormal caller contract. Impact is limited to a potential information disclosure from adjacent memory regions or a process crash (denial of service) if the over-read crosses a	4.3	More Details

	page boundary.		
CVE-2026-12113	The Appointment Booking Calendar plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.4.02 via the cpabc_appointments_filter_list. This makes it possible for authenticated attackers, with contributor-level access and above, to extract customer names, email addresses, phone numbers, appointment comments, and other booking personally identifiable information.	4.3	More Details
CVE-2026-57720	Missing Authorization vulnerability in Codexpert Inc ThumbPress allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects ThumbPress: from n/a through 6.3.2.	4.3	More Details
CVE-2026-46700	Actual is a local-first personal finance tool. Prior to 26.6.0, the GET /secret/:name endpoint in @actual-app/sync-server checks only that the caller has a valid session and does not verify the caller is an admin, while the sibling POST /secret/ handler enforces an admin check in OpenID mode. Any authenticated non-admin BASIC user in OpenID multi-user deployments can probe the secrets store and learn which admin-managed bank-sync integrations have been configured, including simplefin_accessKey, pluggyai_clientSecret, pluggyai_itemIds, and the gocardless secrets. This issue is fixed in version 26.6.0.	4.3	More Details
CVE-2026-12435	The Motors – Car Dealership & Classified Listings Plugin plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.4.111. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to mark or unmark any other user's car listing as sold by replaying a valid nonce harvested from their own listing against an arbitrary victim post ID, triggering a site-wide 'Sold' badge on the victim's listing and silently stripping its special_car featured post meta as a side effect. Exploitation requires the attacker to hold an active listing of their own (obtainable by a Subscriber via the plugin's add-listing form) in order to harvest a valid nonce for the 'stm_mark_as_sold_car' action, which can then be replayed against any other listing's post ID.	4.3	More Details
CVE-2026-12133	The JoomSport – for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to Missing Authorization to Arbitrary Group Deletion in versions up to, and including, 5.7.8. This is due to a missing capability check in the joomsport_season_groupdel() AJAX handler, which only verifies a nonce before executing a DELETE query on attacker-supplied group IDs. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary JoomSport group records.	4.3	More Details
CVE-2026-12408	The Slim SEO – A Fast & Automated SEO Plugin For WordPress plugin for WordPress is vulnerable to Unauthorized Private Content Disclosure in all versions up to, and including, 4.9.8 via the `/wp-json/slim-seo/meta-tags/ai` REST API endpoint. This is due to the endpoint's `permission_callback` performing only a top-level `edit_posts` capability check without verifying that the requesting user has read access to the specific post supplied via the `object.ID` parameter, allowing the `generate` function to pass the attacker-controlled post ID to `Data::get_post_content()`, which calls `get_post()` regardless of post status or ownership. This makes it possible for authenticated attackers with Contributor-level access and above to retrieve AI-generated summaries of the raw `post_content` of arbitrary posts they are not authorized to view — including private posts, drafts, pending, future, and password-protected content authored by other users — with the substance of the protected content disclosed via the HTTP response.	4.3	More Details
CVE-2026-10096	The Qi Blocks plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.4.9 via the 'page_id' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with author-level access and above, to modify the stored Qi Blocks styles of arbitrary posts, templates, or widgets they do not own — including site-wide surfaces via the reserved 'template' and 'widget' page_id values — enabling unauthorized frontend defacement, content hiding, and degradation of any page on the site. The endpoint's permission_callback checks only the generic edit_posts and publish_posts capabilities, meaning any user with the built-in Author role satisfies the check regardless of post ownership.	4.3	More Details
CVE-2026-14783	A vulnerability was determined in NousResearch hermes-agent 2026.5.29.2. The impacted element is the function skill_view of the file tools/skills_tool.py. Executing a manipulation of the argument Name can lead to path traversal. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. This patch is called 56f833efa427ccb444c0f9ad1759af1012f2124d. It is advisable to implement a patch to correct this issue.	4.3	More Details
CVE-2026-12902	The Kadence Blocks — Page Builder Toolkit for Gutenberg Editor plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.7.7. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to create arbitrary Media Library attachments by downloading remote images to the site's uploads directory via wp_upload_bits() and wp_insert_attachment(), bypassing the upload_files capability boundary.	4.3	More Details
CVE-2026-11887	The Salon Booking System WordPress plugin before 10.30.20 does not have proper authorisation checks on one of its AJAX actions, allowing any authenticated user, such as a subscriber, to modify a Salon Booking System WordPress plugin before 10.30.20 setting and bypass the manual approval of new bookings.	4.3	More Details
	The Kadence Blocks – Gutenberg Blocks for Page Builder Features plugin for WordPress is vulnerable to		

CVE-2026-12904	Insecure Direct Object Reference in versions up to and including 3.7.7. This is due to a mismatch between the object used for authorization and the object actually accessed in the Optimize_Rest_Controller's create_item(), get_item(), delete_item(), and bulk_delete_items() endpoints — authorization is checked via current_user_can('edit_post'/'delete_post', $post_id) against the user-supplied post_id, while the storage layer keys analysis records on sha256($post_path) from a separately supplied, attacker-controlled post_path parameter, with no enforcement that post_path corresponds to post_id. This makes it possible for authenticated attackers, with Contributor-level access and above, to read or delete optimizer analysis records belonging to posts owned by other users by submitting their own post_id (which passes the capability check) together with the victim post's path.	4.3	More Details
CVE-2026-48891	A bug in Apache Airflow's `/ui/dependencies` scheduling graph endpoint applied the caller's readable-Dag filter to the top-level serialized Dag key but still emitted referenced Dag IDs through the `dep.source` and `dep.target` fields of trigger / sensor dependency entries. An authenticated UI user with read permission on some Dags could enumerate the identifiers of other Dags they were not authorized to read by inspecting the dependency graph for trigger / sensor references. Affects deployments that rely on per-Dag read scoping to keep Dag identifiers private across teams. This is a residual gap in the fix for CVE-2026-28563, which filtered the top-level Dag key but did not propagate the filter into the trigger / sensor dep-source / dep-target fields. Users who already upgraded for CVE-2026-28563 should additionally upgrade to `apache-airflow` 3.3.0 or later to cover the residual trigger / sensor dependency leak.	4.3	More Details
CVE-2026-59709	Ghostfolio's PUT /api/v1/portfolio/holding/:dataSource/:symbol/tags endpoint fails to verify Access.permissions field when processing the Impersonation-Id header, allowing read-only access grantees to modify portfolio holding tags. Attackers with valid read-only share tokens can assign or remove tags on victim holdings, corrupting portfolio categorization and reports.	4.3	More Details
CVE-2026-14794	A flaw has been found in Craft CMS up to 4.18.0.1. Affected by this vulnerability is the function actionGetNewUsersData of the file src/controllers/ChartsController.php of the component Charts Endpoint. This manipulation of the argument userGroupId causes improper authorization. The attack is possible to be carried out remotely. Upgrading to version 4.18.1 addresses this issue. Patch name: 9ee53efc1314e6aba32771c66a13e072a246f4ce. It is suggested to upgrade the affected component.	4.3	More Details
CVE-2026-11562	The WS Form LITE WordPress plugin before 1.11.8 does not have a capability check on one of its settings-update actions, allowing authenticated users with subscriber-level access and above to modify the WS Form LITE WordPress plugin before 1.11.8's settings.	4.3	More Details
CVE-2026-5137	The RTMKit (rometheme-for-elementor) plugin for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 2.0.7 This is due to insufficient path validation on the 'template' parameter in the render_templates AJAX endpoint, which is used directly in a require/include statement without sanitization. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute files on the server ending in _templates.php, allowing the execution of any PHP code in those files.	4.3	More Details
CVE-2026-14800	A weakness has been identified in imhamzaazam ecommerceFlask up to cb7d9e24c30a99379651b7493b32048126ef402b. The affected element is an unknown function. This manipulation causes cross-site request forgery. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-14629	A flaw has been found in RT-Thread up to 5.2.2. Affected is the function read/write/sys_ioctl of the file components/lwp/lwp_syscall.c of the component Parameter Handler. Executing a manipulation can lead to divide by zero. The attack may be launched remotely. The exploit has been published and may be used. The pull request to fix this issue awaits acceptance.	4.3	More Details
CVE-2026-57730	Subscriber Broken Access Control in Flatsome <= 3.20.5 versions.	4.3	More Details
CVE-2026-57690	Unauthenticated Cross Site Request Forgery (CSRF) in Werkstatt <= 4.7.2 versions.	4.3	More Details
CVE-2026-14656	A security vulnerability has been detected in code-projects Assessment Management 1.0. This affects an unknown part of the file /admin/remove-user.php. The manipulation of the argument ID leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2026-11592	The Email Subscribers & Newsletters – Email Marketing, Post Notifications & Newsletter Plugin for WordPress plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.9.27. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to overwrite plugin mail settings (from name and from email address), create audience lists, insert arbitrary contacts into those lists, create and overwrite newsletter broadcasts and post notifications, add workflows, and queue and dispatch mass email to	4.3	More Details

	arbitrary recipients.		
CVE-2026-57689	Subscriber Broken Access Control in Werkstatt <= 4.7.2 versions.	4.3	More Details
CVE-2026-11600	The Envo's Templates & Widgets for Elementor and WooCommerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing authorization check on the Envo Tabs (and Off Canvas) widget's template rendering in versions up to, and including, 1.4.26. The render() method of the Tabs widget passes a user-controlled template/post ID directly to Elementor's get_builder_content_for_display() without verifying the referenced post's status (published/private/draft) or the visitor's authorization to view it. This makes it possible for authenticated attackers, with Author-level access and above, to disclose the contents of private Elementor-driven pages and templates to anonymous visitors by configuring an Envo Tabs widget on a public post to reference the private content's ID (which can be supplied by editing the underlying Elementor widget JSON via the Elementor editor REST API).	4.3	More Details
CVE-2026-14647	A weakness has been identified in onnx up to 1.21.x. This vulnerability affects the function convPoolShapeInference_opset19 of the file onnx/defs/nn/old.cc of the component onnxruntime. This manipulation causes out-of-bounds read. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. Patch name: a7bf3a0f1d18bb62575236ef6e4944980c40e045. It is recommended to apply a patch to fix this issue.	4.3	More Details
CVE-2026-41123	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper access control vulnerability in the RBAC. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to information tampering.	4.3	More Details
CVE-2026-14634	A vulnerability was identified in kirilkirkov Ecommerce-CodeIgniter-Bootstrap up to 213babdbaa949e94557246414db0130e01394517. This vulnerability affects the function checkForPostRequests of the file application/core/MY_Controller.php of the component Subscribed Emails Admin Page. Such manipulation of the argument User-Agent leads to cross site scripting. The attack may be performed from remote. The exploit is publicly available and might be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The name of the patch is 23105f25dadf57b4314fc015a63a7c6e910c89df. It is advisable to implement a patch to correct this issue.	4.3	More Details
CVE-2026-14633	A vulnerability was determined in kirilkirkov Ecommerce-CodeIgniter-Bootstrap up to 49b20f53de2b7ec34e920b11c863f1491d911a04. This affects an unknown part of the file /index.php/api/product/set of the component Hidden REST API Endpoint. This manipulation of the argument title/description causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. Patch name: d9785f995da77bdc62fb2d34bad5f7a162c9ad23. To fix this issue, it is recommended to deploy a patch.	4.3	More Details
CVE-2026-11900	The Ad Inserter – Ad Manager & AdSense Ads plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to and including 2.8.16 via the 'data' attribute of the [adinserter] shortcode. This is due to the replace_ai_tags() function processing a {reusable-block-N} tag pattern that calls get_post_field('post_content', N) without verifying the requesting user's capability with current_user_can('read_post'), without restricting the post type to 'wp_block', and without checking the post status. This makes it possible for authenticated attackers, with Contributor-level access and above, to read the full content of arbitrary posts including Private, Draft, Pending, Trashed, and password-protected posts owned by other users, by placing the shortcode in a post they own and previewing it.	4.3	More Details
CVE-2026-14632	A vulnerability was found in kirilkirkov Ecommerce-CodeIgniter-Bootstrap up to 95dfa8cebbb87ab46ae450643a07241274a74dce. Affected by this issue is the function setReferrer of the file application/core/MY_Controller.php of the component Trusted Backend Interface. The manipulation of the argument href results in open redirect. The attack can be executed remotely. The exploit has been made public and could be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The patch is identified as 213babdbaa949e94557246414db0130e01394517. A patch should be applied to remediate this issue.	4.3	More Details
CVE-2026-9230	The Quiz and Survey Master (QSM) – Easy Quiz and Survey Maker plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 11.1.4. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to modify quizzes they do not own, overwrite quiz results pages, and reroute quiz-result notification emails to attacker-controlled addresses. An attacker first calls the /quiz/structure endpoint with an arbitrary victim quiz ID to obtain a valid nonce bound to that quiz ID and their own user ID, then presents that nonce to the /quizzes/{id}/emails save endpoint, which accepts it without verifying quiz ownership.	4.3	More Details
	The JoomSport – for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to		

CVE-2026-12134	authorization bypass in all versions up to, and including, 5.7.8. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to create arbitrary season groups or modify existing group names, participants, and round-type options. Exploitation requires obtaining the joomsportajaxnonce, which is exposed on frontend pages that render a JoomSport shortcode.	4.3	More Details
CVE-2026-14418	Uninitialized Use in ANGLE in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-57685	Subscriber Broken Access Control in Martfury - WooCommerce Marketplace WordPress Theme <= 3.2.8 versions.	4.3	More Details
CVE-2026-14626	A weakness has been identified in NousResearch hermes-agent up to 2026.4.30. The impacted element is the function AIAgent.run_conversation of the file run_agent.py of the component HTTP API. This manipulation of the argument todos causes denial of service. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-14613	A vulnerability was discovered in Keycloak's administrative interface that allows certain administrators to see information about groups they shouldn't have access to. When the new Fine-Grained Admin Permissions (FGAP v2) are turned on, an administrator who is allowed to see a specific "role" can also see a list of all groups assigned to that role. The system fails to check if the administrator has permission to see those specific groups. This could allow a restricted administrator to discover "hidden" groups and see their details, such as internal names and custom settings, which might contain sensitive deployment information.	4.3	More Details
CVE-2026-14615	A flaw was found in the Fine-Grained Admin Permissions (FGAP) v2 implementation within Keycloak's administrative services. When FGAP v2 is enabled, the system fails to properly filter child groups based on the caller's specific permissions when requested through a parent group. This allows a delegated administrator to view details of child groups they are not authorized to access directly, including group names, paths, and custom attributes.	4.3	More Details
CVE-2026-14608	A security vulnerability has been detected in SourceCodester CET Automated Grading System with AI Predictive Analytics 1.0. This vulnerability affects unknown code of the file /index.php?action=view_student of the component POST Handler. The manipulation of the argument ID leads to authorization bypass. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2026-14611	A vulnerability has been found in DeepMyst Mysti up to 0.4.0. The affected element is the function initProjectMemory of the file src/managers/MemoryManager.ts of the component Per-Project Auto-Memory Handler. Such manipulation of the argument workspacePath leads to exposure of resource. The attack may be performed from remote. Upgrading to version 0.4.0 is sufficient to fix this issue. The name of the patch is 6d709229b5199f6769fb3cf763e5122dcc43c079. It is advisable to upgrade the affected component.	4.3	More Details
CVE-2026-14624	A vulnerability was identified in omec-project amf up to 2.0.2/2.1.1. Impacted is an unknown function of the file /go/src/amf/ngap/handler.go of the component NGSetupRequest Handler. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. The identifier of the patch is 34bc6724acc97dba1f8691e586da95b042cb612d. To fix this issue, it is recommended to deploy a patch.	4.3	More Details
CVE-2026-14623	A vulnerability was determined in omec-project amf up to 2.1.1. This issue affects the function RRCInactiveTransitionReport of the component NGAP Message Handler. Executing a manipulation can lead to denial of service. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. This patch is called 34bc6724acc97dba1f8691e586da95b042cb612d. A patch should be applied to remediate this issue.	4.3	More Details
CVE-2026-12729	The weDocs: AI Powered Knowledge Base, Docs, Documentation, Wiki & AI Chatbot plugin for WordPress is vulnerable to Missing Authorization in versions up to and including 2.3.0. This is due to a missing capability check on the do_migration() function registered as the wedocs_migrate_betterdocs_to_wedocs AJAX action, which performs no nonce verification via check_ajax_referer() and no capability check via current_user_can() before executing sensitive operations. This makes it possible for authenticated attackers, with Subscriber-level access and above, to trigger a full BetterDocs-to-weDocs data migration, creating and modifying 'docs' custom post type entries with attacker-controlled titles, updating site options, and deactivating the BetterDocs and BetterDocs Pro plugins via deactivate_plugins().	4.3	More Details
CVE-2026-27783	Gitea versions up to and including 1.26.1 do not enforce repository-unit authorization on issue-template API endpoints.	4.3	More Details
CVE-2026-25714	Gitea versions up to and including 1.26.1 do not apply public-only token filtering consistently to the user organization API, leaving an incomplete fix for CVE-2025-68941.	4.3	More Details

CVE-2026-14618	A vulnerability was detected in Open5GS up to 2.7.7. Affected by this vulnerability is the function amf_nnrf_handle_nf_discover of the file src/amf/nnrf-handler.c of the component AMF. The manipulation results in denial of service. The attack may be launched remotely. The exploit is now public and may be used. The patch is identified as fb5f67703de0213fb9c6e6ef3b48b6c1707e9503. It is best practice to apply a patch to resolve this issue.	4.3	More Details
CVE-2026-8482	A vulnerability was discovered on StormShield Network Security 4.3.0 to 4.3.41 (included), 4.8.0 to 4.8.15 (included) , 5.0.0 to 5.0.5 (included) There is a possible leak of secret information if administration commands have been passed with the CLI command line tool. Someone with SSH access to the firewall (if SSH multiuser mode is enabled) could possibly get the proxy CA passphrase or TPM password.	4.3	More Details
CVE-2026-14704	A vulnerability was found in stephen-kruger bluebox up to 4.5.12. Affected by this vulnerability is an unknown functionality. Performing a manipulation of the argument code results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report.	4.3	More Details
CVE-2026-27761	Gitea versions up to and including 1.26.2 allow repository RSS and Atom feed endpoints to bypass API access token scope checks, exposing private repository commit data to tokens without the required repository scope.	4.3	More Details
CVE-2026-58597	Insufficient ui warning of dangerous operations in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	4.3	More Details
CVE-2026-14410	Inappropriate implementation in Skia in Google Chrome prior to 150.0.7871.46 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-54259	Wagtail is an open source content management system built on Django. In versions prior to 7.0.8, 7.3.3 and 7.4.2, the Documents and Images chooser's chosen endpoint incorrectly listed items for which the user has not been granted choose permission. A user with access to the Wagtail admin could see the filename and name and URLs of documents and images in those collections. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. This issue has been fixed in versions 7.0.8, 7.3.3, and 7.4.2.	4.3	More Details
CVE-2026-54260	Wagtail is an open source content management system built on Django. In versions prior to 7.0.8, 7.3.3 and 7.4.2, an authenticated admin user can trigger expensive rendition processing with purposefully crafted filter specs resulting in potentially service degradation. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. This issue has been fixed in versions 7.0.8, 7.3.3, and 7.4.2.	4.3	More Details
CVE-2026-58653	PraisonAI before 0.1.7 fails to validate that project_id in issue create and update request bodies belongs to the URL workspace. An attacker can create issues referencing projects from other workspaces, causing cross-tenant data pollution in project statistics aggregation without workspace constraints.	4.3	More Details
CVE-2026-53422	Observable Response Discrepancy vulnerability in Erlang OTP ssh (ssh_sftpd module) allows an authenticated SFTP user to enumerate the existence of files and directories outside the configured root directory. The SSH_FXP_REALPATH handler in ssh_sftpd calls relate_file_name/3 with Canonicalize=false, unlike every other SFTP operation handler. This allows .. components in the requested path to bypass the is_within_root/2 check without being resolved. The un-canonicalized path then enters resolve_symlinks/2, which walks up the directory tree above the configured root and issues read_link() syscalls on arbitrary filesystem paths. An authenticated SFTP client can exploit this by sending a REALPATH request with a crafted traversal path. The server response differs depending on whether the target path exists on the host filesystem (SSH_FXP_NAME when the path resolves successfully, SSH_FX_NO_SUCH_FILE when it does not). This creates a path-existence oracle that an attacker can use to enumerate the filesystem structure outside the configured root, including the existence of sensitive files, directories, and mount points. The vulnerability leaks only the existence of paths. No file contents, credentials, or write access are obtainable through this issue alone. The information gained may assist further attacks when combined with other vulnerabilities. This vulnerability is associated with program files lib/ssh/src/ssh_sftpd.erl and program routine ssh_sftpd:handle_op/4. This issue affects OTP from OTP 17.0 until OTP 29.0.3, 28.5.0.3, and 27.3.4.14 corresponding to ssh from 3.0.1 until 6.0.2, 5.5.2.2, and 5.2.11.9.	4.3	More Details
CVE-2026-	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in Erlang OTP ssh (ssh_sftpd module) allows an authenticated SFTP user to render an SFTP channel permanently unresponsive. The handle_data/4 function in ssh_sftpd contains a catch-all clause that accepts channel data of any type. When channel data with a non-zero type code (SSH_MSG_CHANNEL_EXTENDED_DATA) arrives with an empty pending buffer and a payload at or below the SFTP packet size limit, the clause tail-calls itself with identical arguments, creating an infinite loop. The SFTP protocol operates exclusively on normal channel data (type 0). Extended data (non-zero type) is meaningless for SFTP and is never sent by conforming clients. However, the SSH protocol permits any channel participant to send extended data on an open channel, so an authenticated SFTP client can trigger the loop by sending SSH_MSG_CHANNEL_EXTENDED_DATA with any data_type_code and any non-empty payload at or below the size limit. The targeted ssh_sftpd process enters an infinite tail-recursive loop. It never processes another message, its message queue grows without bound, and it can only be stopped by	4.3	More

