SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 05 August 2026

Generated on 05 August 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-2026-57834	Apache Traffic Server allows request smuggling if chunked messages are malformed. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	10.0	More Details
CVE-2026-48323	Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Special Elements Used in a Template Engine vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	10.0	More Details
CVE-2026-67429	Flyto2 Core is an execution kernel for automation and AI-agent workflows. Prior to 2.26.6, image.download and related file-writing modules use caller-controlled output_dir instead of validate_path_with_env_config and its FLYTO_SANDBOX_DIR confinement, allowing attacker-controlled response bytes to be written to arbitrary filesystem paths the process can access. This issue is fixed in version 2.26.6.	10.0	More Details
CVE-2026-54735	Prebid Server is an open-source solution for running real-time advertising auctions in the cloud. Prior to version 4.4.0, certain bidder adapters in Prebid Server interpolate user-supplied parameters into outbound request URLs without properly validating host and subdomain values, allowing crafted bid request parameters to cause server-side requests to unintended destinations and potentially expose internal network services or sensitive server endpoints. This issue is fixed in version 4.4.0.	10.0	More Details
CVE-2026-66803	Improper access control in Azure Cosmos DB allows an unauthorized attacker to execute code over a network.	10.0	More Details
CVE-2026-48331	Adobe Campaign Classic (ACC) is affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in privilege escalation. Exploitation of this issue does not require user interaction. Scope is changed.	10.0	More Details
	The Apache Traffic Server certifier plugin generates certificates based on attacker-controlled		

CVE-2026-58162	client SNI. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	10.0	More Details
CVE-2026-48330	Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary SQL commands, potentially gaining elevated access or control over the application. Exploitation of this issue does not require user interaction. Scope is changed.	10.0	More Details
CVE-2026-58150	Apache Traffic Server does not reject Transfer-Encoding in HTTP/2 requests, allowing downgrade request smuggling. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	10.0	More Details
CVE-2026-16326	In consul-mcp-server, versions 0.1.0 up to 0.1.3 did not properly isolate session state in stateless mode, which may allow one client's Consul authentication token to be used for subsequent requests from other clients. This vulnerability (CVE-2026-16326) is fixed in consul-mcp-server 0.1.4.	10.0	More Details
CVE-2026-33267	Improper Input Validation vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 9.2.0 through 9.2.14, from 10.1.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fixes the issue.	10.0	More Details
CVE-2026-48449	Adobe Campaign Classic (ACC) is affected by an Incorrect Authorization 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-2026-18452	DMS+ (Non-Mobile) developed by Rich Source has a Use of Hard-coded Credentials vulnerability. Unauthenticated remote attackers can exploit a fixed API key to gain control over all installed DMS+ devices.	10.0	More Details
CVE-2026-69085	SiYuan before v3.7.3 contains a SQL injection vulnerability in the /api/filetree/searchDocs endpoint, where the caller-supplied keyword parameter is concatenated directly into SQL statements with no escaping or parameter binding. The endpoint is reachable by a publish RoleReader token, or unauthenticated when publish mode is enabled with Publish.Auth.Enable set to false. Because the statement executes on a read-write SQLite handle via a driver that supports stacked (semicolon-separated) statements, an attacker can read and modify database content across all cleartext (non-encrypted) notebooks on the instance.	10.0	More Details
CVE-2026-69084	SiYuan versions <= v3.7.2 expose the /api/search/searchEmbedBlock endpoint, which passes a client-supplied SQL statement verbatim to the main read-write siyuan.db handle with no single-statement, read-only, or admin restrictions. The endpoint is gated only by CheckAuth, making it reachable by the publish RoleReader token and by anonymous users when publish authentication is disabled. Because the underlying driver executes stacked statements, an attacker can read and modify content across all opened cleartext notebooks (encrypted per-box notebooks are excluded). Fixed in v3.7.3.	10.0	More Details
CVE-2026-69083	SiYuan versions before v3.7.3 contain SQL injection vulnerabilities in the fullTextSearchAssetContent endpoint reachable by unauthenticated users and publish RoleReader tokens. Attackers can execute arbitrary SQL on the read-write asset-content database via unescaped method parameters and REGEXP clauses to read, modify, or delete cross-notebook data.	10.0	More Details
CVE-2026-54680	Logging operator automates the deployment and configuration of Kubernetes logging pipelines. Prior to 6.6.0, the Fluentd configuration renderer FluentRender in pkg/sdk/logging/model/render/fluent.go writes CRD strings such as Flow record_transformer.records values directly into fluent.conf without escaping, allowing a user who can create Flow resources to inject a Fluentd <match **> block using @type exec and execute arbitrary commands inside the Fluentd aggregator. This issue is fixed in version 6.6.0.	9.9	More Details