54886	killing the process. BEAM's reduction-based scheduler preemption continues to function, so other processes on the node are not starved, but each stuck channel process consumes its full CPU time share continuously and accumulates unbounded message queue memory. Opening many channels amplifies the CPU and memory impact. Erlang/OTP SSH configurations using the default max_channels setting (infinity) allow an authenticated user to open unlimited channels per connection, amplifying the attack without requiring multiple TCP connections or authentications. No file contents, credentials, or write access are obtainable through this issue. The impact is limited to denial of service on targeted SFTP channels, with secondary CPU degradation and memory growth. This vulnerability is associated with program file lib/ssh/src/ssh_sftpd.erl and program routine ssh_sftpd:handle_data/4. This issue affects OTP from OTP 17.0 until OTP 29.0.3, 28.5.0.3, and 27.3.4.14 corresponding to ssh from 3.0.1 until 6.0.2, 5.5.2.2, and 5.2.11.9.		Details
CVE-2026-54262	Wagtail is an open source content management system built on Django. In versions prior to 7.0.8, 7.3.3 and 7.4.2, a low-level user with the "Can submit translation" permission can create translations for any page, including those they do not have permissions for. This issue has been fixed in versions 7.0.8, 7.3.3, and 7.4.2.	4.3	More Details
CVE-2026-14612	Two off-by-one errors in the FreeIPA ipa-otpd daemon's OAuth2 device authorization handler can cause out-of-bounds memory access when processing an oversized response from a configured external OAuth2/OIDC Identity Provider. An attacker who controls or can man-in-the-middle the IdP endpoint may be able to trigger ipa-otpd to write or read one byte past the end of a fixed-size buffer. Exploitation requires FreeIPA to be configured with an external IdP, attacker control or MITM of that IdP, and a user to initiate the OAuth2 device authorization flow. The most likely impact is limited denial of service affecting the ipa-otpd daemon.	4.2	More Details
CVE-2026-11570	The User Submitted Posts WordPress plugin before 20260608 does not escape a submitted value before outputting it in an admin-configured display template, leading to a Stored Cross-Site Scripting that can be triggered by unauthenticated users when a non-default display option is enabled.	4.2	More Details
CVE-2026-50179	Actual is a local-first personal finance tool. Prior to 26.6.0, exportToCSV and exportQueryToCSV in packages/loot-core/src/server/transactions/export/export-to-csv.ts pass user-controlled Payee, Notes, Account, and Category strings to csv-stringify with no cast callback and no formula-prefix neutralization. Strings that begin with equals sign, plus, minus, at sign, tab, or carriage return survive verbatim into the exported CSV, and when a recipient opens the file in Excel, LibreOffice Calc, or Google Sheets, the strings are interpreted as formulas, enabling transaction data exfiltration and attacker-chosen spreadsheet display values. This issue is fixed in version 26.6.0.	4.2	More Details
CVE-2026-46730	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an incorrect authorization vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to unauthorized command execution.	4.2	More Details
CVE-2026-55945	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Edge (Chromium-based) allows an authorized attacker to disclose information locally.	4.2	More Details
CVE-2026-13323	In Open VSX Registry before 1.0.2, the /vscode/unpkg/ endpoint serves user-supplied HTML files with Content-Type: text/html and without a Content-Security-Policy or Content-Disposition: attachment response header. An unauthenticated attacker can register a publisher account, upload a VSIX containing a crafted HTML payload, and induce an authenticated user to visit the resulting URL. The browser renders the file inline in the open-vsx.org origin context, enabling session token exfiltration, persistent Personal Access Token (PAT) generation, and unauthorized publication of malicious extension versions. Because Open VSX extensions are distributed to VS Code, VSCodium, Cursor, Windsurf, and compatible editors, a compromised extension update constitutes a supply chain attack against all downstream users.	4.1	More Details
CVE-2026-13199	EEPROM firmware on Raspberry Pi 5 and Compute Module 5 devices produced non-random KASLR and RNG seed values. This resulted in consistent kernel addresses across boots and devices, potentially making it easier to exploit other vulnerabilities. Additionally, the low-quality RNG seed may affect the quality of random numbers or delay booting while sufficient entropy is accumulated from other sources.	4.0	More Details
CVE-2026-55688	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. In versions from 2.0.0 prior to 2.16.0 and from 3.0.0.Beta1 prior to 3.0.11, ThreadSafeCookieStore stored a cookie under the value of its Domain attribute without verifying that the responding host is allowed to set a cookie for that domain, leading to a cookie tossing / cookie injection issue. A host the client connects to can therefore plant a cookie scoped to an unrelated domain, and the client will then send that cookie on later requests to that domain. Applications that use a single AsyncHttpClient instance - and thus the default, shared CookieStore - to reach both an attacker-influenced host and a trusted host are impacted. This issue has been fixed in versions 2.16.0 and 3.0.11.	4.0	More Details
CVE-2026-55592	Dashy is a self-hostable personal dashboard. Prior to 4.3.7, Dashy's workspace view trusts the url query parameter and assigns it directly to an iframe source without scheme validation. If a logged-in user opens a crafted workspace link containing a javascript: URL, JavaScript runs on the Dashy origin and can read same-origin browser data, interact with the Dashy DOM, and send requests as the victim. This issue is fixed in version 4.3.7.	3.9	More Details

CVE-2026-12386	Improper null termination vulnerability in TUBITAK BILGEM Software Technologies Research Institute Pardus Pen allows Overflow Buffers. This issue affects Pardus Pen: from <=4.1.5 before 4.2.1.	3.9	More Details
CVE-2026-42148	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, the buildHelperImage method in app/Livewire/Settings/Index.php constructs a Docker build command using the dev_helper_version field without shell escaping, allowing an attacker who can set the helper version and trigger the helper image build in a development environment to execute arbitrary commands on the server. This issue is fixed in version 4.0.0-beta.474.	3.8	More Details
CVE-2026-42546	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 3.3.0 and prior to version 4.11.0, a resource leak exists in OP-TEE's shared memory cleanup logic because the function `cleanup_shm_refs()` in `core/tee/entry_std.c` fails to apply a required bitmask (`OPTEE_MSG_ATTR_TYPE_MASK`) to parameter attributes. When processing non-contiguous memory parameters from a normal-world caller, the system fails to match the attribute type in its internal switch statement and skips the necessary mobj_put() call. This results in a persistent reference leak of `mobj_reg_shm` objects, which remain on internal lists with dangling refcounts. This affects non-FF-A configurations that support non-contiguous, non-secure shared memory. Over time, these accumulated leaks progressively consume the secure-world heap, degrading the system's ability to service trusted application operations and eventually requiring a reboot to recover. Version 4.11.0 contains a patch. No known workarounds are available.	3.8	More Details
CVE-2026-54891	Improper Enforcement of Message Integrity During Transmission in a Communication Channel vulnerability in Erlang/OTP ssl (tls_gen_connection module) allows a network-positioned attacker to inject unauthenticated plaintext that the TLS client application later treats as authenticated server data. The function tls_gen_connection:handle_protocol_record/3 rejects APPLICATION_DATA records that arrive in pre-handshake states when the TLS endpoint acts as a server, but does not apply the same check when the endpoint acts as a client. A network-positioned attacker can send plaintext APPLICATION_DATA records to the client during the handshake. The records are buffered and, once the handshake completes successfully, delivered to the application as if they were authenticated post-handshake data. The attacker cannot observe the client's response or steer the connection, so the impact is limited to blind injection of unauthenticated bytes. The injection window is wider for TLS versions prior to TLS 1.3 than for TLS 1.3. This vulnerability is associated with program file lib/ssl/src/tls_gen_connection.erl. This issue affects OTP from OTP 17.0 before 29.0.3, 28.5.0.3 and 27.3.4.14 corresponding to ssl from 5.3.4 before 11.7.3, 11.6.0.3 and 11.2.12.10. TLS 1.3 is affected starting with OTP 22.0, when TLS 1.3 support was added.	3.7	More Details
CVE-2026-10657	Zephyr's DNS resolver detects mDNS (.local) queries in dns_resolve_name_internal() (subsys/net/lib/dns/resolve.c) with memcmp(strrchr(query, '.'), ".local", 7), which always reads a fixed 7 bytes from the suffix pointer. When the resolved hostname's final label is shorter than 7 bytes (e.g. names ending in .org, .com, .net, .io, or a trailing dot), the comparison reads 1-2 bytes past the string's NUL terminator. The hostname (query) is the caller-supplied name passed through the standard getaddrinfo()/dns_get_addr_info()/dns_resolve_name() path and is influenceable by operators or remote inputs (server names from configuration, parsed URLs, or app-facing interfaces). On a tightly-sized buffer with no slack (for example a userspace getaddrinfo call where the hostname is copied with k_usermode_string_alloc_copy to exactly strlen+1 bytes), the over-read crosses the allocation boundary; if that boundary is unmapped (guard page, memory-domain boundary under MPU, or an address sanitizer) the over-read faults, causing a denial of service. The over-read bytes are never returned, so there is no information disclosure. The flaw is compiled only when CONFIG_MDNS_RESOLVER is enabled, exists since v1.10.0, and is fixed by replacing the fixed-length memcmp with a NUL-safe strcmp(ptr, ".local").	3.7	More Details
CVE-2026-14935	A logic vulnerability was found in GStreamer's webrtcbin component. The _check_sdp_crypto() function contains an inverted boolean condition that causes it to accept remote SDP offers or answers that lack the required a=fingerprint attribute, while incorrectly rejecting those that include it. An attacker with the ability to intercept and modify WebRTC signaling messages could exploit this to bypass the SDP-level DTLS certificate fingerprint binding, weakening defenses against man-in-the-middle attacks on media streams.	3.7	More Details
CVE-2026-46584	Improper Input Validation, Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Camel Mail Component. The camel-mail producer (MailProducer.getSender) scanned the outgoing Exchange for message headers in the mail.smtp. / mail.smtps. namespace and, when any were present, built a per-message JavaMail sender with those values applied as JavaMail session properties, overriding the endpoint configuration. This namespace is Camel-internal - only MailProducer interprets it - and was not blocked by any HeaderFilterStrategy, so the values could originate from any inbound protocol (for example platform-http query parameters or request headers, or JMS / Kafka messages from untrusted producers) that feeds a route ending in an smtp / smtps producer without an intervening removeHeaders. The maximal impact is version-dependent: on releases before 4.19.0, setting mail.smtp.host redirects the SMTP connection to a server under the attacker's control, and because the producer then authenticates with the endpoint's configured username and password those credentials are transmitted to the attacker; on 4.19.0 and later the producer connects to the endpoint's configured host explicitly, so the reachable impact is limited to weakening transport security (for example mail.smtp.ssl.trust, mail.smtp.starttls.enable or mail.smtp.socks.host) and interception of the	3.7	More Details

	outgoing message rather than host redirect. Exploitation requires a route that channels untrusted input into the mail producer without stripping the namespace. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, the per-message override is disabled by default; enable it only on trusted endpoints with useJavaMailSessionPropertiesFromHeaders=true. For deployments that cannot upgrade immediately, strip the namespace before the mail producer with removeHeaders('mail.smtp.*') and removeHeaders('mail.smtps.*') between any untrusted ingress and the smtp / smtps producer. Even with the opt-in enabled, route authors should still strip the namespace on any path that carries untrusted input.		
CVE-2026-44042	UltraVNC repeater through 1.8.2.2 contains an off-by-one error in the Base64 decode helper used for HTTP Basic authentication. In repeater/webgui/webutils.c:817, the wi_uudecode() function checks whether the input length exceeds the output buffer with a strict greater-than comparison (>), while the correct check should be greater-than-or-equal (>=). When strlen(authdata) equals sizeof(decode), the decoded output length (approximately 3/4 of input) does not overflow the buffer in current practice because the outer HTTP request bounds constrain the Authorization header. However, the defective check leaves a latent off-by-one condition that could become exploitable if the buffering constraints change. The current risk is limited to a one-byte write at the boundary of a 1024-byte stack buffer under constrained conditions.	3.7	More Details
CVE-2026-14738	A security flaw has been discovered in exo-explore exo up to 1.0.71. Affected is the function _image_cache_key of the file src/exo/worker/engines/mlx/vision.py of the component Vision Feature Cache. The manipulation results in use of weak hash. It is possible to launch the attack remotely. A high complexity level is associated with this attack. The exploitability is told to be difficult. The exploit has been released to the public and may be used for attacks. The pull request to fix this issue awaits acceptance.	3.7	More Details
CVE-2026-14791	A weakness has been identified in crater-invoice-inc crater up to 6.0.6. This affects the function getFormattedString of the file app/Http/Requests/InvoicesRequest.php of the component Invoice Note Handler. Executing a manipulation of the argument notes can lead to cross site scripting. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	3.5	More Details
CVE-2026-14752	A security vulnerability has been detected in mjperpinosa stumasy up to 327d1b0f2915ba79d7ef8ebb74553e987609d9be. This affects the function add_definition of the file application/PHP/objects/notes/add_into_dictionary.php. Such manipulation of the argument reference leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	3.5	More Details
CVE-2025-13475	In multi-tenanted deployments, the application consent management mechanism fails to correctly isolate consent scopes between tenants. Consent granted by a user for a specific SaaS application within one tenant can be incorrectly applied to SaaS applications with the same name in other tenants, leading to unintended cross-tenant consent sharing. This vulnerability may result in the exposure of user data across tenants, enabling SaaS applications in different tenants to access and modify information without explicit user authorization. This can lead to unauthorized data access and privacy violations. This vulnerability has no impact if the deployment does not support multi-tenancy.	3.5	More Details
CVE-2026-41434	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 3.10.0 and prior to version 4.11.0, an unbounded recursion can crash the PKCS#11 TA. Version 4.11.0 contains a patch. No known workarounds are available.	3.3	More Details
CVE-2026-34049	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. From 4.0.0-beta.451 through 4.0.0-beta.470, database backup handling for MongoDB collection names did not fully validate shell metacharacters, allowing a highly privileged attacker who can configure backup inputs to inject commands. This issue is fixed in version 4.0.0-beta.471.	3.3	More Details
CVE-2026-56085	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an use of uninitialized resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to information exposure.	3.3	More Details
CVE-2025-15667	A vulnerability was determined in GPAC up to 2.5-DEV. This vulnerability affects the function gf_isom_nalu_sample_rewrite of the file src/isomedia/avc_ext.c of the component MP4Box. This manipulation of the argument nalu_out_bs causes double free. It is possible to launch the attack on the local host. The exploit has been publicly disclosed and may be utilized. Patch name: f29f955f2a3b5e8e507caad3e52319f961bf37bf. To fix this issue, it is recommended to deploy a patch.	3.3	More Details
CVE-2026-	A security flaw has been discovered in radareorg radare2 up to 6.1.6. This impacts the function r_str_word_get0set of the file libr/util/str.c. The manipulation results in integer overflow. The attack must be initiated from a local position. The exploit has been released to the public and may be used for attacks. The	3.3	More

14786	patch is identified as 11ac224c0eb8d57830fccc99e1c1cd8e5d958813. It is best practice to apply a patch to resolve this issue.		Details
CVE-2026-14787	A weakness has been identified in radareorg radare2 up to 6.1.6. Affected is the function cmd_print in the library libr/core/cmd_print.inc of the component pb Print Command Handler. This manipulation causes integer overflow. The attack needs to be launched locally. The exploit has been made available to the public and could be used for attacks. Patch name: 2b6265476c75567006b0fcbb749f4ae7b189c5df. It is recommended to apply a patch to fix this issue.	3.3	More Details
CVE-2025-15668	A vulnerability was identified in GPAC up to b40ce70f5. This issue affects the function sgpd_del_entry of the file src/isomedia/box_code_base.c of the component MP4Box. Such manipulation of the argument data leads to heap-based buffer overflow. Local access is required to approach this attack. The exploit is publicly available and might be used. The name of the patch is f29f955f2a3b5e8e507caad3e52319f961bf37bf. It is advisable to implement a patch to correct this issue.	3.3	More Details
CVE-2026-14788	A security vulnerability has been detected in radareorg radare2 up to 6.1.6. Affected by this vulnerability is the function r_core_bin_load of the file libr/core/cfile.c. Such manipulation leads to use after free. The attack needs to be performed locally. The exploit has been disclosed publicly and may be used. The name of the patch is 635ab1eeb30340c26076722a90cb91fb2272130b. Applying a patch is advised to resolve this issue.	3.3	More Details
CVE-2026-14684	A flaw has been found in HdrHistogram up to 2.2.2. This affects the function org.HdrHistogram.AbstractHistogram.decodeFromByteBuffer of the file src/main/java/org/HdrHistogram/AbstractHistogram.java. This manipulation of the argument numberOfSignificantValueDigits causes uncontrolled memory allocation. The attack can only be executed locally. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-42201	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, database credential fields (redis_password, keydb_password, dragonfly_password, clickhouse_admin_user, clickhouse_admin_password, postgres_user, mysql_user) are validated only as 'string' at the API layer, with zero shell-safety checks. These values are then interpolated directly into Docker Compose YAML command: strings without any escaping. This issue is fixed in version 4.0.0-beta.474.	3.3	More Details
CVE-2026-14761	A security vulnerability has been detected in radareorg radare2 up to 6.1.6. The affected element is the function r_str_ndup/r_str_append of the file libr/util/str.c. The manipulation leads to integer overflow. An attack has to be approached locally. The exploit has been disclosed publicly and may be used. The identifier of the patch is a20a56917ae85d732e683f8d9078bdcfee92446c. Applying a patch is the recommended action to fix this issue.	3.3	More Details
CVE-2026-14760	A weakness has been identified in radareorg radare2 up to 6.1.6. Impacted is the function r_core_seek_arch_bits of the file libr/core/disasm.c of the component regprofile Handler. Executing a manipulation can lead to use after free. The attack requires local access. The exploit has been made available to the public and could be used for attacks. This patch is called 8b25c773785d85cb0103410a0905089d286921c2. It is advisable to implement a patch to correct this issue.	3.3	More Details
CVE-2026-14699	A weakness has been identified in zcaceres markdownify-mcp up to 1.1.0. The affected element is the function assertPathAllowed of the file src/Markdownify.ts. Executing a manipulation can lead to symlink following. The attack can only be executed locally. The pull request to fix this issue awaits acceptance.	3.3	More Details
CVE-2026-14759	A security flaw has been discovered in radareorg radare2 up to 6.1.6. This issue affects the function r_bin_java_inner_classes_attr_calc_size of the file shlr/java/class.c of the component RBinJava Line Number Table Parser. Performing a manipulation results in heap-based buffer overflow. The attack requires a local approach. The exploit has been released to the public and may be used for attacks. The patch is named cd62d15a6cbecdc67fd03f3ebdbbbeb741d18f87. To fix this issue, it is recommended to deploy a patch.	3.3	More Details
CVE-2026-14801	A security vulnerability has been detected in GPAC 26.03-DEV-rev342-g80071f700-master. The impacted element is the function txtin_probe_duration of the file src/filters/load_text.c of the component TeXML File Handler. Such manipulation of the argument txml_timescale leads to divide by zero. An attack has to be approached locally. The name of the patch is 86a5191f2e750c767253e27ed6cfd6d547afebc2. A patch should be applied to remediate this issue.	3.3	More Details
CVE-2026-14686	A vulnerability was found in HdrHistogram up to 2.2.2. This issue affects the function org.HdrHistogram.DoubleHistogram.recordValue of the file src/main/java/org/HdrHistogram/DoubleHistogram.java of the component Range Check. Performing a manipulation results in incorrect comparison. The attack is only possible with local access. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, DatabaseBackupJob interpolates user-controlled database credentials and MongoDB collection exclusion names into backup shell commands without adequate escaping, allowing an	3.3	More Details

34149	authenticated user with database management permissions to execute commands on managed servers. This issue is fixed in version 4.0.0-beta.471.		
CVE-2026-14685	A vulnerability has been found in HdrHistogram up to 2.2.2. This vulnerability affects the function recordValueWithCount of the file src/main/java/org/HdrHistogram/AbstractHistogram.java of the component AbstractHistogram. Such manipulation of the argument Count leads to state issue. The attack can only be performed from a local environment. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-14683	A vulnerability was detected in HdrHistogram up to 2.2.2. Affected by this issue is the function org.HdrHistogram.AbstractHistogram.decodeFromCompressedByteBuffer of the file src/main/java/org/HdrHistogram/AbstractHistogram.java. The manipulation of the argument lengthOfCompressedContents results in uncontrolled memory allocation. The attack needs to be approached locally. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-14790	A flaw has been found in GPAC 26.02.0. This affects the function nhmldump_send_frame of the file src/filters/write_nhml.c of the component Media File Handler. Executing a manipulation can lead to null pointer dereference. The attack requires local access. The exploit has been published and may be used. This patch is called bd1d94e70e3bef364c07c5a1d94eca5c9f56e160. A patch should be applied to remediate this issue. The project explains: "I would consider most of these more as bugs than vulns but anyway they're good to fix".	3.3	More Details
CVE-2026-14789	A vulnerability was detected in radareorg radare2 up to 6.1.6. Affected by this issue is some unknown functionality of the file libr/bin/format/mdmp/mdmp.c of the component Memory64ListStream Parser. Performing a manipulation results in stack-based buffer overflow. The attack requires a local approach. The exploit is now public and may be used. The patch is named 175d4addb68981331c85b10681c2161c38fb5762. It is suggested to install a patch to address this issue.	3.3	More Details
CVE-2026-14758	A vulnerability was identified in radareorg radare2 up to 6.1.6. This vulnerability affects the function cmd_anal_opcode of the file libr/core/cmd_anal.inc.c of the component hexpairs Parser. Such manipulation leads to integer overflow. The attack needs to be performed locally. The exploit is publicly available and might be used. The name of the patch is 84e773986e7e5bb30453a9384f498ec0ccc9d0a9. A patch should be applied to remediate this issue.	3.3	More Details
CVE-2026-14651	A vulnerability has been found in connorskees grass up to 0.13.4. The impacted element is the function grass_compiler::selector::extend/grass_compiler::evaluate::visitor. The manipulation leads to denial of service. The attack must be carried out locally. The exploit has been disclosed to the public and may be used. The project maintainer explains: "DoS vulnerabilities are generally fine in Sass compilers -- they are trivially possible with recursive functions, infinite loops, nested mixins, etc. The description here is wrong. Compile time is not expected to be linear relative to the input, and the @extend algorithm is definitionally exponential."	3.3	More Details
CVE-2026-14650	A flaw has been found in connorskees grass up to 0.13.4. The affected element is the function grass_compiler::raw_to_parse_error of the component UTF-8 Character Handler. Executing a manipulation can lead to denial of service. The attack is restricted to local execution. The exploit has been published and may be used. In Issue #117 with similar structure the project maintainer explains: "DoS vulnerabilities are generally fine in Sass compilers -- they are trivially possible with recursive functions, infinite loops, nested mixins, etc. The description here is wrong. Compile time is not expected to be linear relative to the input, and the @extend algorithm is definitionally exponential."	3.3	More Details
CVE-2026-41579	runc is a CLI tool for spawning and running containers according to the OCI specification. In versions prior to 1.3.6, 1.4.0-rc.1, 1.4.0-rc.12, 1.5.0-rc.1, and 1.5.0-rc.1, when setting up the container rootfs, setupPtmx and setupDevSymlinks call os.Remove and os.Symlink with a filepath.Join string which allow an image with /dev as a symlink to trick runc into deleting files called ptmx on the host or creating a hardcoded set of symlinks with specific names and targets in an arbitrary pre-existing host directory. This issue is not exploitable under Docker, because Docker creates a top-level read-only layer that masks any malicious /dev symlink present in the container image — unlike some other Linux container tooling, whose higher-level runtimes built on runc remain exposed to exploitation via a malicious image. This issue has been fixed in versions 1.3.6, 1.4.3 and 1.5.0.	3.3	More Details
CVE-2026-48588	An issue was discovered in Django 6.0 before 6.0.7 and 5.2 before 5.2.16. `UpdateCacheMiddleware` and the `cache_page()` decorator cache responses that vary on cookies when the incoming request carries unrelated cookies, which allows remote attackers to read private data from the shared cache. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Chris Whyland for reporting this issue.	3.1	More Details
CVE-2026-11880	The Fluent Forms WordPress plugin before 6.2.1 does not properly verify ownership before processing a subscription cancellation request, allowing authenticated users with a low-privilege account to cancel subscriptions belonging to other users.	3.1	More Details
	A vulnerability was determined in langchain-ai langgraph up to 1.2.4. The affected element is the function		

CVE-2026-14742	_freeze of the file libs/langgraph/langgraph/_internal/_cache.py of the component Task Result Cache. This manipulation of the argument default_cache_key causes use of weak hash. The attack is possible to be carried out remotely. The complexity of an attack is rather high. The exploitability is described as difficult. The exploit has been publicly disclosed and may be utilized. The pull request to fix this issue awaits acceptance.	3.1	More Details
CVE-2026-42145	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, the file upload endpoint (app/Http/Controllers/UploadController.php) for database backup restore uploads did not enforce file type or size validation, allowing an authenticated user to upload unexpected or oversized files that could affect service availability. This issue is fixed in version 4.0.0-beta.474.	3.1	More Details
CVE-2026-14621	A vulnerability has been found in FederatedAI FATE up to 2.2.0. This affects the function QueuePushReqStreamObserver.initEggroll of the file java/osx/osx-broker/src/main/java/org/fedai/osx/broker/grpc/QueuePushReqStreamObserver.java of the component OSX Broker. Such manipulation of the argument rollSiteSessionId/dstRole/dstPartyId leads to exposure of data element to wrong session. The attack can be executed remotely. A high complexity level is associated with this attack. It is indicated that the exploitability is difficult. The exploit has been disclosed to the public and may be used. The pull request to fix this issue awaits acceptance.	3.1	More Details
CVE-2026-42172	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, Sanctum API tokens did not expire, allowing a leaked token to retain access indefinitely until manually revoked. This issue is fixed in version 4.0.0-beta.474.	3.1	More Details
CVE-2026-14630	A vulnerability has been found in ForceInjection AI-fundermentals 2.0/3.0. Affected by this vulnerability is the function get_conversation_history of the file 08_agentic_system/memory/langchain/code/smart_customer_service.py of the component Memory Recall Handler. The manipulation leads to use of weak hash. Remote exploitation of the attack is possible. A high degree of complexity is needed for the attack. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier of the patch is f57277fdd9ba373ace72d83c272023ec67f720d6. It is suggested to install a patch to address this issue. The project confirms (translated from Chinese): "We now require session ownership verification in methods such as `username`, `sessionowner`, etc., and we've chat()changed the generation of `sessionowner` to include verified user identity and security context metadata."	3.1	More Details
CVE-2026-28378	The public dashboard deletion endpoint does not enforce organization isolation, allowing an Org Admin in one organization to delete public dashboards belonging to a different organization by supplying the target dashboard's identifiers.	3.1	More Details
CVE-2026-14617	A security vulnerability has been detected in NousResearch hermes-agent up to 2026.4.30. Affected is the function GatewayStreamConsumer._filter_and_accumulate of the file gateway/stream_consumer.py of the component Streaming Reasoning Tag Filter. The manipulation leads to improper handling of case sensitivity. The attack may be initiated remotely. The attack's complexity is rated as high. The exploitability is told to be difficult. The exploit has been disclosed publicly and may be used. The project decided to not implement a dedicated fix: "[T]he analysis and the fix are both sound. It just lands below the bar for the maintenance cost of a duplicated scrub path."	3.1	More Details
CVE-2026-27844	Uncaught Exception (CWE-248) in the Controller 6000 and Controller 7000 diagnostic web interface allows an authenticated and authorized operator to trigger a Controller restart by sending specific requests, resulting in a temporary denial of service. Version of Command Centre affected: * 9.50 prior to vCR9.50.260616a (distributed in 9.50.1587(MR1)) * 9.40 prior to vCR9.40.260616a (distributed in 9.40.3130(MR3)) * 9.30 prior to vCR9.30.260616a (distributed in 9.30.3983(MR5)) * 9.20 prior to vCR9.20.260616a (distributed in 9.20.4349(MR7)) * all versions of 9.10 and prior.	2.7	More Details
CVE-2026-11578	The Fluent Forms WordPress plugin before 6.2.5 does not properly restrict the deletion of form submission entries to the forms a restricted Manager is authorized to manage, allowing a Manager limited to specific forms to permanently delete submission entries belonging to other forms. This requires a non-default configuration in which an administrator has created at least one Manager restricted to specific forms.	2.7	More Details
CVE-2026-27790	Uncaught Exception (CWE-248) in the T20 Readers allows an authenticated and authorized operator to trigger a restart by sending specific requests, resulting in a temporary denial of service. Version of Command Centre affected: * 9.50 prior to vCR9.50.260616a (distributed in 9.50.1587(MR1)) * 9.40 prior to vCR9.40.260616a (distributed in 9.40.3130(MR3)) * 9.30 prior to vCR9.30.260616a (distributed in 9.30.3983(MR5)) * 9.20 prior to vCR9.20.260616a (distributed in 9.20.4349(MR7)) * all versions of 9.10 and prior.	2.7	More Details
CVE-2026-46466	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an use of less trusted source vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to information tampering.	2.7	More Details
	The Adminify WordPress plugin before 4.2.10 does not perform per-user read-capability checks on the results		

CVE-2026-11781	returned by one of its administration search features, allowing users with a low-privilege role (Contributor) to disclose non-public content that WordPress would not otherwise expose to them, such as other authors' unpublished post titles, pending comment content, the site's Adminify WordPress plugin before 4.2.10 inventory, and user account names.	2.7	More Details
CVE-2026-41515	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 3.9.0 and prior to version 4.11.0, the RSA-OAEP decryption implementation in the NXP CAAM crypto driver uses non-constant-time `memcmp()` for label hash verification and has multiple distinguishable error paths. This creates a Manger-style padding oracle that allows an attacker to recover RSA-OAEP plaintext with approximately 1000-2000 adaptive chosen ciphertext queries. Version 4.11.0 contains a patch. As a workaround, disable the NXP CAAM RSA driver with `CFG_CRYPTO_DRV_RSA=n`.	2.5	More Details
CVE-2026-14702	A flaw has been found in zcaceres markdownify-mcp up to 1.1.0. This impacts the function saveToTempFile of the file src/Markdownify.ts of the component webpage-to-markdown/youtube-to-markdown/bing-search-to-markdown. This manipulation causes insufficiently random values. The attack is restricted to local execution. A high degree of complexity is needed for the attack. The exploitability is said to be difficult. The exploit has been published and may be used. The pull request to fix this issue awaits acceptance.	2.5	More Details
CVE-2026-41514	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 4.5.0 and prior to version 4.11.0, the RSA-OAEP decryption implementation in the Hisilicon HPRE crypto driver uses non-constant-time `memcmp()` for label hash verification and has multiple distinguishable error paths. This creates a Manger-style padding oracle that allows an attacker to recover RSA-OAEP plaintext with approximately 1000-2000 adaptive chosen ciphertext queries. Only affects plat-d06 with `CFG_HISILICON_ACC_V3=y`, which seems to be disabled by default. Version 4.11.0 contains a patch. As a workaround, disable Hisilicon HPRE RSA driver with `CFG_HISILICON_ACC_V3=n`.	2.5	More Details
CVE-2026-41516	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 4.5.0 and prior to version 4.11.0, the RSA PKCS#1 v1.5 decryption implementation in the Hisilicon HPRE crypto driver uses non-constant-time `memcmp()` for label hash verification and has multiple distinguishable error paths. This creates a Bleichenbacher-style padding oracle that allows an attacker to recover RSA PKCS#1 v1.5 plaintext. Version 4.11.0 contains a patch. As a workaround, disable Hisilicon HPRE RSA driver with `CFG_HISILICON_ACC_V3=n`.	2.5	More Details
CVE-2026-14655	A weakness has been identified in code-projects Assessment Management 1.0. Affected by this issue is some unknown functionality of the file admin/view-users.php. Executing a manipulation of the argument User can lead to cross site scripting. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	2.4	More Details
CVE-2026-41124	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an Improper limitation of a pathname to a restricted directory ('path traversal') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure.	2.3	More Details
CVE-2026-12948	A stored cross-site scripting (XSS) vulnerability in the web management interface of the Digi PortServer TS, Digi One SP, Digi One SP IA, and Digi One IA allows a remote, authenticated administrator to inject script into certain system configuration fields. The script subsequently executes in the browser of a user who views the affected pages (CWE-79).	N/A	More Details
CVE-2026-57871	Relative path traversal vulnerability in MicroRealEstate file upload functionality allows attackers to potentially overwrite system files. This issue affects MicroRealEstate: through 1.0.0-alpha3.	N/A	More Details
CVE-2026-13722	WatchGuard Fireware OS contains a firmware validation bypass when processing a backup image via the backup/restore feature. An authenticated administrator can exploit this vulnerability to install a tampered firmware image.This vulnerability affects Fireware OS 11.0 up to and including 11.12.4_Update1, 12.0 up to and including 12.12 and 2025.1 up to and including 2025.6.2.	N/A	More Details
CVE-2026-58518	Cross-Site request forgery (CSRF) vulnerability in The Wikimedia Foundation Mediawiki - RedirectManager Extension allows Cross Site Request Forgery. This issue affects Mediawiki - RedirectManager Extension: from * before 1.3.3.	N/A	More Details
CVE-2026-57870	Broken object-level access control on the Template API in MicroRealEstate allows attackers to retrieve document templates used by other organizations without authorization. This issue affects MicroRealEstate: through 1.0.0-alpha3.	N/A	More Details
CVE-2026-14867	Credentials of built-in users are insecurely stored in the User directory of PcVue projects, all versions prior to 17.0.0. A local attacker could retrieve users’ credentials. Active Directory accounts are not affected by this vulnerability.	N/A	More Details

CVE-2026-13728	In exception circumstances, WatchGuard Fireware OS on a FireCluster may use a hard-coded encryption key to encrypt saved credentials for Access Portal resources. This vulnerability affects Fireware OS 12.1 up to and including 12.12 and 2025.1 up to and including 2026.2. This vulnerability does not affect devices that do not support the Access Portal feature or standalone Fireboxes not deployed in a FireCluster.	N/A	More Details
CVE-2026-57869	Broken object-level access controls and the use of a deterministic pattern during random ID generation in MicroRealEstate allows attackers to access documents uploaded by landlords or tenants without authorization. This issue affects MicroRealEstate: through 1.0.0-alpha3.	N/A	More Details
CVE-2026-57868	MicroRealEstate is affected by broken object-level access controls in PDF generator functionality. This issue affects MicroRealEstate: through 1.0.0-alpha3.	N/A	More Details
CVE-2026-57867	MicroRealEstate allows adversaries to bypass authentication due to a lack of token state management. This would permit adversaries targeting MicroRealEstate deployments to brute-force One-Time Passwords (OTP) to log in as any user. This issue affects MicroRealEstate: through 1.0.0-alpha3.	N/A	More Details
CVE-2026-50043	Improper neutralization of special elements used in an OS command ('OS Command Injection') issue exists in SkyBridge MB-A100/MB-A110. If this vulnerability is exploited, an arbitrary OS command may be executed by an attacker who can log in to the product with an administrative privilege.	N/A	More Details
CVE-2026-27771	Gitea versions up to and including 1.26.1 have insufficient permission checks for Composer package source links, which can expose private or internal package source information.	N/A	More Details
CVE-2026-10834	The WP Travel Engine WordPress plugin before 6.8.1 does not properly validate the source of a user-supplied profile image path before moving the file, allowing authenticated users with subscriber-level access and above to relocate arbitrary files within the WordPress uploads directory into their own profile-image path. This removes the targeted media from its original location and can break content across the site.	N/A	More Details
CVE-2026-56811	Allocation of Resources Without Limits or Throttling vulnerability in phoenixframework phoenix (Phoenix.Socket module) allows an unauthenticated attacker to cause a denial of service against any endpoint that mounts a Phoenix socket with a reachable channel transport (WebSocket or LongPoll). This vulnerability is associated with program files lib/phoenix/socket.ex and program routine 'Elixir.Phoenix.Socket':handle_in/4. Phoenix transports do not limit the number of channels that a single transport process may join. Every phx_join message a client sends over one connection starts a persistent channel process, and the socket process accepts an unbounded number of them. A single unauthenticated client can therefore open one WebSocket or LongPoll connection and stream a large number of phx_join messages, spawning hundreds of thousands of channel processes over that one connection and eventually reaching the BEAM maximum process limit. Once the process table is exhausted the virtual machine can no longer start new processes, denying service to legitimate traffic across the whole node. Because the amplification happens inside a single connection, network-layer connection caps and rate limiting do not mitigate it. The fix adds a :max_channels_per_transport option (default 100) that bounds the number of channels a single transport process can join, forcing abusive clients to open many connections instead, where external load balancers and reverse proxies can throttle them. This issue affects phoenix: from 0.11.0 before 1.5.15, from 1.6.0-rc.0 before 1.6.17, from 1.7.0-rc.0 before 1.7.24, and from 1.8.0-rc.0 before 1.8.9.	N/A	More Details
CVE-2026-8247	An Out-of-bounds Write vulnerability in WatchGuard Fireware OS may allow an unauthenticated attacker on the same local network segment to execute arbitrary code. This vulnerability affects Fireware OS 11.0 up to and including 11.12.4_Update1, 12.0 up to and including 12.12 and 2025.1 up to and including 2026.2.	N/A	More Details
CVE-2026-13384	An Out-of-bounds Write vulnerability in WatchGuard Fireware OS wgagent process could allow an authenticated privileged user to execute arbitrary code via a specially crafted requests to the Management Web UI.This vulnerability affects Fireware OS 12.1 up to and including 12.12 and 2025.1 up to and including 2026.2.	N/A	More Details
CVE-2026-13371	An authenticated administrator can trigger a denial-of-service condition in the Fireware Management Web UI by sending malformed or crafted data to the put_data endpoint, which performs unsafe deserialization of the attacker-supplied input.	N/A	More Details
CVE-2026-13054	A path traversal vulnerability in the WatchGuard Fireware OS Management Web UI allows a privileged authenticated attacker to write arbitrary files on the Firebox's filesystem. This vulnerability affects Fireware OS 11.0 up to and including 11.12.4_Update1, 12.0 up to and including 12.12 and 2025.1 up to and including 2026.2.	N/A	More Details
CVE-2026-14868	The encryption algorithm used to protect the configuration of user accounts, stored in the built-in user directory of PcVue projects, all versions prior to 17.0.0, is not strong enough for the level of protection required. A local attacker could alter the existing configuration and ultimately gain privileged access to the PcVue application.	N/A	More Details
CVE-2026-	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WatchGuard Fireware OS (Tigerpaw Technology Integration module) allows Stored XSS. This vulnerability is	N/A	More

13373	an additional unmitigated attack path for CVE-2025-13936. This issue affects Fireware OS 12.4 up to and including 12.12, 12.5 up to and including 12.5.18, and 2025.1 up to and including 2026.2.		Details
CVE-2026-13368	WatchGuard Fireware OS contains a race condition leading to a use-after-free vulnerability in LDAP authentication for the Mobile User VPN with IKEv2. A remote unauthenticated attacker could exploit this vulnerability to execute arbitrary code in the context of the iked process on Fireboxes that have a Mobile VPN with IKEv2 configured to use an external LDAP authentication server. This vulnerability affects Fireware OS 11.0 up to and including 11.12.4_Update1, 12.0 up to and including 12.12 and 2025.1 up to and including 2026.2.	N/A	More Details
CVE-2026-13084	A null pointer dereference vulnerability in WatchGuard Fireware OS may allow a remote unauthenticated attacker to create a denial-of-service (DoS) condition by sending specially crafted IKEv2 messages. This vulnerability affects both the Mobile User VPN with IKEv2 and the Branch Office VPN using IKEv2 when configured with a dynamic gateway peer. This vulnerability affects Fireware OS 11.10.2 up to and including 11.12.4_Update1, 12.0 up to and including 12.12 and 2025.1 up to and including 2026.2	N/A	More Details
CVE-2026-13079	A local privilege escalation vulnerability in the WatchGuard Mobile VPN with SSL client for Windows allows a local attacker to escalate their privileges to NT AUTHORITY\SYSTEM on the machine where the client is installed. This issue affects the Mobile VPN with SSL client for Windows up to and including 2026.2.	N/A	More Details
CVE-2026-13374	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WatchGuard Fireware OS (ConnectWise Technology Integration module) allows Stored XSS. This vulnerability is an additional unmitigated attack path for CVE-2025-13937. This issue affects Fireware OS 12.4 up to and including 12.12, 12.5 up to and including 12.5.18, and 2025.1 up to and including 2026.2.	N/A	More Details
CVE-2026-12577	DVP80ES3 with Improperly Implemented Security Check for Standard vulnerability.	N/A	More Details
CVE-2026-56812	Improper Check for Unusual or Exceptional Conditions vulnerability in phoenixframework phoenix (Presence JavaScript client) allows an attacker with ordinary channel access to cause a persistent client-side denial of service against every viewer of a presence channel topic. This vulnerability is associated with program files assets/js/phoenix/presence.js and program routines Presence.syncState and Presence.syncDiff. The Phoenix JavaScript presence client checks whether a presence already exists with a bare truthiness test (state[key]) instead of an own-property check. Presence keys can be attacker-controlled, because applications track presences under a username or id supplied by the client. A user who joins a channel choosing a key that is an Object.prototype member name (__proto__, constructor, toString, hasOwnProperty, and similar) makes that lookup return JavaScript's built-in Object.prototype instead of undefined. Because the prototype is truthy, the code treats it as an existing presence and reads .metas.map(...) off it, which throws an uncaught TypeError. The exception propagates out of the presence message handler, so the local state is never updated and onSync() never fires. Because the malicious key is tracked on the server, it is re-pushed on every presence update and keeps re-throwing, so presence sync stays broken for every viewer of that channel topic until the attacker leaves. Both syncState and syncDiff use the same unsafe existence-check pattern. The impact is limited to the affected topic and is a read-time confusion of the prototype object, not a mutation of Object.prototype (it is not prototype pollution). This issue affects phoenix: from 1.2.0-rc.0 before 1.5.15, from 1.6.0-rc.0 before 1.6.17, from 1.7.0-rc.0 before 1.7.24, and from 1.8.0-rc.0 before 1.8.9.	N/A	More Details
CVE-2026-13383	An Out-of-bounds Write vulnerability in WatchGuard Fireware OS ikestubd process could allow an authenticated privileged user to execute arbitrary code via a specially crafted requests to the Management Web UI.This vulnerability affects Fireware OS 12.1 up to and including 12.12 and 2025.1 up to and including 2026.2.	N/A	More Details
CVE-2026-13050	An Out-of-bounds Write vulnerability in WatchGuard Fireware OS networkd process could allow an authenticated privileged user to execute arbitrary code via a specially crafted requests to the Management Web UI.This vulnerability affects Fireware OS 11.8 up to and including 11.12.4_Update1, 12.0 up to and including 12.12 and 2025.1 up to and including 2026.2.	N/A	More Details
CVE-2026-13375	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WatchGuard Fireware OS (Autotask Technology Integration module) allows Stored XSS. This vulnerability is an additional unmitigated attack path for CVE-2025-13938. This issue affects Fireware OS 12.4 up to and including 12.12, 12.5 up to and including 12.5.18, and 2025.1 up to and including 2026.2.	N/A	More Details
CVE-2026-13743	CubeSpace CW0057 Reaction Wheel firmware versions prior to 5.0.20 are vulnerable to an Improper Verification of Cryptographic Signature vulnerability. This could allow an attacker with physical access to the product to upload arbitrary malicious firmware to the device without authentication.	N/A	More Details
CVE-2026-13376	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WatchGuard Fireware OS spamBlocker module allows Stored XSS. This vulnerability is an additional unmitigated attack path for CVE-2025-1071. This issue affects Fireware OS 12.0 up to and including 12.12, 12.5 up to and including 12.5.18, and 2025.1 up to and including 2026.2.	N/A	More Details
	A stored Cross-Site Scripting (XSS) vulnerability has been identified in the web-based management interface of Archer C5 v6.8 routers, due to insufficient server-side validation and lack of proper output encoding of		

CVE-2026-8699	user-controlled input in a certain field. An attacker with administrative privileges can inject crafted HTML or JS payloads into the affected field. The payload is stored and later executed when the affected page is rendered in an administrator's browser.Successful exploitation allows execution of arbitrary JavaScript in an admin's browser, potentially leading to session hijacking and unauthorized access to router configuration, possibly resulting in exposure of sensitive data and modification of device settings. The vulnerability affects ISP-managed firmware variants of the product. Remediation is coordinated through service providers.	N/A	More Details
CVE-2026-58315	Cross-site request forgery vulnerability exists in SEIKO EPSON Web Config. If a user views a malicious page while logged into Web Config, unintended operations may be performed.	N/A	More Details
CVE-2026-13377	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WatchGuard Fireware OS SIP Proxy module allows Stored XSS. This vulnerability is an additional unmitigated attack path for CVE-2025-6947. This issue affects Fireware OS 12.0 up to and including 12.12, 12.5 up to and including 12.5.18, and 2025.1 up to and including 2026.2.	N/A	More Details
CVE-2026-13053	An Out-of-bounds Write vulnerability in WatchGuard Fireware OS's CLI could allow an authenticated privileged user to execute arbitrary code via a specially crafted CLI command. This vulnerability affects Fireware OS 11.0 up to and including 11.12.4_Update1, 12.0 up to and including 12.12 and 2025.1 up to and including 2026.2.	N/A	More Details
CVE-2026-50529	DataEase is an open source data visualization and analysis tool. Prior to 2.10.24, the /de2api/share/proxyInfo share interface generates and returns X-DE-LINK-TOKEN before validating the share password or ticket, allowing unauthenticated attackers who know a protected share UUID to obtain a valid link token for subsequent share-related API calls even with missing or invalid credentials. This issue is fixed in version 2.10.24.	N/A	More Details
CVE-2022-4989	** UNSUPPORTED WHEN ASSIGNED ** Improper Validation of Specified Quantity in Input in the ASUS AI Suite 3 driver allows a local user to access unintended memory regions via crafted IOCTL requests, leading to privilege escalation.	N/A	More Details
CVE-2026-59153	Anki is a program for creating and reviewing flashcards. Prior to 25.09.3, Anki launches a local HTTP server to serve media files and web pages for parts of its interface, but requests from other origins were not sufficiently blocked. A malicious website could potentially trigger side-effecting requests to the local server, with severity varying by browser depending on Private Network Access protections. This issue is fixed in version 25.09.3.	N/A	More Details
CVE-2026-59234	Authorization Bypass Through User-Controlled Key (CWE-639) in CalendarDeleteEventController (app/Http/Controllers/Calendar/CalendarDeleteEventController.php), exposed at GET /calendar/event/delete/{id}, in Prospero Flow CRM before 5.5.3 allows a remote, authenticated attacker to delete arbitrary calendar events belonging to other users by manipulating the {id} path parameter, because the delete handler resolves the record with Calendar::find($id)->delete() and performs no ownership check (no user_id/company_id scoping) before deletion. This results in unauthorized destruction of other users' calendar events across the platform.	N/A	More Details
CVE-2026-42953	The application contains an out-of-bounds write vulnerability that can be exploited by an attacker to cause the program to write data past the end of an allocated memory buffer. This can lead to arbitrary code execution.	N/A	More Details
CVE-2026-47896	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache Lucene.Net (Lucene.Net.Replicator library). This issue affects Apache Lucene.Net.Replicator: from 4.8.0-beta00005 through 4.8.0-beta00017. Users are recommended to upgrade to version 4.8.0-beta00018, which fixes the issue.	N/A	More Details
CVE-2026-50238	Rejected reason: Red Hat Product Security has concluded that this CVE is not required. The reported issue has been classified as a regular bug and will be addressed through the standard bug-fixing process.	N/A	More Details
CVE-2026-54502	Oj (Optimized JSON) is a JSON parser and Object marshaller packaged as a Ruby gem. In versions prior to 3.17.2, Oj.dump is vulnerable to a stack-based buffer overflow when a large :indent value is provided by the developer. fill_indent in dump.h calls memset(indent_str, ' ', (size_t)opts->indent) without validating the size. When opts->indent is set to INT_MAX (2,147,483,647), the (size_t) cast preserves the large value and memset writes 2 GB into the stack-allocated out buffer (4,184 bytes), corrupting the stack and crashing the process. This issue has been fixed in version 3.17.2.	N/A	More Details
CVE-2026-54602	FastGPT is a knowledge-based AI application platform. Prior to 4.15.0, GET /api/core/ai/record/getRecord authenticates the caller but loads LLM request and response traces only by requestId without team scoping, allowing any authenticated user to read another team's prompts, retrieved RAG chunks, and completions if the requestId is known. This issue is fixed in version 4.15.0.	N/A	More Details
CVE-2026-	Oj (Optimized JSON) is a JSON parser and Object marshaller packaged as a Ruby gem. In versions prior to 3.17.2, Oj.load is vulnerable to heap corruption when parsing a JSON string longer than 2 GB. An integer overflow in buf_append_string (buf.h:61) converts the string length to a large negative size_t, causing	N/A	More