CVE-2026-48326	Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could result in arbitrary code execution in the context of the current user. A low-privileged attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	9.9	More Details

CVE-2026-17566	pgAdmin 4's Import/Export Data tool builds a psql \copy (...) command line by interpolating a user-supplied SQL query into a Jinja template and passing the rendered line to psql via --command. To stop an attacker from breaking out of the (...) wrapper, create_import_export_job() (route POST /import_export/job/<sid>, gated only by the ordinary, commonly-granted tools_import_export_data permission) validated the query with a hand-written parenthesis-balance checker, _is_query_parens_balanced(). That checker always treated a backslash before a single quote (\') as escaping the quote, i.e. as if standard_conforming_strings were off. PostgreSQL has defaulted standard_conforming_strings to on since 9.1 (2010), the default on every PostgreSQL version pgAdmin 4 currently supports (13-18); under that default psql's own \copy tokenizer treats \ as an ordinary character, so a single quote immediately after it closes the string literal. A query such as SELECT 'a\') TO PROGRAM 'echo pwned' x' was therefore accepted as "balanced" by pgAdmin's checker (which believed the) was still inside the string), while psql, run through the actual rendered command line, closes the string at that point and treats the following) as the end of the wrapping \copy (...) subquery, exposing an attacker-chosen TO PROGRAM '<command>' clause that psql executes via popen() -- independent of a subsequent syntax error later on the same line. This is the same class of bug as CVE-2025-12762/CVE-2025-13780 (RCE via psql meta-command/COPY injection during PLAIN-format dump restore), reached through an independently written defense in a different module (Import/Export Data rather than Restore) that had its own, different logic bug (inverted backslash-escape semantics rather than a BOM-defeated regex anchor). The fix rejects any backslash inside a single-quoted string in the query outright, rather than picking one of the two possible psql interpretations. This is intentionally conservative: because the correct interpretation of \ depends on the target server's standard_conforming_strings setting, which the checker cannot reliably know at validation time, refusing the query is safer than guessing. This issue affects pgAdmin 4: from the introduction of _is_query_parens_balanced() before 9.18.	9.9	More Details
CVE-2026-58046	Improper neutralization in the Plesk XML-RPC API allows a remote authenticated low-privileged user to perform SQL injection and read arbitrary data from the Plesk database, leading to full compromise of the panel.	9.9	More Details
CVE-2026-52855	Wings is the server control plane for Pterodactyl, a free, open-source game server management panel. Prior to 1.12.3, {{config.}} placeholders in egg configuration-file templates allow a low-privileged user to read {{config.token}}, {{config.token_id}}, and {{config.docker.registries}} from the full daemon configuration. This issue is fixed in version 1.12.3.	9.9	More Details
CVE-2026-13435	IBM Langflow OSS 1.0.0 through 1.10.1 contains an improper input validation vulnerability in the PythonREPL sandbox implementation.	9.9	More Details
CVE-2026-67330	@better-auth/scim (a better-auth plugin) versions >= 1.4.0-beta.27 through <= 1.6.21 and >= 1.7.0-beta.0 through <= 1.7.0-beta.9 contain an authorization bypass. SCIM token issuance did not reject provider IDs already used by existing SSO, SAML, OIDC, generic OAuth, or social account providers, and the same logical provider ID was used for both SCIM provider configuration and account ownership. An authenticated user could mint a SCIM token whose provider ID collided with an existing provider namespace, causing SCIM user routes to resolve account rows the token never provisioned. This allowed listing, reading, updating (including rewriting global profile/email fields without uniqueness checks), and deleting global user accounts and sessions, resulting in account takeover and unauthorized deprovisioning. Fixed in 1.6.22 and 1.7.0-beta.10 (1.7.0-rc.0).	9.9	More Details
CVE-2026-63233	A SQL injection and unsafe deserialisation vulnerability in Koollab LMS allowed an authenticated attacker to inject through the assessment overall answer endpoint, control data passed to unserialize(), write a webshell to a publicly accessible location, and execute arbitrary code on the server.	9.9	More Details
CVE-2026-63232	A SQL injection and unsafe deserialisation vulnerability in Koollab LMS allowed an authenticated attacker to inject through the assessment reinforcement endpoint, control data passed to unserialize(), write a webshell to a publicly accessible location, and execute arbitrary code on the server.	9.9	More Details
CVE-2026-12946	IBM Langflow OSS 1.0.0 through 1.10.0 could allow a remote attacker to inject arbitrary code on the system, due to the improper control of user input code.	9.9	More Details
CVE-2026-63227	An unrestricted SCORM file upload vulnerability in Koollab LMS allowed an authenticated module designer to upload a SCORM package containing a PHP webshell to a publicly	9.9	More Details

	accessible directory and execute arbitrary code on the server.		