54903	memcpy to copy an astronomically large amount of data out of bounds. This crashes the process and can corrupt adjacent heap memory. The issue has been fixed in version 3.17.2.		Details
CVE-2026-54698	Hasura is an open-source product that provides users GraphQL or REST APIs. Prior to 2.49.2 and 2.45.5, a user can use a where clause on a table computed field (returning SETOF some_table) to infer row values that ought to be filtered for their role based on some_table's row-level permissions. While such rows cannot be returned directly, like predicates on strings for instance allow values to be brute forced efficiently with the where clause as an oracle. This issue is fixed in versions 2.49.2 and 2.45.5.	N/A	More Details
CVE-2026-54902	Oj (Optimized JSON) is a JSON parser and Object marshaller packaged as a Ruby gem. Prior to version 3.17.2, is vulnerable to Use-After-Free when in SAJ mode. The Oj::Parser does not protect cached object keys (≥ 35 bytes) from garbage collection, and a Ruby callback that triggers GC inside hash_end can cause the key string to be reclaimed while the C parser still holds a pointer to it. The subsequent access to the freed string VALUE results in a segfault, confirmed by an RIP pointing to address 0x4242 (a canary-style pattern suggesting control over the freed memory's content). This issue has been fixed in version 3.17.2.	N/A	More Details
CVE-2026-55408	Koodo Reader is an ebook reader. In version 2.3.0 and earlier, Koodo Reader is vulnerable to remote code execution through malicious EPUB files because the open-book IPC handler enables nodeIntegrationInSubFrames and EPUB chapter content is rendered with unsanitized innerHTML. An attacker can craft an EPUB book that, when imported and opened by the victim, instantiates a hidden iframe with Node.js API access and executes arbitrary operating system commands with the victim user's privileges. This issue is fixed in version 2.3.1.	N/A	More Details
CVE-2026-54901	Oj (Optimized JSON) is a JSON parser and Object marshaller packaged as a Ruby gem. In versions prior to 3.17.2, Oj::Parser in usual mode does not mark array_class and hash_class references during garbage collection, leading to Use-After-Free. If GC runs after the class is assigned but before a parse, the class object is reclaimed, leaving the parser holding a dangling VALUE. The subsequent parse call dereferences the freed object, producing a segfault. This issue has been fixed in version 3.17.2.	N/A	More Details
CVE-2026-54900	Oj (Optimized JSON) is a JSON parser and Object marshaller packaged as a Ruby gem. In versions prior to 3.17.2, when in usual mode with create_id enabled, Oj::Parser#parse is vulnerable to heap corruption via a negative-size memcpy. When a JSON object key is exactly 65,535 bytes long, an integer truncation in form_attr (usual.c:63) converts the length to -1 before passing it to memcpy. This causes memcpy to copy SIZE_MAX bytes (interpreted as a huge size_t), corrupting heap memory and crashing the process. The issue has been fixed in version 3.17.2.	N/A	More Details
CVE-2026-54899	Oj (Optimized JSON) is a JSON parser and Object marshaller packaged as a Ruby gem. Prior to version 3.17.2, disabling symbol_keys on a reused Oj::Parser instance triggers a heap use-after-free. When symbol_keys is toggled from true to false, opt_symbol_keys_set frees the internal key cache (cache_free) but does not clear the pointer. The next parse call reads from the freed cache via cache_intern, producing a use-after-free. This issue has been fixed in version 3.17.2.	N/A	More Details
CVE-2026-14380	DBI versions before 1.650 for Perl are vulnerable to code injection via caller-influenced Profile. When a string is assigned to a DBI handle's Profile attribute, DBI splits it into path, package and arguments, and interpolates the package part in a string eval with no validation of the package name. Any caller-influenced value that reaches the Profile attribute is therefore arbitrary Perl code execution, including calls to run system commands. The Profile attribute can be set from three different sources that can carry untrusted data: the DBI_PROFILE environment variable, a direct attribute assignment, and a DSN driver-attribute clause dbi:Driver(Profile=>SPEC):db. An attacker controlling any of those inputs runs arbitrary Perl in the host process. The strongest remote position is a network-exposed DBI::Gofer / DBI::ProxyServer whose per-request DSN reaches the Profile attribute, letting a client execute code on the broker host.	N/A	More Details
CVE-2026-26307	Gitea versions before 1.25.5 do not enforce a timeout on git grep searches, allowing expensive searches to consume server resources.	N/A	More Details
CVE-2026-14739	DBI versions before 1.650 for Perl have a heap overflow when preparsing SQL statements with an extreme number of placeholders. The fix for CVE-2026-10879 did not allocate enough memory to handle approximately 1.2-million placeholders. DBI version 1.650 sets a hard limit of 99,999 placeholders.	N/A	More Details
CVE-2026-14740	DBI versions before 1.650 for Perl read one byte out-of-bounds in preparse when deleting an initial SQL comment. The preparse method normalises SQL and removes comments. When the SQL starts with a comment line, the deletion of that line during normalisation led to an out-of-bounds read by one byte. The result is a fault on memory-hardened builds and nondeterministic newline retention on normal builds.	N/A	More Details
CVE-2026-14895	String::Util versions before 1.36 for Perl are susceptible to a regular expression denial of service. The trim and rtrim functions stripped trailing whitespace with s/\s*$//u. Because \s* matches greedily and the $ anchor fails whenever a non-whitespace character follows the whitespace, the regex engine retries the match at each offset of a long whitespace run, producing quadratic backtracking. The fix replaces \s*$ with \s+$. Any caller that passes untrusted input to trim or rtrim can trigger CPU exhaustion with a string containing a long run of whitespace.	N/A	More Details

CVE-2026-36162	An authenticated stored cross-site scripting (XSS) vulnerability in the Upload File Shares API of LiquidFiles v4.2.7 allows attackers to execute arbitrary Javascript or HTML via injecting a crafted payload into the Name parameter.	N/A	More Details
CVE-2026-36163	An HTML injection vulnerability in the file view endpoint of LiquidFiles v4.2.7 allows authenticated attackers to execute arbitrary JavaScript in the context of the victim's browser via the uploading of and user interaction with a crafted HTML file.	N/A	More Details
CVE-2026-37270	Trueview Security camera T18161- AF v4.9.60.0 contains an authentication bypass vulnerability caused by improper password validation and the presence of hard-coded credentials in the firmware.	N/A	More Details
CVE-2026-37271	Fire-Boltt Smartwatch FB BGS001 Firmware: MOY-JS14-2.0.4 is vulnerable to Improper Authentication, The device accepts GATT Write Request commands without sufficient authentication or strong session validation. Under specific conditions, previously captured BLE packets can be replayed from a nearby device to trigger functionality on the smartwatch.	N/A	More Details
CVE-2026-50810	A NULL pointer dereference in smooth_parse_stream_index() in src/media_tools/mpd.c in GPAC master HEAD before commit b35c61f104b85fbb16520ac2838d5d2ef70845b5 allows attackers to cause a denial of service	N/A	More Details
CVE-2026-50811	An out-of-bounds read vulnerability exists in FreeType 2.14.3 and versions before commit 5a280ecde6f324de0d226261036e736e0cb49a71 in src/truetype/ttgxvar.c, in the TT_Get_Var_Design implementation used by FT_Get_Var_Design_Coordinates	N/A	More Details
CVE-2026-51937	An issue in Oneblog V2.3.9 allows a remote attacker to obtain sensitive information via the RestApiController.java, JsApiTicketComponent.java, and the GetAccessTokenComponent.java component	N/A	More Details
CVE-2026-54898	Oj (Optimized JSON) is a JSON parser and Object marshaller packaged as a Ruby gem. In versions prior to 3.17.2,Oj::Parser#parse is vulnerable to a heap use-after-free when a SAJ/SAJ2 callback mutates the input JSON string during parsing. The C engine holds a raw const byte * pointer into the Ruby string's internal buffer. If a callback (e.g. hash_start) resizes the string — for example by calling String#replace with a longer value — Ruby reallocates the string buffer and frees the old one. The C parser's pointer is left dangling; the next character read at parser.c:607 is a use-after-free. This issue has been fixed in version 3.17.2.	N/A	More Details
CVE-2026-54897	Oj (Optimized JSON) is a JSON parser and Object marshaller packaged as a Ruby gem. Prior to 3.17.2, Oj::Doc iterators (each_value, each_child, each_leaf) were vulnerable to a heap use-after-free. When a Ruby block yielded during iteration calls doc.close or d.close, the document's heap memory is freed while the C iterator is still running. When control returns from the block, the iterator reads from the freed region, producing a use-after-free accessible from pure Ruby. This issue has been fixed in version 3.17.2.	N/A	More Details
CVE-2026-54896	Oj (Optimized JSON) is a JSON parser and Object marshaller packaged as a Ruby gem. In versions prior to 3.17.2, when in object mode, Oj.dump is vulnerable to a heap buffer overflow when serializing Exception objects with a large :indent value. The serializer allocates a buffer sized for the object's attributes but does not account for the indent bytes added on each write. With indent: 5000, the accumulation of 5,000-byte indent strings overflows the 13,150-byte heap allocation, corrupting adjacent heap memory. This issue has been fixed in version 3.17.2.	N/A	More Details
CVE-2026-57172	DataEase is an open source data visualization and analysis tool. Prior to 2.10.24, ShareSecretManage uses a hardcoded default share link signature key, allowing an attacker who can obtain a passwordless share for a resource and user to use the known key link-pwd-fit2cloud to forge linkToken JWTs, bypass TokenFilter verification, and access backend resources as the share creator even if the original share has been revoked. This issue is fixed in version 2.10.24.	N/A	More Details
CVE-2026-55647	DataEase is an open source data visualization and analysis tool. Prior to 2.10.24, dashboard text components render stored component content with Vue v-html without server-side HTML sanitization, allowing an authenticated user who can edit dashboard component data to inject HTML with executable event handlers that execute when another user or shared-link visitor views the dashboard. This issue is fixed in version 2.10.24.	N/A	More Details
CVE-2026-55635	DataEase is an open source data visualization and analysis tool. Prior to 2.10.24, chart quota and Y-axis filters embed attacker-controlled filter values directly into generated SQL in Quota2SQLObj.getYWheres() without applying the SQL literal validation and escaping used by other filter paths, allowing an authenticated user who can create or modify chart definitions or submit chart data requests containing quota filters to inject SQL into queries executed against configured datasources. This issue is fixed in version 2.10.24.	N/A	More Details
CVE-2026-55633	DataEase is an open source data visualization and analysis tool. Prior to 2.10.24, a bypass of the H2 zip protocol and file dropper fix allows an authenticated attacker to upload a zip archive disguised with a .ttf extension through FontManage.saveFile and then exploit it through the zip protocol to achieve remote code execution. This issue is fixed in version 2.10.24.	N/A	More Details
CVE-	** UNSUPPORTED WHEN ASSIGNED ** Improper Validation of Specified Quantity in Input in the ASUS AI Suite		More

2022-4990	3 driver allows a local user to bypass security validation and access restricted memory blocks via crafted IOCTL requests, leading to privilege escalation.	N/A	Details
CVE-2026-12960	An Improper Export of Android Application Components vulnerability in ASUS Router App allows a third-party application on the same device to send a crafted Intent that causes ASUS Router App to open an specified URL. Refer to the ' Security Update for ASUS Router Android App ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-48947	An improper access check allows privileged users to overwrite media files without editing permissions.	N/A	More Details
CVE-2026-48948	An improper access check allows user to download vcard exports of com_contact contacts that are inaccessible.	N/A	More Details
CVE-2026-48949	Lack of validation leads to an XSS vulnerability in the MFA management views.	N/A	More Details
CVE-2026-48950	Lack of escaping leads to an XSS vulnerability in the file management view of com_templates.	N/A	More Details
CVE-2026-48951	Lack of escaping leads to XSS vulnerabilities in modalreturn layouts of various components.	N/A	More Details
CVE-2026-48952	Lack of escaping leads to an XSS vulnerability in the update list view of com_installer.	N/A	More Details
CVE-2026-48953	Lack of escaping leads to an XSS vulnerability in the generic image output layout.	N/A	More Details
CVE-2026-48954	Improper validation leads to a generic XSS vector in the language override feature.	N/A	More Details
CVE-2026-48955	An improper access check allows unauthorized users to access workflow stage and transition information.	N/A	More Details
CVE-2026-48956	An improper access check allows users to display a list of modules in the frontend.	N/A	More Details
CVE-2026-48957	An improper access check allows unauthorized users to access com_privacy datasets.	N/A	More Details
CVE-2026-48958	An improper access check allows unauthorized users to create custom fields via webservices endpoints.	N/A	More Details
CVE-2026-8921	External Control of File Name or Path vulnerability in ASUS Business Manager allows a local user to execute arbitrary code with SYSTEM privileges via a tampered IPC message. Refer to the ' Security Update for ASUS Business Manager ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-12481	A vulnerability in keras-team/keras version 3.14.0 allows for arbitrary code execution due to improper handling of deserialization in the `Lambda` layer. Specifically, the `_raise_for_lambda_deserialization()` function fails to enforce the safe-mode guard when `safe_mode` is set to `None`, which is the default value when `from_config()` is called outside of a `SafeModeScope` context. This logic error conflates `None` (unset/default-deny) with `False` (explicitly disabled), bypassing the guard and allowing attacker-controlled `marshal` bytecode to be deserialized. Affected call sites include `keras.layers.deserialize(config)`, `keras.models.clone_model(model)`, and any direct invocation of `Lambda.from_config(config)` without an enclosing `SafeModeScope(True)`. This vulnerability can be exploited to achieve arbitrary OS-level code execution in the context of the server or user process.	N/A	More Details
CVE-2026-	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache Lucene.Net (Lucene.Net.Replicator library). This issue affects Apache Lucene.Net.Replicator: from 4.8.0-beta00005 before 4.8.0-beta00018. Users are recommended to upgrade to version 4.8.0-beta00018, which	N/A	More Details

47897	fixes the issue.		
CVE-2026-47898	Improper Restriction of XML External Entity Reference vulnerability in Apache Lucene.Net (Lucene.Net.Analysis.Common library). This issue affects Apache Lucene.Net.Analysis.Common: from 4.8.0-beta00005 before 4.8.0-beta00018. Users are recommended to upgrade to version 4.8.0-beta00018, which fixes the issue.	N/A	More Details
CVE-2026-50007	Actual is an open-source personal finance application. Prior to 26.7.0, a missing authorization issue allows a shared user with user_access on a budget file to perform owner-only file management actions. A non-owner shared user can call file-management endpoints intended for higher-privilege users, including /delete-user-file, /reset-user-file, and /user-create-key, because requireFileAccess treats ordinary shared access as sufficient for file-management operations that should be restricted to the file owner or an administrator. This issue is fixed in version 26.7.0.	N/A	More Details
CVE-2026-50530	DataEase is an open source data visualization and analysis tool. Prior to 2.10.24, a share mode chart data interface only validates that sceneId matches the resourceId in the link token and fails to validate whether tableId and field IDs in the request body belong to the shared resource, allowing an attacker with a valid share link token to replace dataset identifiers and retrieve unauthorized data through POST /de2api/chartData/getData. This issue is fixed in version 2.10.24.	N/A	More Details
CVE-2026-53511	calibre is an e-book manager. Prior to 9.10.0, a malicious EPUB, OPF, or PDF file can execute arbitrary Python code when its metadata is read by calibre, including through Add books or Edit books, by embedding a custom column definition with a python: template in calibre:user_metadata that is passed unsanitized to exec() in the template formatter. This issue is fixed in version 9.10.0.	N/A	More Details
CVE-2026-53729	DataEase is an open source data visualization and analysis tool. Prior to 2.10.24, any authenticated user can download (/exportCenter/download/{id}), delete (/exportCenter/delete), retry (/exportCenter/retry/{id}), or generate download links (/exportCenter/generateDownloadUri/{id}) for export tasks belonging to other users by manipulating the task ID parameter, and the /exportCenter/download/{id} endpoint is whitelisted from authentication, allowing unauthenticated access to exported files. This issue is fixed in version 2.10.24.	N/A	More Details
CVE-2026-53730	DataEase is an open source data visualization and analysis tool. Prior to 2.10.24, the /de2api/datasetData/previewSql endpoint lacks the mandatory @DePermit permission validation annotation, allowing any authenticated user to specify datasourceId=-1, access the built-in engine database, execute arbitrary SQL statements, and read sensitive core data. This issue is fixed in version 2.10.24.	N/A	More Details
CVE-2026-53751	DataEase is an open source data visualization and analysis tool. Prior to 2.10.24, the H2 database JDBC URL validation logic can be bypassed with special Unicode characters whose case-conversion behavior differs between DataEase validation and H2 parsing, allowing attackers to smuggle dangerous parameters such as init in malicious H2 JDBC connection strings and achieve arbitrary code execution. This issue is fixed in version 2.10.24.	N/A	More Details
CVE-2026-8804	Puppet resource_api (shipped in Puppet Core 8.x and Puppet Enterprise 2023.8.x and 2025.x) does not preserve the sensitive flag on parameters defined via the resource-api, causing values such as passwords to be stored in cleartext in the agent's local transaction state cache. Affected versions of the resource_api module include all versions between 1.5.0 - 1.9.1 and 2.0.0 The issue was fixed in puppet resource_api 1.9.2 and 2.0.1 released with Puppet Core 8.20.0 and PE 2023.8.10 & PE 2025.11.0.	N/A	More Details
CVE-2026-55417	Chevereto is a self-hosted media-sharing platform. Starting in version 3.7.5 and prior to version 4.5.4, when a user enables the private profile option, visiting their profile HTML route (`/username`) correctly returns 404. However, the `/json` AJAX listing endpoint does not apply the same check. An unauthenticated caller who knows the target's user ID can retrieve all of that user's publicly-scoped images, revealing the username (which should be private). This is patched in Chevereto v4.5.4. No known workarounds are available.	N/A	More Details
CVE-2026-55631	DataEase is an open source data visualization and analysis tool. Prior to 2.10.24, the font management module allows authenticated users to submit an arbitrary fileTransName when creating a font record; when the record is later deleted, the backend concatenates that stored value with the font storage directory and passes it to FileUtils.deleteFile() without path traversal sanitization, allowing deletion of arbitrary writable files in the application container. This issue is fixed in version 2.10.24.	N/A	More Details
CVE-2026-50282	Craft CMS is a content management system (CMS). Versions 5.0.0-RC1 and above, prior to 5.9.21 and versions 4.0.0-RC1 and above prior to 4.17.14 contain an authorization issue where a forced folder move can delete a conflicting destination folder without destination delete permission. Function craft\\controllers\\AssetsController::actionMoveFolder() supports moving an asset folder into a destination parent folder. If a folder with the same name already exists at the destination, the action can be called with force=true to overwrite the destination. This issue has been resolved in versions 5.9.21 and 4.17.14.	N/A	More Details
CVE-2026-58517	Improper neutralization of input terminators vulnerability in The Wikimedia Foundation Mediawiki - WikiLambda Extension allows Authentication Bypass. This issue affects Mediawiki - WikiLambda Extension: from * before 1.43.9,1.44.6,1.45.4.	N/A	More Details
	Craft CMS is a content management system (CMS). Versions 5.7.0 and above, prior to 5.9.21 contain a mass-		

CVE-2026-50281	assignment flaw in the bulk-duplicate element action. An attacker who is only able to duplicate their own entires can submit an arbitrary id through the newAttributes request parameter. The duplication routine overrides its own id = null reset with that value and writes the attacker's attributes into the victim's existing entry row. ElementsController::beforeAction() pulls the request body into $this->_attributes and rejects requests that ship an id or canonicalId key at the top level, actionBulkDuplicate(), reads a separate newAttributes array and passes it straight through to the service layer. Elements::duplicateElement() clones the source element, sets id to null, and then hands the attacker's array to Craft::configure(), which overwrites the reset id with any numeric value inside $newAttributes. PHP Yii's saveElement() then performs an UPDATE against the row with that primary key instead of an INSERT. The attackers's title, slug, authorId, postDate, and UID land on the victim's entry. safeAttributes() on Entry includes id because the base element model exposes it, so the Collection::only() filter does not strip it. This issue has been fixed in version 5.9.21.	N/A	More Details
CVE-2026-53360	In the Linux kernel, the following vulnerability has been resolved: KVM: SEV: Require in-GHCB scratch area if GHCB v2+ is in use As per the GHCB spec, when using GHCB v2+ require the software scratch area to reside in the GHCB's shared buffer. Note, things like Page State Change (PSC) requests _rely_ on this behavior, as the guest can't provide a length when making the request, i.e. the size of the guest payload is bounded by the size of the shared buffer. Failure to force usage of the GHCB, and a slew of other flaws, lets a malicious SNP guest corrupt host kernel heap memory, and leak host heap layout information. setup_vmgexit_scratch() allocates a buffer via kvzalloc(exit_info_2), where exit_info_2 is guest-controlled. With exit_info_2=24, this yields a 24-byte allocation in kmalloc-cg-32 (32-byte slab objects). The buffer holds an 8-byte psc_hdr followed by 8-byte psc_entry structs, so only entries[0] and entries[1] are in-bounds. snp_begin_psc() validates end_entry against VMGEXIT_PSC_MAX_COUNT (253) but NOT against the actual buffer size: idx_end = hdr->end_entry; if (idx_end >= VMGEXIT_PSC_MAX_COUNT) { // checks 253, not buffer snp_complete_psc(svm, ...); return 1; } for (idx = idx_start; idx <= idx_end; idx++) { entry_start = entries[idx]; // OOB when idx >= 2 The guest sets end_entry=10+, causing the host to iterate entries[2+] which are OOB into adjacent slab objects. For each OOB entry: - The host reads 8 bytes (OOB READ / info leak oracle) - If the data passes PSC validation, __snp_complete_one_psc() writes cur_page = 1 or 512 into the entry (OOB WRITE, sev.c:3806) - If validation fails, the error response reveals whether adjacent memory is zero vs non-zero (information disclosure to guest) The guest controls allocation size (exit_info_2), entry range (cur_entry/end_entry), and can fire unlimited VMGEXITs to repeatedly hit different slab positions. By exploiting the variety of bugs, a malicious SEV-SNP guest can: - OOB read adjacent kmalloc-cg-32 objects (heap layout disclosure) - OOB write cur_page bits into adjacent objects (heap corruption) - Trigger use-after-free conditions across VMGEXITs E.g. with KASAN enabled, a single insmod of the PoC guest module produces 73 KASAN reports: BUG: KASAN: slab-out-of-bounds in snp_begin_psc+0x126/0x890 Read of size 8 at addr ffff888219ffb5e0 by task qemu-system-x86/2199 BUG: KASAN: slab-out-of-bounds in snp_begin_psc+0x468/0x890 Write of size 8 at addr ffff888351566648 by task qemu-system-x86/2199 The buggy address belongs to the object at ffff888XXXXXXXXX which belongs to the cache kmalloc-cg-32 of size 32 The buggy address is located N bytes to the right of allocated 32-byte region [ffff888XXXXXXXXX, ffff888XXXXXXXXX) Breakdown: 62 slab-out-of-bounds (reads + writes past allocation) 7 slab-use-after-free 4 use-after-free All credit to Stan for the wonderful description and reproducer! [sean: write changelog]	N/A	More Details
CVE-2026-58027	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wikimedia Foundation AbuseFilter. This vulnerability is associated with program files includes/Api/QueryAbuseFilters.Php. This issue affects AbuseFilter: from * before 1.46.0, 1.45.4, 1.44.6, 1.43.9.	N/A	More Details
CVE-2026-58026	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/Parser/Parser.Php. This issue affects MediaWiki: from * before 1.46.0, 1.45.4, 1.44.6, 1.43.9.	N/A	More Details
CVE-2026-58025	Deserialization of untrusted data vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/Import/WikiImporter.Php, includes/Import/WikiRevision.Php, includes/Logging/LogEntryBase.Php. This issue affects MediaWiki: from * before 1.46.0, 1.45.4, 1.44.6, 1.43.9.	N/A	More Details
CVE-2026-58024	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/Api/ApiUserrights.Php. This issue affects MediaWiki: from * before 1.46.0, 1.45.4, 1.44.6, 1.43.9.	N/A	More Details
CVE-2026-56810	Allocation of Resources Without Limits or Throttling vulnerability in elixir-mint mint (Mint.HTTP1 module) allows a denial of service via an oversized chunked transfer-encoded response. This vulnerability is associated with program files lib/mint/http1.ex and program routines 'Elixir.Mint.HTTP1':decode_body/5, 'Elixir.Mint.HTTP1':add_body_to_buffer/2. When Mint decodes a chunked HTTP response body, it accumulates each partial fragment of the current chunk in the connection's data_buffer (an unbounded iolist) via add_body_to_buffer/2 and does not emit the data to the caller until the full declared chunk length has been received. The chunk size is taken directly from the server and parsed with no upper bound, so a malicious or compromised server can announce one enormous chunk (for example a size line of 7FFFFFFF, about 2 GiB) and then send the body bytes slowly without ever completing the chunk. The client buffers every received byte while it waits for a completion that never arrives, and because no data responses are produced until the chunk finishes, a caller that otherwise streams large content-length bodies safely gains no protection. An unauthenticated remote server (reachable whenever a client follows redirects, fetches user-supplied URLs, or processes webhooks) can drive the client's memory arbitrarily high and trigger an out-of-memory condition. This issue affects mint: from 0.5.0 before 1.9.1.	N/A	More Details

CVE-2026-58226	Inefficient Algorithmic Complexity vulnerability in elixir-mint hpax allows unauthenticated denial-of-service via unbounded HPACK integer decoding. hpax decodes HPACK variable-length integers with no upper bound on the decoded value or the number of continuation octets. 'Elixir.HPAX.Types':decode_remaining_integer/3 accumulates the integer as int + (value <<< m), shifting by 7 more bits for each continuation octet and stopping only on a terminating octet or truncated input, never because the integer grew too large. Because BEAM integers are arbitrary precision, a run of N continuation octets builds an O(N)-bit bignum and re-adds into an ever-larger bignum on each step, so the total decoding cost is superlinear (about O(N^2)). An unauthenticated attacker who can send an HTTP/2 header block to a server using this decoder (reached through the 'Elixir.HPAX':decode/2 entry point) can supply a small header block that forces a large, attacker-controlled amount of CPU (and transient memory), a denial-of-service amplification. This issue affects hpax from 0.1.1 before 1.0.4.	N/A	More Details
CVE-2026-13707	Session fixation vulnerability in Wikimedia Foundation OAuth. This vulnerability is associated with program files src/Backend/MWOAuthServer.Php. This issue affects OAuth: from * through 1.46.0, 1.45.4, 1.44.6, 1.43.9.	N/A	More Details
CVE-2026-13706	Improper input validation vulnerability in Wikimedia Foundation UrlShortener. This vulnerability is associated with program files includes/UrlShortenerUtils.Php.	N/A	More Details
CVE-2026-13698	A memory leak in OpenVPN version 2.5.0 through 2.5.11, 2.6.0 through 2.6.20 and 2.7_alpha1 through 2.7.4 allows remote attackers with a valid tls-crypt-v2 client key to potentially cause a denial of service	N/A	More Details
CVE-2026-54893	URL path injection in the Microsoft Graph adapter of Swoosh. Swoosh.Adapters.MsGraph builds its Microsoft Graph API request URL by interpolating the sender's email address into the URL path (/users/{from}/sendMail) without percent-encoding or validation. In applications that derive the from address from untrusted or user-influenced input (for example a relay, a contact form, or a "send as" feature), an attacker can place URL-special characters such as /, ?, or # in the local part of the address to escape the intended path segment and rewrite the path and query string of the request. Because the same authenticated POST is sent with the application's Microsoft Graph bearer token, the attacker can redirect it to other Graph endpoints within the token's scopes and control the request's query string. Applications that always use a fixed, trusted from address are not affected. This issue affects swoosh from 1.12.0 before 1.26.3.	N/A	More Details
CVE-2026-7185	A validation vulnerability has been identified in certain web features related to file management or upload in several products of the TAO 2.0 suite. This vulnerability could allow an attacker capable of interacting with the affected feature to attempt to access file system resources outside the scope intended by the application.	N/A	More Details
CVE-2026-13122	OpenVPN version 2.6.0 through 2.6.20 and 2.7_alpha1 through 2.7.4 allows remote attackers to cause a denial of service via a malformed authentication token that triggers a reachable assertion when external-auth is enabled	N/A	More Details
CVE-2026-53362	In the Linux kernel, the following vulnerability has been resolved: ipv6: account for fraggap on the paged allocation path In __ip6_append_data(), when the paged-allocation branch is taken (MSG_MORE / NETIF_F_SG / large fraglen), alloclen and pagedlen are computed as alloclen = fragheaderlen + transhdrlen; pagedlen = datalen - transhdrlen; datalen already includes fraggap (datalen = length + fraggap). When fraggap is non-zero, this is not the first skb and transhdrlen is zero. The fraggap bytes carried over from the previous skb are copied just past the fragment headers in the new skb's linear area. The linear area is therefore undersized by fraggap bytes while pagedlen is overstated by the same amount, and the copy writes past skb->end into the trailing skb_shared_info. An unprivileged user can trigger this via a UDPv6 socket using MSG_MORE together with MSG_SPLICE_PAGES. The bad accounting was introduced by commit 773ba4fe9104 ("ipv6: avoid partial copy for zc"). Before commit ce650a166335 ("udp6: Fix __ip6_append_data()'s handling of MSG_SPLICE_PAGES"), the negative copy value caused -EINVAL to be returned. That later commit allowed MSG_SPLICE_PAGES to proceed in this case, making the corruption triggerable. The non-paged branch sets alloclen to fraglen, which already accounts for fraggap because datalen does. Bring the paged branch in line by adding fraggap to alloclen and subtracting it from pagedlen. After this adjustment, copy no longer collapses to -fraggap on the paged path, so remove the stale comment describing that old arithmetic. Since a negative copy is no longer expected for a valid MSG_SPLICE_PAGES case, remove the MSG_SPLICE_PAGES exception from the negative copy check.	N/A	More Details
CVE-2026-53361	In the Linux kernel, the following vulnerability has been resolved: af_unix: Set gc_in_progress to true in unix_gc(). Igor Ushakov reported that unix_gc() could run with gc_in_progress being false if the work is scheduled while running: Thread 1 Thread 2 Thread 3 -------- -------- -------- unix_schedule_gc() unix_schedule_gc() `- if (!gc_in_progress) `- if (!gc_in_progress) |- gc_in_progress = true | `- queue_work() | unix_gc() <----------------/ | | |- gc_in_progress = true ... `- queue_work() | | `- gc_in_progress = false | | unix_gc() <-----------------------------------------' | ... /* gc_in_progress == false */ | `- gc_in_progress = false unix_peek_fpl() relies on gc_in_progress not to confuse GC by MSG_PEEK. Let's set gc_in_progress to true in unix_gc().	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: Fix shadow paging use-after-free		

CVE-2026-53359	due to unexpected role Commit 0cb2af2ea66ad ("KVM: x86: Fix shadow paging use-after-free due to unexpected GFN") fixed a shadow paging mismatch between stored and computed GFNs; the bug could be triggered by changing a PDE mapping from outside the guest, and then deleting a memslot. The rmap_remove() call would miss entries created after the PDE change because the GFN of the leaf SPTE does not match the GFN of the struct kvm_mmu_page. A similar hole however remains if the modified PDE points to a non-leaf page. In this case the gfn can be made to match, but the role does not match: the original large 2MB page creates a kvm_mmu_page with direct=1, while the new 4KB needs a kvm_mmu_page with direct=0. However, kvm_mmu_get_child_sp() does not compare the role, and therefore reuses the page. The next step is installing a leaf (4KB) SPTE on the new path which records an rmap entry under the gfn resolved by the walk. But when that child is zapped its parent kvm_mmu_page has direct=1 and kvm_mmu_page_get_gfn() computes the gfn for the 4KB page as sp->gfn + index instead of using sp->shadowed_translation[] (or sp->gfns[] in older kernels). It therefore fails to remove the recorded entry. When the memslot is dropped the shadow page is freed but the rmap entry survives, as in the scenario that was already fixed. Code that later walks that gfn (dirty logging, MMU notifier invalidation, and so on) dereferences an sptep that lies in the freed page, causing the use-after-free.	N/A	More Details
CVE-2026-44937	Potential forgery of webhook requests when using a unauthenticated webhook in SUSE Rancher Fleet 0.15 before 0.15.2, 0.14 before 0.14.6, 0.13 before 0.13.11 and 0.12 before 0.12.5 could be used by remote attackers to cause a denial of service or a downgrade attack on other repositories on the system.	N/A	More Details
CVE-2026-58399	@acastellon/auth is an authentication control system for microservices. Versions prior to 2.3.0 appear to allow an unauthenticated authentication bypass in validateToken() through spoofable auth-user and Host request headers. The validateToken middleware contains a service-to-service bypass for auth-user: service-brother when req.get('host').startsWith(getHostName()). Both values involved in the check can be influenced by an unauthenticated HTTP client: auth-user is a request header, and Host is also client-controlled. As a result, a remote unauthenticated attacker can send a request with crafted headers and bypass token validation before the normal legacy/JWT/OIDC validation logic runs. A fix has been implemented in v2.3.0.	N/A	More Details
CVE-2026-58035	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files resources/src/mediawiki.Special.Block/SpecialBlock.Vue.	N/A	More Details
CVE-2026-58034	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation CheckUser. This vulnerability is associated with program files modules/ext.CheckUser.TempAccounts/components/blockConnectedTempAccountsField.Vue. This issue affects CheckUser: from 1.46.0-rc.0 before 1.46.0.	N/A	More Details
CVE-2026-12196	HestiaCP panel cronjob feature is affected by a broken access control vulnerability. Low privilege users can modify the panel cronjob to execute scripts HestiaCP management scripts with passwordless sudo. This could result in the takeover of administrator users in the application and the underlying webserver.	N/A	More Details
CVE-2026-58031	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files resources/src/mediawiki.Special.Apisandbox/ApiSandboxLayout.Js. This issue affects MediaWiki: from 1.46.0-rc.0 before 1.46.0.	N/A	More Details
CVE-2026-2891	The following Poly Voice IP devices, CCX, Trio, and Edge E, might be inoperable if they connect to a malicious SIP server and receive malformed data. HP is releasing updates to mitigate these potential vulnerabilities.	N/A	More Details
CVE-2026-12195	myVesta is affected by an authenticated remote code execution vulnerability. Low privileged users can insert arbitrary commands as a part of the v_ftp_user parameter when deleting FTP usernames. This could result in the execution of commands as the admin user or takevoer of the admin user in myVesta.	N/A	More Details
CVE-2026-13602	We found a chain of combining multiple weaknesses in the product that could allow an attacker to become any user in the backend and access any data: * The payment integration plugins Stripe (included in the core system), pretix-mollie, pretix-oppwa, pretix-bitpay, pretix-payone, pretix-secuconnect, pretix-sofort, and pretix-saferpay contain a code path that is intended for the transport of session parameters from a tab with isolated cookies (e.g. in the pretix widget) to a new tab. For this purpose, a set of session parameters is cryptographically signed and then passed to the new tab as a URL parameter. The plugins perform no further validation of the session parameters, other than the cryptographic signature being valid. This is fixed with the releases issued today by strictly validating that no session parameters outside of the scope of the respective plugin may be set. * An unrelated feature in the core system is used to generate redirect links that obfuscate any Referer headers for outgoing links to prevent leakage of secrets in URLs. This redirect page also requires cryptographically signed parameters. Unfortunately, it uses the same key and salt for the signature as the previously mentioned feature in the payment integration plugins. A motivated attacker with access to at least one event in the backend can trick the system into cryptographically signing arbitrary content using specially crafted links. In combination with the previous issue, the attacker could use this to set and modify arbitrary parameters on their user session by injecting the signed parameters into the feature of the payment providers. This is fixed with the releases issued today by using different salts for the signature for each plugin and feature. * A third, unrelated feature in the core system is used for admin users to act on behalf of another user, mostly for debugging purposes. With being able to insert arbitrary parameters into a session,	N/A	More Details

	an attacker can abuse this feature to change their session from their actual user to any user in the system by guessing a valid user ID. This is fixed with the release today by requiring unguessable information to be contained in the session of the user to switch to.		
CVE-2026-12374	Improper certificate validation and a time-of-check time-of-use (TOCTOU) race condition in the PrivilegedHelperTool XPC service in Cato Client before v.5.13.1 on macOS allows a local authenticated attacker to escalate privileges to root via a self-signed certificate that bypasses the XPC caller verification and a symlink swap during package installation.	N/A	More Details
CVE-2026-54291	pgjdbc is an open source postgresql JDBC Driver. In releases 42.7.4 through 42.7.11, channelBinding=require connections can be silently downgraded from SCRAM-SHA-256-PLUS with channel binding to plain SCRAM-SHA-256 without it, losing the man-in-the-middle protection the setting is meant to guarantee. An attacker who can intercept the TLS connection can trigger the downgrade with a certificate whose signature algorithm has no tls-server-end-point channel-binding hash, because the bundled com.ongres.scram:scram-client returns an empty byte array instead of failing and pgJDBC ScramAuthenticator checks only that the server advertised a PLUS mechanism, without rejecting the empty binding or checking that the negotiated mechanism uses channel binding. This issue is fixed in version 42.7.12.	N/A	More Details
CVE-2026-53356	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gem: Fix phys BO pread/pwrite with offset sg_page() returns struct page pointer not (void *) so the scaling of pread/pwrite is wrong for phys BO and wrong parts of BO would be accessed if non-zero offset is used. Last impacted platform with overlay or cursor planes using phys mapping was Gen3/945G/Lakeport. (cherry picked from commit 3e49a2f85070b2fb672c1e0fdba281a4ea3aebe6)	N/A	More Details
CVE-2026-53355	In the Linux kernel, the following vulnerability has been resolved: net: rds: clear i_sends on setup unwind The RDS IB connection teardown path is written so it can run during partial startup and on repeated shutdown attempts. It uses NULL pointers to distinguish resources that are still owned from resources that have already been released. When rds_ib_setup_qp() fails after allocating i_sends but before allocating i_recvs, the sends_out path frees i_sends without clearing the pointer. A later shutdown pass can still treat that stale pointer as a live send ring allocation. Clear i_sends after vfree() in the error unwind path so the existing shutdown logic continues to use the correct ownership state.	N/A	More Details
CVE-2026-11405	The web server binary /bin/httpd contains a hidden backdoor authentication mechanism in the login() function at 004c88b8. - The function contains a normal authentication path using MD5/hash-based password verification (prod_encode64/PasswordToMd5/check_rand_key). - After normal authentication fails, it calls GetValue("sys.rzadmin.password") to read a backdoor password from the device configuration. - It performs a direct strcmp() comparison (plaintext, not hashed) between the config value and the user-supplied password. A successful match grants role=2 (admin-level access) and creates a valid session. The rzadmin username is never checked — any username works with the backdoor	N/A	More Details
CVE-2026-14536	Improper enforcement of a mandatory multi-factor authentication policy in Devolutions Server 2026.2.9.0 allows an attacker with valid user credentials to bypass the MFA Required policy and authenticate without completing multi-factor authentication. The problem occurs when DVLS encounters an invalid default MFA value.	N/A	More Details
CVE-2026-58028	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki, Wikimedia Foundation CentralAuth. This vulnerability is associated with program files includes/Api/ApiFormatBase.Php, includes/Api/ApiHelp.Php, includes/ResourceLoader/Module.Php, includes/Hooks/Handlers/PageDisplayHookHandler.Php, includes/LogFormatter/PermissionChangeLogFormatter.Php. This issue affects MediaWiki: from * before 1.46.0, 1.45.4, 1.44.6, 1.43.9; CentralAuth: from * before 1.46.0, 1.45.4, 1.44.6, 1.43.9.	N/A	More Details
CVE-2026-12686	An authenticated user could manipulate a company ID parameter in a POST request to the backend to gain unauthorised access to other companies hosted within the same subdomain environment. The application does not adequately verify whether the requested company ID belongs to the authenticated user’s session, resulting in a cross-tenant authorisation bypass. If this vulnerability is successfully exploited, it allows unauthorised access to sensitive customer information, including billing data, and may enable the unauthorised modification of third-party data.	N/A	More Details
CVE-2026-53358	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: use chan timer to close channels in cleanup_listen() l2cap_chan_close() removes the channel from conn->chan_l, which must be done under conn->lock. cleanup_listen() runs under the parent sk_lock, so acquiring conn->lock would invert the established conn->lock -> chan->lock -> sk_lock order. Instead of calling l2cap_chan_close() directly, schedule l2cap_chan_timeout with delay 0 to close the channel asynchronously. The timeout handler already acquires conn->lock and chan->lock in the correct order. The timer is only armed when chan->conn is still set: if it is already NULL, l2cap_conn_del() has already processed this channel (l2cap_chan_del + l2cap_sock_teardown_cb + l2cap_sock_close_cb), so there is nothing left to do. If l2cap_conn_del() races in after the timer is armed, __clear_chan_timer() inside l2cap_chan_del() cancels it; if the timer has already fired, the handler returns harmlessly because chan->conn was cleared.	N/A	More Details
	Craft CMS is a content management system (CMS). IN versions 5.0.0-RC1 and above prior to 5.9.21,		

CVE-2026-50279	theEntriesController::actionSaveEntry() performs entry-edit permission checks before request-controlled author changes are applied to the model, allowing for authorship spoofing. The subsequent author mutation path accepts attacker-supplied authors / author parameters and allows the change when the current user is one of the old authors. Because the controller does not re-run authorization after mutating the author list, a low-privileged user can reassign an entry's authorship to another user without holding the dedicated peer-author-change permission. This issue has been fixed in version 5.9.21.	N/A	More Details
CVE-2026-54908	Pion DTLS is a Go implementation of Datagram Transport Layer Security. Versions prior to 3.1.4 are vulnerable to Remote Denial of Service via panic while parsing a crafted ECDHE_PSK ServerKeyExchange message. This issue has been fixed in version 3.1.4.	N/A	More Details
CVE-2026-54756	Jodit Editor is a WYSIWYG editor with written in pure TypeScript file and image editing capabilities. In versions prior to 4.12.18, Jodit.configure(options) — and the internal ConfigMerge / ConfigProto helpers — merged user-supplied options into the editor configuration without filtering prototype-mutating keys, potentially causing a Prototype Pollution vulnerability. A payload nested under an existing plain-object option such as controls could reach and mutate Object.prototype. Applications that pass user-controlled or partially user-controlled configuration into Jodit.configure() may be vulnerable. This issue was fixed in version 4.12.18.	N/A	More Details
CVE-2026-55660	Tina is a headless content management system. In versions prior to @tinacms/app 2.5.6 and tinacms 3.9.3, cross-origin postMessage handlers and a rich-text URL-sanitization bypass enable stored XSS and session takeover. The library registers window message listeners — the useTina overlay handler, the OAuth authentication popup handler, and the admin↔preview iframe GraphQL reducer — that act on event.data without verifying event.origin or event.source and post messages using non-specific target origins, while insufficient URL sanitization in rich-text content allows malicious URLs to persist and execute. A page the victim visits (or a window in an opener/iframe relationship with a Tina admin) can forge messages to drive the editor, inject preview content, or observe/forge the OAuth popup channel to take over an authenticated editing session. This issue has been fixed in versions @tinacms/app 2.5.6 and tinacms 3.9.3.	N/A	More Details
CVE-2026-55661	Tina is a headless content management system. In versions prior to @tinacms/mdx 2.1.7 and tinacms 3.9.3, rich-text parsing and the default link/image renderers did not sanitize the url field on Slate link/image nodes. Content containing javascript: or data:text/html URLs — including case-variant, whitespace-padded, and control-character-obfuscated forms — is rendered into href/src and executes when the content is viewed. Any actor able to author rich-text content (for example a lower-privileged editor, or imported/external content) can achieve stored XSS against editors and site viewers. This issue is fixed in versions @tinacms/mdx 2.1.7 and tinacms 3.9.3.	N/A	More Details
CVE-2026-59509	An unauthenticated improper input validation vulnerability in the POST /fetch_cve_data endpoint in cve-search. A remote attacker can manipulate request parameters controlling the MongoDB collection, projected fields, and regular-expression filters to read arbitrary application MongoDB collections. This can expose administrative usernames and password hashes from the mgmt_users collection, enabling offline password cracking and potential administrative account compromise.	N/A	More Details
CVE-2026-55886	Jodit Editor is a WYSIWYG editor with written in pure TypeScript file and image editing capabilities. Versions prior to 4.12.26 are vulnerable to Prototype Pollution through Jodit.modules.Helpers.set(chain, value, obj), which walks the dot-separated chain, creating and following each path segment without filtering prototype-mutating keys. A chain that begins with (or contains) __proto__, constructor, or prototype lets the final assignment reach and mutate Object.prototype. Applications that pass a user-controlled or partially user-controlled key path into Jodit.modules.Helpers.set() could be vulnerable, causing unexpected property injection, logic bypass, denial of service, or secondary security issues. This issue has been fixed in version 4.12.26.	N/A	More Details
CVE-2026-55793	Craft CMS is a content management system (CMS). In versions 5.0.0-RC1 through 5.9.22, an author-level control panel user can store a malicious JavaScript payload in an entry title. When an admin, or any control panel user with saveEntries for the same Structure section, drags another entry under the poisoned entry in table view, the payload executes in the victim's session. The issue is exploitable because the title is escaped into data-title by the server, decoded again by the browser, read with jQuery .data('title'), and then concatenated into a new HTML string without attribute escaping. To exploit, an attacker must have an existing control panel account (Author role minimum), the victim must perform a drag operation (not just visit the page), and the victim's session needs to be elevated at trigger time. This issue has been fixed in version 5.9.23.	N/A	More Details
CVE-2026-11950	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-14358	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in The Wikimedia Foundation Mediawiki - Charts Extension allows Cross-Site Scripting (XSS). This issue affects Mediawiki - Charts Extension: from * before 1.43.9,1.44.6,1.45.4.	N/A	More Details
	A path traversal vulnerability exists in the Git Service component shared by Altium Enterprise Server and Altium 365. The service accepts a sequence of post-clone file-manipulation operations that use user-supplied		

CVE-2026-14439	paths without validation, allowing an authenticated user with basic git access to move arbitrary files outside the intended repository area. This file-move primitive can be used to place attacker-controlled script content into directories where it is later executed by the service, resulting in remote code execution under the Git Service account. On multi-tenant Altium 365 deployments, this could have allowed access to data belonging to other tenants on the same infrastructure node. Altium Enterprise Server is fixed in 8.1.1. The issue has been remediated across Altium 365 shared multi-tenant deployments at the service level; remediation is in progress on remaining Altium 365 deployments.	N/A	More Details
CVE-2026-50283	Craft CMS is a content management system (CMS). Versions 5.0.0-RC1 through 5.9.20, and 4.0.0-RC1 through 4.17.13 contain an authorization issue in the AssetsController::actionReplaceFile that can delete a source asset without source delete permission by supplying both assetId and sourceAssetId. AssetsController::actionReplaceFile() supports replacing a target asset file using another existing asset as the source. The action loads: assetId -> $assetToReplace and sourceAssetId -> $sourceAsset, then enforces replace permissions using ($assetToReplace ?: $sourceAsset). When both IDs are provided, this expression resolves to the target asset so no permission check is performed against the source asset volume. When both assets are present, Craft copies the source file into the target and then deletes the source asset. There is no deletion check for for the source asset. An authenticated user who can replace files in one volume can delete assets in another volume where they do not have delete permission, as long as they can obtain a sourceAssetId, leading to broken content references and data loss. This issue has been fixed in versions 4.17.14 and 5.9.21.	N/A	More Details
CVE-2026-50284	Craft CMS is a content management system (CMS). In versions 5.0.0-RC1 through 5.9.21 and 4.0.0-RC1 through 4.17.14, theAssetsController::actionDeleteFolder() only requires the deleteAssets:<volume-uid> permission for the target folder. It never enforces deletePeerAssets:<volume-uid>, even though Assets::deleteFoldersByIds() cascades deletion to every descendant folder and every asset inside, regardless of the uploader's assigned privileges. A low-privilege user who has been granted folder-management rights on a shared volume can therefore destroy assets uploaded by other users (peer assets), bypassing the per-asset peer-permission check that the sibling actionDeleteAsset endpoint correctly applies. This issue has been fixed in versions 4.17.15 and 5.9.22.	N/A	More Details
CVE-2026-55790	Craft CMS is a content management system (CMS). In versions 5.0.0-RC1 through 5.9.22 and 4.0.0-RC1 through 4.17.15, an attacker with only a GitHub account can plant a JavaScript payload in a craftcms/cms issue title. When a Craft admin uses the CraftSupport widget’s "Give feedback" screen and types a search term that returns the poisoned issue, the payload executes in the admin’s control panel session. No control panel account or elevated privileges are required on the attacker’s side. This issue has been fixed in versions 4.17.16 and 5.9.23.	N/A	More Details
CVE-2026-58520	URL redirection to untrusted site ('open redirect') vulnerability in The Wikimedia Foundation Mediawiki - UrlShortener Extension allows Cross-Site Flashing. This issue affects Mediawiki - UrlShortener Extension: from * before 1.43.9, 1.44.6, 1.45.4.	N/A	More Details
CVE-2026-50280	Craft CMS is a content management system (CMS). In versions 5.0.0-RC1 and above prior to 5.9.21, the EntriesController::actionMoveToSection() endpoint gates the destination section only by viewEntries:$section->uid rather than requiring saveEntries permission (the source entry is separately checked via Entry::canMove()). As a result, a low-privileged authenticated control-panel user who can move an entry out of its current section can call moveEntryToSection() to rewrite the entry's sectionId and save it into a section where they have read access but no write access. This breaks the section-level authorization model, letting a user with limited permissions inject content into a protected section and interfere with editorial boundaries, approval workflows, and section-specific business logic. This issue has been fixed in version 5.9.21.	N/A	More Details
CVE-2026-58029	Vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/Api/ApiChangeAuthenticationData.Php, includes/Api/ApiLinkAccount.Php, includes/Api/ApiRemoveAuthenticationData.Php, includes/Specials/SpecialLinkAccounts.Php, includes/Specials/SpecialUnlinkAccounts.Php. This issue affects MediaWiki: from * before 1.46.0, 1.45.4, 1.44.6, 1.43.9.	N/A	More Details
CVE-2026-55791	Craft CMS is a content management system (CMS). Versions 4.0.0-RC1 and above, prior to 4.18.0 and 5.0.0-RC1, and above, prior to 5.10.0, are vulnerable to Server-Side Request Forgery (SSRF) and Arbitrary JavaScript Injection through the /actions/app/resource-js endpoint. By exploiting the default permissive trustedHosts configuration, an attacker can poison the Host or X-Forwarded-Host header to manipulate the application’s $baseUrl. This bypasses the endpoint’s internal URL validation, forcing the backend Guzzle client to fetch a malicious payload from an attacker-controlled server and reflect it to the client with a Content-Type: application/javascript header. The vulnerability manifests when assetManager.cacheSourcePaths is set to false. This issue has been fixed in versions 4.18.0 and 5.10.0.	N/A	More Details
CVE-2026-55792	Craft CMS is a content management system (CMS). In versions starting from 4.0.0-RC1 and prior to 4.18.0, and 5.0.0-RC1 and above, prior to 5.10.0, the dataUrl() Twig function is included in Craft’s Twig sandbox allowlist, allowing any control panel user granted the utility:system-messages permission to embed a file-reading payload into system email templates. When those emails are sent, the server reads the target file and returns its contents as a base64-encoded data URL embedded in the email body. The .env file, which typically contains the database password, CRAFT_SECURITY_KEY, and third-party API keys, passes all of	N/A	More Details

	Craft’s existing dataUrl() protection checks and is fully exfiltrated. Obtaining CRAFT_SECURITY_KEY enables an attacker to forge session tokens and escalate to full admin account takeover. This issue has been fixed in versions 4.18.0 and 5.10.0.		
CVE-2026-1433	uniFLOW Universal Login Manager (ULM) Standalone contains an information disclosure vulnerability that may allow an authenticated administrator to access sensitive configuration information through the ULM Remote User Interface (RUI). Exploitation requires administrative privileges and may disclose configuration data associated with SMTP or LDAP integrations. ULM deployments connected to uniFLOW Server or uniFLOW Online are not affected.	N/A	More Details
CVE-2026-55794	Craft CMS is a content management system (CMS). In versions 5.9.0 and above prior to 5.10.0, control panel users with the ability to edit entries can execute unsandboxed Twig code via the HTTP Referrer header, potentially leading to authenticated RCE. The issue happens when a user is saving entries. Strings for a signed redirect URL are being compiled as a Twig template via renderObjectTemplate(), and while a sandboxed alternative already exists (renderSandboxedObjectTemplate()), it is not used in this case. This signed URL can be specified by users, as it is reflected in the “Referer” HTTP request header, which is under attacker control. This issue has been fixed in version 5.10.0.	N/A	More Details
CVE-2026-44934	A information disclosure when DEBUG loglevel is set in SUSE Rancher AI Agent 1.0 before 1.0.2 could leak API keys or LLM response text with potential sensitive data into logfiles, allowing local attackers to misuse respective gained data or credentials.	N/A	More Details
CVE-2026-12480	Keras versions up to and including 3.13.2 are vulnerable to an arbitrary HDF5 file read due to an incomplete fix for CVE-2026-1669. The vulnerability resides in the `H5IOStore._verify_dataset()` and `file_editor.py` methods, which fail to check the `dataset.is_virtual` property of HDF5 datasets. This allows an attacker to craft a malicious `.keras` model archive or `.h5` weights file containing a Virtual Dataset (VDS) that references external HDF5 files on the victim's filesystem. When the victim loads the model using `keras.models.load_model()` or `keras.saving.load_model()`, the external file is transparently read, leading to potential information disclosure. Fixed in versions 3.12.2 and 3.14.1.	N/A	More Details
CVE-2026-8857	A vulnerability in Wikimedia Foundation timeline. This vulnerability is associated with program files scripts/EasyTimeline.Pl, includes/Timeline.Php. This issue affects timeline: from * before 1.46.0, 1.45.4, 1.44.6, 1.43.9.	N/A	More Details
CVE-2026-58038	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation timeline. This vulnerability is associated with program files includes/Timeline.Php, scripts/EasyTimeline.Pl. This issue affects timeline: from * before 1.46.0, 1.45.4, 1.44.6, 1.43.9.	N/A	More Details
CVE-2026-58037	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/Language/Language.Php, includes/Logging/BlockLogFormatter.Php, includes/Logging/LogFormatter.Php, includes/Logging/PatrolLogFormatter.Php, includes/Logging/RenameuserLogFormatter.Php, includes/Logging/TagLogFormatter.Php, includes/Specials/SpecialVersion.Php. This issue affects MediaWiki: from * before 1.46.0, 1.45.4, 1.44.6, 1.43.9.	N/A	More Details
CVE-2026-58036	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/Api/ApiQueryAllUsers.Php, includes/Api/ApiQueryUsers.Php, includes/Permissions/PermissionManager.Php, includes/User/UserGroupManager.Php.	N/A	More Details
CVE-2026-58033	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/Actions/InfoAction.Php. This issue affects MediaWiki: from * before 1.46.0, 1.45.4, 1.44.6, 1.43.9.	N/A	More Details
CVE-2026-58032	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files resources/src/mediawiki.Api/index.Js. This issue affects MediaWiki: from * before 1.46.0, 1.45.4, 1.44.6, 1.43.9.	N/A	More Details
CVE-2026-58030	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation SyntaxHighlight_GeSHi. This vulnerability is associated with program files includes/SyntaxHighlight.Php. This issue affects SyntaxHighlight_GeSHi: from * before 1.46.0, 1.45.4, 1.44.6, 1.43.9.	N/A	More Details
CVE-2026-8147	In MLflow versions prior to 3.14.0, when running with authentication enabled, the trace API endpoints lack proper authorization validators. This allows any authenticated user to bypass experiment-level authorization controls on all trace operations, including reading, deleting, and modifying traces on experiments they do not have permission to access. The issue arises from the `_before_request` handler, which does not register authorization validators for trace endpoints, resulting in requests proceeding without validation. This vulnerability can expose sensitive data, destroy audit logs, and allow unauthorized modifications.	N/A	More Details

CVE-2026-53354	In the Linux kernel, the following vulnerability has been resolved: arm64: errata: Mitigate TLBI errata on various Arm CPUs A number of CPUs developed by Arm suffer from errata whereby a broadcast TLBI;DSB sequence may complete before the global observation of writes which are translated by an affected TLB entry. These errata ONLY affect the completion of memory accesses which have been translated by an invalidated TLB entry, and these errata DO NOT affect the actual invalidation of TLB entries. TLB entries are removed correctly. This issue has been assigned CVE ID CVE-2025-10263. To mitigate this issue, Arm recommends that software follows any affected TLBI;DSB sequence with an additional TLBI;DSB, which will ensure that all memory write effects affected by the first TLBI have been globally observed. The additional TLBI can use any operation that is broadcast to affected CPUs, and the additional DSB can use any option that is sufficient to complete the additional TLBI. The ARM64_WORKAROUND_REPEAT_TLBI workaround is sufficient to mitigate the issue. Enable this workaround for affected CPUs, and update the silicon errata documentation accordingly. Note that due to the manner in which Arm develops IP and tracks errata, some CPUs share a common erratum number.	N/A	More Details
CVE-2026-50133	Hugo is a static site generator. Prior to 0.162.0, Hugo accepts content files in several markup formats. Files mapped to the text/html media type (typically .html files under /content, or pages produced by a content adapter that sets content.mediaType = "text/html") had their body emitted verbatim into the rendered page. A site that ingests HTML content from an untrusted source could therefore be served stored cross-site scripting. This vulnerability is fixed in 0.162.0.	N/A	More Details
CVE-2026-50134	Hugo is a static site generator. From 0.91.0 until 0.162.0, resources.GetRemote enforces security.http.urls on the URL it is called with, but it did not re-validate intermediate URLs on HTTP 3xx redirects. An allowed server (or an attacker controlling its DNS or response) could therefore redirect the request to a host that the policy was meant to forbid and Hugo would fetch from the redirected target. The same bypass also lifted any host-shape restriction the operator had put in place. This vulnerability is fixed in 0.162.0.	N/A	More Details
CVE-2026-43928	FOSSBilling is a free, open-source billing and client management system. Prior to version 0.8.0, the PayPalEmail payment adapter accepts PayPal IPN callbacks and credits the IPN-supplied amount (`mc_gross`) to the client's balance without validating it against the invoice total. Combined with a $0.05 floating-point epsilon tolerance in the invoice credit-payment logic, this allows a client to underpay an invoice by up to $0.04 and still have it marked as fully paid. Version 0.8.0 patches the issue. There is no effective workaround without modifying the source code. Merchants using the PayPalEmail adapter should monitor IPN transactions for amounts that do not match their corresponding invoice totals, and manually review and refund suspicious payments.	N/A	More Details
CVE-2026-53336	In the Linux kernel, the following vulnerability has been resolved: nvmem: layouts: onie-tlv: fix hang on unknown types The EEPROM on my board has a vendor specific entry of type 0x41. When stumbling upon that, this driver hangs in an endless loop. Fix it by keep incrementing the offset on unknown entries, so the loop will eventually stop.	N/A	More Details
CVE-2026-53335	In the Linux kernel, the following vulnerability has been resolved: mm/damon/lru_sort: handle ctx allocation failure DAMON_LRU_SORT allocates the damon_ctx object for its kdamond in its init function. damon_lru_sort_enabled_store() wrongly assumes the allocation will always succeed once tried. If the damon_ctx allocation was failed, therefore, code execution reaches to damon_commit_ctx() while 'ctx' is NULL. As a result, it dereferences the NULL 'ctx' pointer. Avoid the NULL dereference by returning -ENOMEM if 'ctx' is NULL.	N/A	More Details
CVE-2026-53334	In the Linux kernel, the following vulnerability has been resolved: mm/damon/reclaim: handle ctx allocation failure Patch series "mm/damon/{reclaim,lru_sort}: handle ctx allocation failures". DAMON_RECLAIM and DAMON_LRU_SORT could dereference NULL pointers if their damon_ctx object allocations fail. The bugs are expected to happen infrequently because the allocations are arguably too small to fail on common setups. But theoretically they are possible and the consequences are bad. Fix those. The issues were discovered [1] by Sashiko. This patch (of 2): DAMON_RECLAIM allocates the damon_ctx object for its kdamond in its init function. damon_reclaim_enabled_store() wrongly assumes the allocation will always succeed once tried. If the damon_ctx allocation was failed, therefore, code execution reaches to damon_commit_ctx() while 'ctx' is NULL. As a result, it dereferences the NULL 'ctx' pointer. Avoid the NULL dereference by returning -ENOMEM if 'ctx' is NULL.	N/A	More Details
CVE-2026-53333	In the Linux kernel, the following vulnerability has been resolved: mm/mincore: handle non-swap entries before !CONFIG_SWAP guard mincore_swap() also fields migration/hwpoison entries (and shmem swapin-error entries), which can exist on !CONFIG_SWAP builds when CONFIG_MIGRATION or CONFIG_MEMORY_FAILURE is enabled. The !IS_ENABLED(CONFIG_SWAP) guard ran before the non-swap-entry early return, so mincore_pte_range() can spuriously WARN and report these pages nonresident on !CONFIG_SWAP kernels. Move the guard below the non-swap-entry check so only true swap entries trip the WARN, and migration/hwpoison entries take the existing "uptodate / non-shmem" path.	N/A	More Details
CVE-2026-38973	mrubyc through release3.4.1 was found to contain an out-of-bounds read in builtin missing-method lookup inside mrbc_find_method().	N/A	More Details
	AIL Framework contains a path traversal vulnerability in its PDF object handling. Prior to commit		

CVE-2026-59510	14c618fce4d1df02358717c48ea903706abecdf2, the PDF.get_filepath() function constructed a file path by joining the configured PDF storage directory with a path derived from a PDF object identifier, without verifying that the resolved path remained within the intended PDF_FOLDER directory. An authenticated attacker able to invoke PDF object operations with a crafted identifier could use relative traversal sequences or absolute path components to cause AIL Framework to open files located outside the PDF storage directory. This could allow disclosure of files readable by the AIL process, including application configuration, credentials, or other sensitive local data. This vulnerability is potential due to additional errors before being able to be executed. The fix canonicalises the resulting path with os.path.realpath() and rejects paths whose common directory is outside the configured PDF directory.	N/A	More Details
CVE-2026-38979	ajenti through v2.2.13 has a clickjacking weakness in the browser-facing login and administrative UI. In ajenti-core/aj/http.py, the core HTTP response path initializes an empty header list, forwards handler-added headers verbatim, and finalizes responses through WSGI start_response() without adding anti-framing protections such as X-Frame-Options or a Content-Security-Policy frame-ancestors restriction.	N/A	More Details
CVE-2026-53331	In the Linux kernel, the following vulnerability has been resolved: slimbus: qcom-ngd-ctrl: Avoid ABBA on tx_lock/ctrl->lock During the SSR/PDR down notification the tx_lock is taken with the intent to provide synchronization with active DMA transfers. But during this period qcom_slim_ngd_down() is invoked, which ends up in slim_report_absent(), which takes the slim_controller lock. In multiple other codepaths these two locks are taken in the opposite order (i.e. slim_controller then tx_lock). The result is a lockdep splat, and a possible deadlock: rprocctl/449 is trying to acquire lock: ffff00009793e620 (&ctrl->lock){+.+.}-{4:4}, at: slim_report_absent (drivers/slimbus/core.c:322) slimbus but task is already holding lock: ffff00009793fb50 (&ctrl->tx_lock){+.+.}-{4:4}, at: qcom_slim_ngd_ssr_pdr_notify (drivers/slimbus/qcom-ngd-ctrl.c:1475) slim_qcom_ngd_ctrl which lock already depends on the new lock. Possible unsafe locking scenario: CPU0 CPU1 ---- ---- lock(&ctrl->tx_lock); lock(&ctrl->lock); lock(&ctrl->tx_lock); lock(&ctrl->lock); The assumption is that the comment refers to the desire to not call qcom_slim_ngd_exit_dma() while we have an ongoing DMA TX transaction. But any such transaction is initiated and completed within a single qcom_slim_ngd_xfer_msg(). Prior to calling qcom_slim_ngd_exit_dma() the slim_controller is torn down, all child devices are notified that the slimbus is gone and the child devices are removed. Stop taking the tx_lock in qcom_slim_ngd_ssr_pdr_notify() to avoid the deadlock.	N/A	More Details
CVE-2026-53330	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix out-of-bounds read in dp_get_eq_aux_rd_interval() [Why & How] The aux_rd_interval array in struct dc_lttpr_caps is declared with MAX_REPEATER_CNT - 1 (7) elements, indexed 0..6. However, the offset parameter passed to dp_get_eq_aux_rd_interval() can be as large as MAX_REPEATER_CNT (8) when a sink reports 8 LTTPR repeaters via DPCD. This leads to an out-of-bounds read of aux_rd_interval[7] when offset is 8. Fix this by growing aux_rd_interval to MAX_REPEATER_CNT elements to accommodate the full range of valid repeater counts defined by the DP spec. (cherry picked from commit a55a458a8df37a65ffda5cf721d554a8f74f6b04)	N/A	More Details
CVE-2026-53329	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Use krealloc_array() in dal_vector_reserve() [Why & How] dal_vector_reserve() computes the allocation size as "capacity * vector->struct_size" using uint32_t arithmetic, which can silently wrap to a small value on overflow. This would cause krealloc to return a smaller buffer than expected, leading to heap overflows on subsequent vector appends. Replace krealloc() with krealloc_array() which performs an internal overflow check and returns NULL on wrap, preventing the issue. (cherry picked from commit 37668568641ccc4cc1dbca4923d0a16609dd5707)	N/A	More Details
CVE-2026-43918	FOSSBilling is a free, open-source billing and client management system. Prior to version 0.8.0, when a client or staff/admin account is suspended or marked inactive, existing authenticated sessions are not invalidated. The session identity loaders in src/di.php (loggedin_client and loggedin_admin) only reject sessions if the backing account record no longer exists in the database. They do not verify that the account's status is still active. This allows a suspended or deactivated user to retain full access until their session naturally expires. This issue has been fixed in version 0.8.0.	N/A	More Details
CVE-2026-43921	FOSSBilling is a free, open-source billing and client management system. Versions 0.6.10 through 0.7.2 have a PHP code injection vulnerability in FOSSBilling's `Config::prettyPrintArrayToPHP()` method. When configuration values are updated, string values are written into `config.php` without escaping single quotes. Because `config.php` is loaded via a bare `include` on every HTTP request, an attacker with admin privileges can inject arbitrary PHP code that executes on every subsequent request. Version 0.8.0 contains a patch. Some workarounds are available. Restrict admin access to trusted personnel only; audit `config.php` for unexpected PHP code; and/ or at the reverse proxy/WAF level, restrict access to admin API endpoints that modify configuration.	N/A	More Details
CVE-2026-43925	FOSSBilling is a free, open-source billing and client management system. Prior to version 0.8.0, an unauthenticated mass assignment vulnerability in the client self-registration endpoint allows any visitor to assign themselves to an arbitrary client group during sign-up. Because client groups can gate promo code eligibility, an attacker may apply group-restricted discount codes and receive unauthorized discounts. Version 0.8.0 contains a patch. As a workaround, administrators can either remove group restrictions from promo codes or disable client self-registration (Settings → Clients → Disable signup).	N/A	More Details
	FOSSBilling is a free, open-source billing and client management system. Prior to version 0.8.0, a race condition in the cart checkout flow allows an authenticated client to apply a promo code beyond its		

CVE-2026-43927	configured maximum uses. By sending concurrent checkout requests before any single request completes the usage increment, a client can obtain unlimited discounted or free orders from a single-use or limited-use promo code. Version 0.8.0 patches the issue. Some workarounds are available. Disable promo codes entirely until a patch is available or monitor the `promo` table for `used` values exceeding `maxuses` and manually review affected orders.	N/A	More Details
CVE-2026-53640	FOSSBilling is a free, open-source billing and client management system. Prior to version 0.8.0, low-privileged staff accounts may read sensitive data via admin API endpoints that lack permission checks. While sibling write endpoints correctly enforce fine-grained permissions, the corresponding read endpoints have no authorization guards. Version 0.8.0 contains a fix. Some workarounds are available. Restrict staff accounts to only those who need access to sensitive data and/or use a reverse proxy or WAF to restrict access to the affected endpoints.	N/A	More Details
CVE-2026-53763	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 3.0.0 and prior to version 4.11.0, 32-bit integer overflows in OP-TEE core's AES-GCM implementation cause the authentication tag to be computed with incorrect bit-length values after processing more than 512 megabytes of payload or Additional Authenticated Data (AAD). Version 4.11.0 contains a patch. No known workarounds are available.	N/A	More Details
CVE-2026-53641	FOSSBilling is a free, open-source billing and client management system. Versions 0.6.0 through 0.7.2 have a stored cross-site scripting (XSS) vulnerability in the client-facing email history views of FOSSBilling. Email HTML content (`content_html`) is rendered into a JavaScript template literal using the `|raw` filter, bypassing all output escaping. An attacker with admin access can inject malicious JavaScript payloads into email content that execute in the browser of any client who views their email history. Version 0.8.0 contains a fix. Some workarounds are available. Restrict admin account access, audit email content in the database for suspicious payloads, and/or monitor client accounts for unusual activity.	N/A	More Details
CVE-2026-53642	FOSSBilling is a free, open-source billing and client management system. In versions 0.5.6 through 0.7.2, when the "Require Email Confirmation" setting is enabled, a logged-in client with an unverified email address (`email_approved = 0`) can access all client-area pages (e.g. `/client/balance`, `/client/order/list`, `/client/invoice`) and read real account data, including wallet balances and transaction history. The API-side enforcement correctly restricts unverified clients to only profile-related endpoints, but the page-side enforcement is overly permissive, allowing any request whose path starts with `/client`. Version 0.8.0 contains a fix. No known workarounds that don't involve modifying the source code are available.	N/A	More Details
CVE-2026-53643	FOSSBilling is a free, open-source billing and client management system. Versions prior to 0.8.0 allow low-privileged staff accounts to perform unauthorized actions via admin API endpoints. The root cause is a combination of the `can_always_access` module flag (which grants all staff access to certain modules) and insufficient permission checks or unsafe parameter handling on individual endpoints. Version 0.8.0 contains a fix. Some workarounds are available. Restrict staff accounts to only those who need access to sensitive settings and/or use a reverse proxy or WAF to restrict access to the affected endpoints to trusted IP addresses or higher-privilege roles.	N/A	More Details
CVE-2026-53644	FOSSBilling is a free, open-source billing and client management system. Versions 0.5.3 through 0.7.2 allow authenticated clients to both read and reset API key service secrets for orders that are no longer in an `active` state (e.g., `suspended`, `canceled`). The root cause is missing order-state validation in two client API endpoints, despite an `isActive()` helper already existing in the `Serviceapikey` module and the frontend UI correctly gating access on `order.status == 'active'`. Version 0.8.0 contains a fix. Some workarounds are available. If the `Serviceapikey` module is not needed, uninstall it to remove the affected endpoints. One may also use a reverse proxy or WAF to restrict access to `/api/client/order/service` and `/api/client/serviceapikey/reset` based on application-level order-state logic.	N/A	More Details
CVE-2026-53645	FOSSBilling is a free, open-source billing and client management system. Versions prior to 0.8.0 allow a low-privileged staff account to grant arbitrary module permissions to itself through the admin API, resulting in persistent privilege escalation. A staff user that only has `staff.create_and_edit_staff` can call `/api/admin/staff/permissions_update` targeting their own account and write any permission structure, bypassing the intended role-based access control boundary. Version 0.8.0 patches the issue. Some workarounds are available. Restrict the `staff.create_and_edit_staff` permission to only highly trusted staff members and/or use a reverse proxy or WAF to restrict access to `/api/admin/staff/permissions_update` to specific trusted roles.	N/A	More Details
CVE-2026-53646	FOSSBilling is a free, open-source billing and client management system. In versions 0.5.6 through 0.7.2, when a `ClientPasswordReset` record already exists for a client (from a previous unexpired reset request), subsequent calls to the `reset_password` guest API endpoint reuse the existing token instead of generating a new one. The 15-minute validity window is anchored to the first request's `created_at` timestamp, not the time of the most recent email. An attacker who obtained the original reset link remains able to use it even after the victim requests a new reset, because the original token is never invalidated or rotated. Version 0.8.0 patches the issue. Some workarounds are available. Configure a reverse proxy (e.g., Nginx, Apache, Cloudflare) to apply per-IP rate limiting to the `/client/reset-password` endpoint to minimize the window of opportunity, and/or manually clear expired `client_password_reset` records from the database after a client reports a suspected compromise.	N/A	More Details

CVE-2026-53647	FOSSBilling is a free, open-source billing and client management system. In versions 0.5.3 through 0.7.2, the Guest `serviceapikey/get_info` API endpoint is accessible without authentication. Any caller with a valid API key can retrieve all custom configuration parameters (`custom_*` fields) stored in the key's database record. These custom fields are populated by billing administrators and can contain business-sensitive data such as pricing tiers, feature flags, rate limits, expiry overrides, or access scope data. Version 0.8.0 patches the issue. Some workarounds are available. Administrators can avoid storing sensitive data in `custom_*` API key configuration fields, monitor API logs for suspicious calls to `/api/guest/serviceapikey/get_info`, and/or disable the Serviceapikey module if not in active use.	N/A	More Details
CVE-2026-53648	FOSSBilling is a free, open-source billing and client management system. Prior to version 0.8.1, downloadable product files are stored using a deterministic filename-derived path. When an administrator uploads a file for a downloadable product, FOSSBilling stores the file as `md5(<original filename>)` under the uploads directory. Because the stored path depends only on the client-supplied filename, two different downloadable products, or product/order files, uploaded with the same original filename will resolve to the same stored file path. A later upload can overwrite an earlier upload, causing customers or administrators downloading the earlier product to receive the later file instead. Version 0.8.1 patches the issue. Some workarounds are available. Restrict the `servicedownloadable.manage` permission to fully trusted administrators only. As an operational mitigation, ensure downloadable product files use unique filenames before upload. This reduces accidental collisions but does not fully address the underlying issue.	N/A	More Details
CVE-2026-53328	In the Linux kernel, the following vulnerability has been resolved: sched_ext: Don't warn on NULL cgrp_moving_from in scx_cgroup_move_task() A WARN fires when systemd's user manager writes "+cpu +memory +pids" to its own subtree_control while a sched_ext scheduler is loaded: WARNING: at kernel/sched/ext.c:3227 scx_cgroup_move_task+0xa8/0xb0 scx_cgroup_move_task+0xa8/0xb0 sched_move_task+0x134/0x290 cpu_cgroup_attach+0x39/0x70 cgroup_migrate_execute+0x37d/0x450 cgroup_update_dfl_csses+0x1e3/0x270 cgroup_subtree_control_write+0x3e7/0x440 scx_cgroup_can_attach() arms cgrp_moving_from only when a task's cpu cgroup changes. It can still be NULL when scx_cgroup_move_task() runs, through this sequence: Step Result ---------- ---------- 1. cpu enabled on cgroup G cpu css = A 2. cpu toggled off then on for G A killed, B created (same cgroup) 3. an exiting task keeps A alive migration skips it, A now stale 4. +memory migrates G stale A vs current B pulls cpu in 5. cpu attach runs for all tasks hits a live, cpu-unchanged task 6. scx_cgroup_move_task() on it cgrp_moving_from NULL -> WARN The mismatch is that scx_cgroup_can_attach() keys on cgroup identity while migration drives the move on css identity, so a NULL cgrp_moving_from here is a legitimate css-only migration, not a missing prep. The call is already gated on cgrp_moving_from, so just drop the warning. ops.cgroup_prep_move() and ops.cgroup_move() stay paired.	N/A	More Details
CVE-2026-53327	In the Linux kernel, the following vulnerability has been resolved: debugobjects: Do not fill_pool() if pi_blocked_on On RT enabled kernels, fill_pool() ends up calling rtlock_lock(), which asserts if current::pi_blocked_on is set, because a task can obviously only block on one lock as otherwise the priority inheritenace chain gets corrupted. Prevent this by expanding the conditional to take current::pi_blocked_on into account.	N/A	More Details
CVE-2026-53326	In the Linux kernel, the following vulnerability has been resolved: debugobjects: Don't call fill_pool() in early boot hardirq context When booting a debug PREEMPT_RT kernel on an ARM64 system, a "inconsistent {HARDIRQ-ON-W} -> {IN-HARDIRQ-W} usage" lockdep warning message was reported to the console. During early boot, interrupts are enabled before the scheduler is enabled. In this window (before SYSTEM_SCHEDULING is set) interrupts can fire and in the hard interrupt context handler attempt to fill the pool This can lead to a deadlock when the interrupt occurred when the interrupt hits a region which holds a lock that is required to be taken in the allocation path. Add a new can_fill_pool() helper and reorder the exception rule and forbid this scenario by excluding allocations from hard interrupt context.	N/A	More Details
CVE-2026-13603	The payment integration pretix-oppwa provides support for the payment providers VR Payment, Hobex, and potentially others based on Oppwa's technology. The integration of Oppwa, following their official documentation, includes a step where the user is redirected from the payment provider back to our system with a query parameter like ?resourcePath=/v1/checkouts/{checkoutId}/payment in the URL. Our system is then supposed to fetch the status of the transaction from the URL given by baseUrl + resourcePath. Our plugin pretix-oppwa did so insecurely by concatenating the parameter form the URL to the base domain of the API without further validation and, critically, without a / at the end of the baseUrl. Therefore, an attacker could inject a resourcePath argument in a way that causes pretix to call a different server instead. Since the request includes the access token (API key) of the Oppwa account, this would leak the access token, giving access to data contained in the payment provider's system. This is fixed with the release today by strictly validating the given API URL. After installing the update, we recommend asking your payment provider for a new access token and updating it in pretix.	N/A	More Details
CVE-2026-8387	A vulnerability in allegroai/clearml versions up to and including 1.16.5 allows for relative path traversal when extracting `.zip` archives using the `ZipFile.extractall()` method in `StorageManager._extract_to_cache()`. This issue arises due to the lack of path traversal validation, enabling an attacker to write arbitrary files to the filesystem. Attack vectors include dataset downloads, artifact downloads, model downloads, and offline session imports. The vulnerability can lead to remote code execution through methods such as cron job injection, SSH key overwrite, or web shell deployment. The issue is resolved in version 2.1.6.	N/A	More Details

CVE-2026-53357	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: fix UAF in l2cap_sock_cleanup_listen() vs l2cap_conn_del() bt_accept_dequeue() unlinks a not-yet-accepted child from the parent accept queue and release_sock()s it before returning, so the returned sk has no caller reference and is unlocked. l2cap_sock_cleanup_listen() walks these children on listening-socket close. A concurrent HCI disconnect drives hci_rx_work -> l2cap_conn_del() which runs l2cap_chan_del() + l2cap_sock_kill() and frees the child sk and its l2cap_chan; cleanup_listen() then uses both: BUG: KASAN: slab-use-after-free in l2cap_sock_kill l2cap_sock_kill / l2cap_sock_cleanup_listen / __x64_sys_close Freed by: l2cap_conn_del -> l2cap_sock_close_cb -> l2cap_sock_kill This is distinct from the two fixes already in this area: commit e83f5e24da741 ("Bluetooth: serialize accept_q access") serialises the accept_q list/poll and takes temporary refs inside bt_accept_dequeue(), and CVE-2025-39860 serialises the userspace close()/accept() race by calling cleanup_listen() under lock_sock() in l2cap_sock_release(). Neither covers l2cap_conn_del() running from hci_rx_work, so this UAF still reproduces on current bluetooth/master. Take the reference at the source: bt_accept_dequeue() does sock_hold() while sk is still locked, before release_sock(); callers sock_put(). cleanup_listen() pins the chan with l2cap_chan_hold_unless_zero() under a brief child sk lock (serialising vs l2cap_sock_teardown_cb()), drops it before l2cap_chan_lock(), and skips a duplicate l2cap_sock_kill() on SOCK_DEAD. conn->lock is not taken here: cleanup_listen() runs under the parent sk lock and that would invert conn->lock -> chan->lock -> sk_lock (lockdep). KASAN/SMP: an unprivileged listen/close vs HCI-disconnect race produced 12 use-after-free reports per run before this change; 0, and no lockdep report, over 1600+ raced iterations after it on bluetooth/master.	N/A	More Details
CVE-2026-53337	In the Linux kernel, the following vulnerability has been resolved: net: bonding: fix NULL pointer dereference in bond_do_ioctl() In bond_do_ioctl(), slave_dev is obtained via __dev_get_by_name() which can return NULL if the requested interface name does not exist. However, the subsequent slave_dbg() call is placed before the NULL check: slave_dev = __dev_get_by_name(net, ifr->ifr_slave); slave_dbg(bond_dev, slave_dev, "slave_dev=%p:\n", slave_dev); //here if (!slave_dev) return -ENODEV; The slave_dbg() macro expands to netdev_dbg(bond_dev, "(slave %s): " fmt, (slave_dev)->name, ...) which unconditionally dereferences slave_dev->name before the NULL check is performed. This results in a NULL pointer dereference kernel oops when a user calls bonding ioctl (e.g. SIOCBONDENSLAVE, SIOCBONDRELEASE, etc.) with a non-existent slave interface name. This is reachable from userspace via the bonding ioctl interface with CAP_NET_ADMIN capability, making it a potential local denial-of-service vector. Fix by moving the slave_dbg() call after the NULL check.	N/A	More Details
CVE-2026-53338	In the Linux kernel, the following vulnerability has been resolved: net: airoha: Add NULL check for of_reserved_mem_lookup() in airoha_qdma_init_hfwd_queues() of_reserved_mem_lookup() may return NULL if the reserved memory region referenced by the "memory-region" phandle is not found in the reserved memory table (e.g. due to a misconfigured DTS or a removed memory-region node). The current code dereferences the returned pointer without checking for NULL, leading to a kernel NULL pointer dereference at the following lines: dma_addr = rmem->base; // line 1156 num_desc = div_u64(rmem->size, buf_size); // line 1160 Add a NULL check after of_reserved_mem_lookup() and return -ENODEV if the lookup fails, which is consistent with the existing error handling for of_parse_phandle() failure in the same code block.	N/A	More Details
CVE-2026-14449	u5CMS through v12.8.8 is vulnerable to reflected XSS via the ‘thanks’ parameter in multiple form components	N/A	More Details
CVE-2026-53339	In the Linux kernel, the following vulnerability has been resolved: i2c: qcom-cci: Fix NULL pointer dereference in cci_remove() On all modern platforms Qualcomm CCI controller provides two I2C masters, and on particular boards only one I2C master may be initialized, and in such cases the device unbinding or driver removal causes a NULL pointer dereference, because cci_halt() is called for all two I2C masters, but a completion is initialized only for the single enabled master: % rmmod i2c-qcom-cci Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 <snip> Call trace: __wait_for_common+0x194/0x1a8 (P) wait_for_completion_timeout+0x20/0x2c cci_remove+0xc4/0x138 [i2c_qcom_cci] platform_remove+0x20/0x30 device_remove+0x4c/0x80 device_release_driver_internal+0x1c8/0x224 driver_detach+0x50/0x98 bus_remove_driver+0x6c/0xbc driver_unregister+0x30/0x60 platform_driver_unregister+0x14/0x20 qcom_cci_driver_exit+0x18/0x1008 [i2c_qcom_cci]	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: hsr: Remove WARN_ONCE() in hsr_addr_is_self(). syzbot reported the warning [0] in hsr_addr_is_self(), whose assumption is simply wrong. hsr->self_node is cleared in hsr_del_self_node(), which is called from hsr_dellink(). Since dev->rtnl_link_ops->dellink() is called before unregister_netdevice_many(), there is a window when user can find the device but without hsr->self_node. Let's remove WARN_ONCE() in hsr_addr_is_self(). [0]: HSR: No self node WARNING: net/hsr/hsr_framereg.c:39 at hsr_addr_is_self+0x211/0x3f0 net/hsr/hsr_framereg.c:39, CPU#0: syz.4.16848/17220 Modules linked in: CPU: 0 UID: 0 PID: 17220 Comm: syz.4.16848 Tainted: G L syzkaller #0 PREEMPT_{RT,(full)} Tainted: [L]=SOFTLOCKUP Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 04/18/2026 RIP: 0010:hsr_addr_is_self+0x211/0x3f0 net/hsr/hsr_framereg.c:39 Code: 33 2f 41 0f b7 dd 89 ee 09 de 31 ff e8 c8 b4 c6 f6 09 dd 74 54 e8 0f b0 c6 f6 31 ed eb 53 e8 06 b0 c6 f6 48 8d 3d 2f 50 9c 04 <67> 48 0f b9 3a 31 ed eb 42 e8 c1 13 1f 00 89 c5 31 ff 89 c6 e8 96 RSP: 0018:ffffc900041c70e0 EFLAGS: 00010283 RAX: ffffffff8afdc6ca RBX: ffffffff8afdc4e6 RCX: 0000000000080000 RDX: ffffc90010493000 RSI: 0000000000000948 RDI: ffffffff8f9a1700 RBP:		

CVE-2026-53353	0000000000000001 R08: 0000000000000000 R09: 0000000000000000 R10: ffffc900041c71e8 R11: fffff52000838e3f R12: dfffffc0000000000 R13: ffff888041f9e3c0 R14: ffff888086ee3802 R15: 0000000000000000 FS: 00007f6fe985d6c0(0000) GS:ffff888126176000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f80bd437dac CR3: 0000000025096000 CR4: 00000000003526f0 DR0: ffffffffffffffff DR1: 00000000000001f8 DR2: 0000000000000002 DR3: fffffffeffffff15 DR6: 00000000ffff0ff0 DR7: 0000000000000400 Call Trace: <TASK> check_local_dest net/hsr/hsr_forward.c:592 [inline] fill_frame_info net/hsr/hsr_forward.c:728 [inline] hsr_forward_skb+0xa11/0x2a80 net/hsr/hsr_forward.c:739 hsr_dev_xmit+0x253/0x370 net/hsr/hsr_device.c:236 __netdev_start_xmit include/linux/netdevice.h:5368 [inline] netdev_start_xmit include/linux/netdevice.h:5377 [inline] xmit_one net/core/dev.c:3888 [inline] dev_hard_start_xmit+0x2df/0x860 net/core/dev.c:3904 __dev_queue_xmit+0x1428/0x3900 net/core/dev.c:4870 neigh_output include/net/neighbour.h:556 [inline] ip_finish_output2+0xcec/0x10b0 net/ipv4/ip_output.c:237 ip_send_skb net/ipv4/ip_output.c:1510 [inline] ip_push_pending_frames+0x8b/0x110 net/ipv4/ip_output.c:1530 raw_sendmsg+0x1547/0x1a50 net/ipv4/raw.c:659 sock_sendmsg_nosec net/socket.c:787 [inline] __sock_sendmsg net/socket.c:802 [inline] ____sys_sendmsg+0x7da/0x9c0 net/socket.c:2698 ___sys_sendmsg+0x2a5/0x360 net/socket.c:2752 __sys_sendmsg net/socket.c:2784 [inline] __do_sys_sendmsg net/socket.c:2789 [inline] __se_sys_sendmsg net/socket.c:2787 [inline] __x64_sys_sendmsg+0x1c3/0x2a0 net/socket.c:2787 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0x15f/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f6feb62ce59 Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 e8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f6fe985d028 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007f6feb8a6090 RCX: 00007f6feb62ce59 RDX: 0000000000000000 RSI: 0000200000000000 RDI: 0000000000000004 RBP: 00007f6feb6c2d6f R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007f6feb8a6128 R14: 00007f6feb8a6090 R15: 00007ffcf01cc488 </TASK>	N/A	More Details
CVE-2026-58402	Hugo is a static site generator. From 0.60.0 until 0.163.3, Hugo's default code-block renderer wrote the Markdown code-fence language or info-string into the code class="language-..." data-lang="..." wrapper without HTML escaping. A fence info-string containing a quote and a script payload breaks out of the attribute and injects a live script element. This issue is fixed in 0.163.3.	N/A	More Details
CVE-2026-58403	Hugo is a static site generator. From v0.123.0 through v0.163.0, Hugo's virtual filesystem is designed so that files under a mount cannot reach outside the mount tree, but a regression caused RootMappingFs.statRoot to call Stat, which follows symlinks, instead of Lstat, so a direct os.ReadFile "somefile" where somefile was a symlink pointing outside the mount would return the target's contents. This effectively let a symlink planted inside a theme or local mount read arbitrary files reachable to the user running hugo. This issue is fixed in v0.163.1.	N/A	More Details
CVE-2026-58404	Hugo is a static site generator. From v0.162.0 through v0.163.0, the default security.http.urls policy denies requests to loopback, internal, and cloud-metadata IPv4 literals, but the deny rule only matched dotted-decimal notation, so alternate IPv4 encodings of the same addresses, including integer, hex, or octal, passed the policy. When a template passes an untrusted or data-derived URL to resources.GetRemote and the host platform uses the cgo system resolver, these encodings resolve to the blocked address, allowing build-time server-side requests to loopback and internal services, including the cloud-metadata endpoint in hosted or CI builds; the same check is reused on redirects, so the gap also applies to each redirect hop. This issue is fixed in v0.163.1.	N/A	More Details
CVE-2026-12194	PHPIPAM is affected by an authenticated local file inclusion vulnerability that allows users with access to the API to execute/include arbitrary PHP files on the web server's file system. The API is not enabled by default on installations.	N/A	More Details
CVE-2026-53352	In the Linux kernel, the following vulnerability has been resolved: signal: clear JOBCTL_PENDING_MASK for caller in zap_other_threads() When a multi-threaded process receives a stop signal (e.g., SIGSTOP), do_signal_stop() sets JOBCTL_STOP_PENDING and JOBCTL_STOP_CONSUME on all threads and sets signal->group_stop_count to the number of threads. If one of the threads concurrently calls execve(), de_thread() invokes zap_other_threads() to kill all other threads. zap_other_threads() aborts the pending group stop by resetting signal->group_stop_count to 0 and clears the JOBCTL_PENDING_MASK for all other threads. However, it fails to clear the job control flags for the calling thread. When execve() completes, the calling thread returns to user mode and checks for pending signals. Seeing the stale JOBCTL_STOP_PENDING flag, it calls do_signal_stop(), which invokes task_participate_group_stop(). Since JOBCTL_STOP_CONSUME is still set, it attempts to decrement the already-zero signal->group_stop_count, triggering a warning: sig->group_stop_count == 0 WARNING: CPU: 1 PID: 6475 at kernel/signal.c:373 task_participate_group_stop+0x215/0x2d0 Call Trace: <TASK> do_signal_stop+0x3be/0x5c0 kernel/signal.c:2619 get_signal+0xa8c/0x1330 kernel/signal.c:2884 arch_do_signal_or_restart+0xbc/0x840 arch/x86/kernel/signal.c:337 exit_to_user_mode_loop+0x8c/0x4d0 kernel/entry/common.c:98 do_syscall_64+0x33e/0xf80 arch/x86/entry/syscall_64.c:100 entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> Fix this race condition by clearing the JOBCTL_PENDING_MASK for the calling thread in zap_other_threads(), ensuring it does not retain any stale job control state after the thread group is destroyed. This aligns with other functions that tear down a thread group and abort group stops, such as zap_process() and complete_signal(), which correctly clear these flags for all threads including the current	N/A	More Details

	one.		
CVE-2026-53351	In the Linux kernel, the following vulnerability has been resolved: riscv/ptrace: Use USER_REGSET_NOTE_TYPE for REGSET_CFI Fixes a warning while dumping core: [54983.546369][C7] WARNING: [!note_name] fs/binfmt_elf.c:1771 at elf_core_dump+0x910/0xf68, CPU#7: abort01/31982	N/A	More Details
CVE-2026-53350	In the Linux kernel, the following vulnerability has been resolved: ASoC: wm_adsp: Fix NULL dereference when removing firmware controls In wm_adsp_control_remove() check that the priv pointer is not NULL before attempting to cleanup what it points to. When cs_dsp creates a control it calls wm_adsp_control_add_cb() so that wm_adsp can create its own private control data. There are two cases where private data is not created: 1. The control is a SYSTEM control, so an ALSA control is not created. 2. The codec driver has registered a control_add() callback that hides the control, so wm_adsp_control_add() is not called. When cs_dsp_remove destroys its control list it calls wm_adsp_control_remove() for each control. But wm_adsp_control_remove() was attempting to cleanup the private data pointed to by cs_ctl->priv without checking the pointer for NULL.	N/A	More Details
CVE-2026-53349	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack: destroy stale expectfn expectations on unregister NAT helpers such as nf_nat_h323 store a raw pointer to module text in exp->expectfn (e.g. ip_nat_q931_expect). nf_ct_helper_expectfn_unregister() only unlinks the callback descriptor and never walks the expectation table, so an expectation pending at module removal survives with a dangling exp->expectfn into freed module text. When the expected connection arrives, init_conntrack() invokes exp->expectfn(), now a stale pointer into the unloaded module. Reproduced on a KASAN build by loading the H.323 helpers, creating a Q.931 expectation, unloading nf_nat_h323, then connecting to the expected port: Oops: int3: 0000 [#1] SMP KASAN NOPTI RIP: 0010:0xffffffffa06102d1 init_conntrack.isra.0 (net/netfilter/nf_conntrack_core.c:1862) nf_conntrack_in (net/netfilter/nf_conntrack_core.c:2049) ipv4_conntrack_local (net/netfilter/nf_conntrack_proto.c:223) nf_hook_slow (net/netfilter/core.c:619) __ip_local_out (net/ipv4/ip_output.c:120) __tcp_transmit_skb (net/ipv4/tcp_output.c:1715) tcp_connect (net/ipv4/tcp_output.c:4374) tcp_v4_connect (net/ipv4/tcp_ipv4.c:345) __sys_connect (net/socket.c:2167) Modules linked in: nf_conntrack_h323 [last unloaded: nf_nat_h323] Reaching the dangling state requires CAP_SYS_MODULE in the initial user namespace to remove a NAT helper that still has live expectations, so this is a robustness fix; leaving an expectation pointing at freed text is wrong regardless. Add nf_ct_helper_expectfn_destroy(), which walks the expectation table and drops every expectation whose ->expectfn matches the descriptor being torn down. Call it from each NAT helper's exit path after the existing RCU grace period, so no expectation outlives the code it points at and no extra synchronize_rcu() is introduced. With the fix, the same reproducer runs to completion without the Oops.	N/A	More Details
CVE-2026-53348	In the Linux kernel, the following vulnerability has been resolved: ASoC: SDCA: fix NULL pointer dereference in sdca_dev_unregister_functions sdca_dev_unregister_functions() iterates over all SDCA function descriptors and calls sdca_dev_unregister() on each func_dev without checking for NULL. When a function registration has failed partway through, or the device cleanup races with probe deferral, func_dev entries may be NULL, leading to a kernel oops: BUG: kernel NULL pointer dereference, address: 0000000000000040 RIP: 0010:device_del+0x1e/0x3e0 Call Trace: sdca_dev_unregister_functions+0x37/0x60 [snd_soc_sdca] release_nodes+0x35/0xb0 devres_release_all+0x90/0x100 device_unbind_cleanup+0xe/0x80 device_release_driver_internal+0x1c1/0x200 bus_remove_device+0xc6/0x130 device_del+0x161/0x3e0 device_unregister+0x17/0x60 sdw_delete_slave+0xb6/0xd0 [soundwire_bus] sdw_bus_master_delete+0x1e/0x50 [soundwire_bus] ... sof_probe_work+0x19/0x30 [snd_sof] This was observed on a Lenovo ThinkPad X1 Carbon G14 (Panther Lake) with the SOF audio driver probe failing due to missing Panther Lake firmware, causing the subsequent cleanup of SoundWire devices to trigger the crash. Fix this with three changes: 1) Add a NULL guard in sdca_dev_unregister() so that callers do not need to pre-validate the pointer (defense in depth). 2) In sdca_dev_unregister_functions(), skip NULL func_dev entries and clear func_dev to NULL after unregistration, making the function idempotent and safe against double-invocation. 3) In sdca_dev_register_functions(), roll back all previously registered functions when a later one fails, so the function array is never left in a partially-populated state.	N/A	More Details
CVE-2026-12252	In nltk/nltk versions 3.9.3 and earlier, five Stanford interface classes (StanfordPOSTagger, StanfordNERTagger, StanfordParser, StanfordDependencyParser, and StanfordNeuralDependencyParser) are vulnerable to untrusted JAR code execution. These classes accept user-controllable JAR paths and execute them via the `java()` function, which invokes `subprocess.Popen()` without integrity verification. This vulnerability is identical to CVE-2026-0848, which was fixed for StanfordSegmenter by adding SHA256 verification. However, the fix was not applied to these additional classes, leaving them susceptible to arbitrary code execution when loading untrusted JAR files.	N/A	More Details
CVE-2026-53347	In the Linux kernel, the following vulnerability has been resolved: drm/virtio: Fix driver removal with disabled KMS DRM atomic and modesetting aren't initialized if virtio-gpu driver built with disabled KMS, leading to access of uninitialized data on driver removal/unbinding and crashing kernel. Fix it by skipping shutting down atomic core with unavailable KMS.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: rust: arm64: set uwtable llvm module flag for CONFIG_UNWIND_TABLES Due to a rustc bug [1] the -Cforce-unwind-tables=y flag only emits the uwtable annotation for functions, but not for the module. This means that compiler-generated functions such as 'asan.module_ctor' do not receive the uwtable annotation. When CONFIG_UNWIND_PATCH_PAC_INTO_SCS is		

CVE-2026-53346	enabled, this leads to boot failures because the dwarf information emitted for the kasan constructors is wrong, which causes the SCS boot patching code to patch the constructor in an illegal manner. Specifically, the paciasp instruction is patched, but the autiasp instruction is not. This mismatch leads to a crash when the constructor is called during boot. == BUG: KASAN: global-out-of-bounds in do_basic_setup+0x4c/0x90 Read of size 8 at addr ffffffe3cc7eb488 by task swapper/0/1 Specifically the faulting instruction is the (*fn)() to invoke the constructor in do_ctors() of the init/main.c file. Once the fix lands in rustc, this flag can be made conditional on the rustc version. Note that passing the flag on a rustc with the fix present has no effect. [The fix [1] has landed for Rust 1.98.0 (expected release on 2026-08-20). Thus add a version check as discussed. - Miguel] [Adjusted link and comment. - Miguel]	N/A	More Details
CVE-2026-54430	liboauth2 is vulnerable to Server-Side Request Forgery in oauth2_jose_jwks_aws_alb_resolve() function. The AWS ALB verifier reads both signer and kid from the unverified JWT header. If signer matches the configured ARN, kid is appended to alb_base_url without URL encoding or path sanitization, and the HTTP GET is issued before signature verification. This allows an attacker to force the server to send a GET request to an attacker-chosen internal path. This issue was fixed in version 2.3.0	N/A	More Details
CVE-2026-53345	In the Linux kernel, the following vulnerability has been resolved: KVM: Don't WARN if memory is dirtied without a vCPU when the VM is dying When marking a page dirty, complain about not having a running/loaded vCPU if and only if the VM is still alive, i.e. its refcount is non-zero. This will allow fixing a memory leak for x86 SEV-ES guests without hitting what is effectively a false positive on the WARN. For some SEV-ES VM-Exits, KVM keeps a writable mapping of a guest page across an exit to userspace, and typically unmaps the page on the next KVM_RUN. But if userspace never calls KVM_RUN after such an exit, then KVM needs to unmap the page when the vCPU is destroyed, which in turn triggers the WARN about not having a running vCPU. Alternatively, SEV-ES could temporarily load the vCPU to suppress the WARN, as is done in nested_vmx_free_vcpu() (but for completely unrelated reasons; suppressing WARN from nested_put_vmcs12_pages() is pure happenstance). But loading a vCPU during destruction is gross (ideally nVMX code would be cleaned up), risks complicating the SEV-ES code (KVM would need to ensure the temporarily load()+put() only runs when the vCPU isn't already loaded), and is ultimately pointless. The motivation for the WARN is to guard against KVM dirtying guest memory without pushing the corresponding GFN to the active vCPU's dirty ring, e.g. to ensure userspace doesn't miss a dirty page. But for the VM's refcount to reach zero, there can't be _any_ userspace mappings to the dirty ring, as mapping the dirty ring requires doing mmap() on the vCPU FD. I.e. if userspace had a valid mapping for the dirty ring, then the vCPU file and thus the owning VM would still be alive. And so since userspace can't possibly reach the dirty ring, whether or not KVM technically "misses" a push to the dirty ring is irrelevant.	N/A	More Details
CVE-2026-53344	In the Linux kernel, the following vulnerability has been resolved: pinctrl: mcp23s08: Initialize mcp->dev and mcp->addr before regmap init Regmap initialization triggers regcache_maple_populate() which attempts SPI read to populate cache. SPI read requires mcp->dev and mcp->addr to be set, without them, NULL pointer dereference occurs during probe. Move initialization before mcp23s08_spi_regmap_init() call.	N/A	More Details
CVE-2026-33734	FOSSBilling is a free, open-source billing and client management system. Versions 0.6.0 through 0.7.2 have a SQL injection vulnerability in the `Massmailer` module filter functionality. An authenticated administrator can supply crafted filter values when updating a mass email message, causing untrusted input to be interpolated directly into SQL in the recipient selection query. Version 0.8.0 patches the issue. Some workarounds are available. Restrict administrator access to trusted users only, disable the `Massmailer` module if it is not required, audit existing records in the `mod_massmailer` table for suspicious filter values, and/or review administrator activity related to `Massmailer` message updates.	N/A	More Details
CVE-2026-42331	FOSSBilling is a free, open-source billing and client management system. Prior to version 0.8.0, the Guest API invoice/update endpoint is missing an authorization check present in other invoice-related endpoints, allowing an unauthenticated user with knowledge of an invoice hash to modify the payment gateway associated with an unpaid invoice. An attacker who obtains an invoice hash, which may leak through shared URLs, referrer headers, or email links, can change the `gateway_id` on an unpaid invoice to any payment gateway configured in the system. This does not allow redirecting payments to an arbitrary external endpoint, as the gateway must already be installed and configured by an administrator. The practical impact is further limited by the `invoice_accessible_from_hash` system setting. Version 0.8.0 contains a patch. No known workarounds are available.	N/A	More Details
CVE-2026-42341	FOSSBilling is a free, open-source billing and client management system. Versions 0.6.0 through 0.7.2 have an unauthenticated payment bypass vulnerability in FOSSBilling's IPN callback endpoint. When the Custom payment adapter is enabled, an attacker can mark any unpaid invoice as paid and credit the associated client account without making an actual payment, by sending a single crafted HTTP request. Version 0.8.0 patches the issue. Some workarounds are available. Disable the Custom payment gateway if not actively needed and/or restrict access to `/ipn.php` at the web server level (e.g., via IP allowlisting), noting that this may interfere with legitimate payment callback processing.	N/A	More Details
CVE-2026-54431	In liboauth2 the Demonstrating Proof-of-Possession (DPoP) verifier accepts a proof whose JSON Web Key (jwk) header contains private key material. RFC 9449 section 4.3 step 7 requires the verifier to reject such a proof but oauth2_token_verify() function returns success for a malformed DPoP proof that embeds the private	N/A	More Details

	Elliptic Curve (EC) key in the header. This issue was fixed in version 2.3.0		
CVE-2026-50135	Hugo is a static site generator. From 0.123.0 to 0.161.1, a regression made RootMappingFs.statRoot use Stat (follows symlinks) instead of Lstat , so a direct resources.Get of a symlink pointing outside its mount returned the target's contents — letting a symlink planted in a local mount (e.g. a vendored themes/ theme) read arbitrary files accessible to the Hugo user. Go-module themes from GitHub (symlinks stripped) and directory walks were unaffected. Fixed in 0.162.0.	N/A	More Details
CVE-2026-53343	In the Linux kernel, the following vulnerability has been resolved: ARM: 9475/1: entry: use byte load for KASAN VMAP stack shadow Commit 44e9a3bb76e5 ("ARM: 9430/1: entry: Do a dummy read from VMAP shadow") added a dummy read from the KASAN VMAP stack shadow in __switch_to(). The read uses ldr, but the KASAN shadow address is byte-granular and is not guaranteed to be word aligned. ARMv5 faults unaligned word loads. With CONFIG_KASAN_VMALLOC and CONFIG_VMAP_STACK enabled, ARM926/VersatilePB crashes in __switch_to() with an alignment exception before reaching init. Use ldrb for the dummy shadow access. The code only needs to fault in the shadow mapping if the stack shadow is missing, so a byte load is sufficient and matches the granularity of KASAN shadow memory.	N/A	More Details
CVE-2026-54709	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-54637. Reason: This candidate is a duplicate of CVE-2026-54637. Notes: All CVE users should reference CVE-2026-54637 instead of this candidate.	N/A	More Details
CVE-2026-54763	Traefik is an HTTP reverse proxy and load balancer. Prior to v2.11.51, v3.6.22, and v3.7.6, Traefik's BasicAuth, DigestAuth, and ForwardAuth middlewares strip canonical-cased spoofed identity headers before writing Traefik's own value, but do not account for underscore-variant header names, which many backends normalize identically to dashed forms. An attacker able to reach a protected route can inject an underscore-variant header that survives Traefik's stripping and reaches the backend alongside, or on the unauthenticated ForwardAuth authResponseHeaders path instead of, the value Traefik intended to set, spoofing identity or authorization context. This issue is fixed in versions v2.11.51, v3.6.22, and v3.7.6.	N/A	More Details
CVE-2026-54764	Traefik is an HTTP reverse proxy and load balancer. Prior to v2.11.51, v3.6.22, and v3.7.6, Traefik's ForwardAuth middleware, even when configured with trustForwardHeader: false, derives the X-Forwarded-Port header sent to the authentication service from the original incoming request instead of the sanitized forwarded request. As a result, an unauthenticated remote attacker can inject an X-Forwarded-Proto: https header over a plain HTTP connection and cause Traefik to forward X-Forwarded-Port: 443 to the authentication service, bypassing port-based authorization checks. This issue is fixed in versions v2.11.51, v3.6.22, and v3.7.6.	N/A	More Details
CVE-2026-54765	Traefik is an open source HTTP reverse proxy and load balancer. From v3.7.0 prior to v3.7.6, Traefik's Kubernetes Gateway API provider may resolve two accepted HTTPRoutes that target the same backend Service:port but configure different backendRef filters to the same child service and apply only one route's filter set to all requests reaching that backend. In Gateway deployments where backendRef filters set security-sensitive headers, such as tenant identity, authorization context, or values the backend trusts, an attacker who can create an accepted HTTPRoute sharing the same backend Service:port may cause their route's filter context to be applied to another route's requests, potentially crossing namespace boundaries when a ReferenceGrant permits cross-namespace targeting. This issue is fixed in version v3.7.6.	N/A	More Details
CVE-2026-53342	In the Linux kernel, the following vulnerability has been resolved: arm64: mm: call pagetable dtor when freeing hot-removed page tables Since 5e8eb9aeeda3 ("arm64: mm: always call PTE/PMD ctor in __create_pgd_mapping()") page-table allocation on ARM64 always calls pagetable_{pte,pmd,pud,p4d}_ctor(). This sets the page_type to PGTY_table, increments NR_PAGETABLE and possible allocates a PTL. However the matching pagetable_dtor() calls were never added. With DEBUG_VM enabled on kernel versions prior to v6.17 without 2dfcd1608f3a9 ("mm/page_alloc: let page freeing clear any set page type") this leads to the following warning when freeing these pages due to page->page_type sharing page->_mapcount: BUG: Bad page state in process ... pfn:284fbb page: refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x284fbb flags: 0x17fffc000000000(node=0|zone=2|lastcpupid=0x1ffff) page_type: f2(table) page dumped because: nonzero mapcount Call trace: bad_page+0x13c/0x160 __free_frozen_pages+0x6cc/0x860 ___free_pages+0xf4/0x180 free_pages+0x54/0x80 free_hotplug_page_range.part.0+0x58/0x90 free_empty_tables+0x438/0x500 __remove_pgd_mapping.constprop.0+0x60/0xa8 arch_remove_memory+0x48/0x80 try_remove_memory+0x158/0x1d8 offline_and_remove_memory+0x138/0x180 It can also lead to leaking the ptl allocation if ALLOC_SPLIT_PTLOCKS is defined and incorrect NR_PAGETABLE stats. Fix this by calling pagetable_dtor() in free_hotplug_pgtable_page() prior to freeing the page to undo the effects of calling pagetable_*_ctor().	N/A	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: fhandle: fix UAF due to unlocked ->mnt_ns read in may_decode_fh() may_decode_fh() accesses mount::mnt_ns without holding any locks; that means the mount can concurrently be unmounted, and the mnt_namespace can concurrently be freed after an RCU grace period. This race can happens as follows, assuming that the mount point was created by open_tree(..., OPEN_TREE_CLONE): thread 1 thread 2 RCU __do_sys_open_by_handle_at do_handle_open handle_to_path may_decode_fh is_mounted [mount::mnt_ns access] [mount::mnt_ns access] __do_sys_close fput_close_sync __fput dissolve_on_fput umount_tree class_namespace_excl_destructor namespace_unlock free_mnt_ns mnt_ns_tree_remove call_rcu(mnt_ns_release_rcu) mnt_ns_release_rcu mnt_ns_release kfree	N/A	More Details

53341	[mnt_namespace::user_ns access] **UAF** Fix it by taking rcu_read_lock() around the mount::mnt_ns access, like in __prepend_path(). Additionally, document the semantics of mount::mnt_ns, and use WRITE_ONCE() for writers that can race with lockless readers. This bug is unreachable unless one of the following is set: - CONFIG_PREEMPTION - CONFIG_RCU_STRICT_GRACE_PERIOD because it requires an RCU grace period to happen during a syscall without an explicit preemption. This doesn't seem to have interesting security impact; worst-case, it could leak the result of an integer comparison to userspace (from the level check in cap_capable()), cause an endless loop, or crash the kernel by dereferencing an invalid address.		
CVE-2026-53340	In the Linux kernel, the following vulnerability has been resolved: i2c: imx: fix clock and pinctrl state inconsistency in runtime PM In i2c_imx_runtime_suspend(), the clock is disabled before switching the pinctrl state to sleep. If pinctrl_pm_select_sleep_state() fails, the runtime suspend is aborted but the clock remains disabled, causing a system crash when the hardware is subsequently accessed. Fix this by switching the pinctrl state before disabling the clock so that a pinctrl failure leaves the clock enabled and the hardware accessible. In i2c_imx_runtime_resume(), restore the pinctrl state back to sleep if clk_enable() fails to keep the consistent.	N/A	More Details
CVE-2026-53332	In the Linux kernel, the following vulnerability has been resolved: slimbus: qcom-ngd-ctrl: Register callbacks after creating the ngd When the remoteproc starts in parallel with the NGD driver being probed, or the remoteproc is already up when the PDR lookup is being registered, or in the theoretical event that we get an interrupt from the hardware, these callbacks will operate on uninitialized data. This result in issues to boot the affected boards. One such example can be seen in the following fault, where qcom_slim_ngd_ssr_pdr_notify() schedules work on the NULL ngd_up_work. [21.858578] ------------[cut here]------------ [21.858745] WARNING: kernel/workqueue.c:2338 at __queue_work+0x5e0/0x790, CPU#2: kworker/2:2/116 ... [21.859251] Call trace: [21.859255] __queue_work+0x5e0/0x790 (P) [21.859265] queue_work_on+0x6c/0xf0 [21.859273] qcom_slim_ngd_ssr_pdr_notify+0x110/0x150 [slim_qcom_ngd_ctrl] [21.859304] qcom_slim_ngd_ssr_notify+0x24/0x40 [slim_qcom_ngd_ctrl] [21.859318] notifier_call_chain+0xa4/0x230 [21.859329] srcu_notifier_call_chain+0x64/0xb8 [21.859338] ssr_notify_start+0x40/0x78 [qcom_common] [21.859355] rproc_start+0x130/0x230 [21.859367] rproc_boot+0x3d4/0x518 ... Move the enablement of interrupts, and the registration of SSR and PDR until after the NGD device has been registered. This could be further refined by moving initialization to the control driver probe and by removing the platform driver model from the picture.	N/A	More Details