CVE-2026-63234	A SQL injection and unsafe deserialisation vulnerability in Koollab LMS allowed an authenticated attacker to inject through the manual mark assessment endpoint, control data passed to unserialize(), write a webshell to a publicly accessible location, and execute arbitrary code on the server.	9.9	More Details
CVE-2025-69936	CodeAstro Membership Management System 1.0 is vulnerable to SQL Injection in /edit_member.php?id=1.	9.8	More Details
CVE-2025-69946	SourceCodester Modern Loan Management System 1.0 is vulnerable to SQL Injection in ajaxData.php via the parameters district_id , division_id, region_id, and ward_id.	9.8	More Details
CVE-2026-16504	Deployment of the VPS.org one-click Zulip template deploys a hardcoded application signing key, a default database password ("zulip"), and DISABLE_HTTPS=True.	9.8	More Details
CVE-2026-15971	SGLang contains an RCE vulnerability when the optional dumper subsystem is enabled, allowing for a sandbox escape when DUMPER_SERVER_PORT is set, enabling code execution on inference requests.	9.8	More Details
CVE-2026-15969	SGLang contains an unauthenticated RCE in /load_lora_adapter_from_tensors via bypass of SafeUnpickler’s incomplete denylist, allowing arbitrary command execution through crafted base64-encoded pickle payloads.	9.8	More Details
CVE-2026-67822	Tenda W6-S 1.0.0.4(510) contains a stack-based buffer overflow vulnerability in the /goform/wifiSSIDset endpoint. The function formwrlSSIDset uses sprintf to copy user-controlled 'GO' and 'index' parameters into a 64-byte stack buffer without length restriction, leading to stack overflow.	9.8	More Details
CVE-2026-38711	TR1200 v2.4.15, TR3000 v2.4.21, WR300 v2.4.25, WR1200 v2.4.23, WR1300 v2.4.22, WR1500 v2.3.10, WR3000 v2.4.19, WR3600 v2.3.16, and WR6500 v2.3.15 were discovered to contain a command injection vulnerability in the system.upgrade_check interface. This vulnerability allows attackers to execute arbitrary commands as root via a crafted input.	9.8	More Details
CVE-2025-69948	SourceCodester Modern Loan Management System 1.0 is vulnerable to SQL Injection in /admin/delete_group.php?id=1.	9.8	More Details
CVE-2026-38708	TR1200 v2.4.15, TR3000 v2.4.21, WR300 v2.4.25, WR1200 v2.4.23, WR1300 v2.4.22, WR1500 v2.3.10, WR3000 v2.4.19, WR3600 v2.3.16, and WR6500 v2.3.15 were discovered to contain a command injection vulnerability in the system.setclock interface. This vulnerability allows attackers to execute arbitrary commands as root via a crafted input.	9.8	More Details
CVE-2026-38713	TR1200 v2.4.15, TR3000 v2.4.21, WR300 v2.4.25, WR1200 v2.4.23, WR1300 v2.4.22, WR1500 v2.3.10, WR3000 v2.4.19, WR3600 v2.3.16, and WR6500 v2.3.15 were discovered to contain a command injection vulnerability in the ipsec_conn interface. This vulnerability allows attackers to execute arbitrary commands as root via a crafted input.	9.8	More Details
CVE-2026-51785	An issue in Hugo Leisink Hiawatha v.12.1 and before allows a remote attacker to execute arbitrary code via a crafted request	9.8	More Details
CVE-2026-68770	sentence-transformers contains a security control bypass vulnerability that allows attackers to achieve arbitrary code execution by exploiting a logic flaw in the import_module_class helper within sentence_transformers/util/misc.py, where the guard condition includes an 'or os.path.exists(model_name_or_path)' clause that satisfies the trust gate whenever the supplied path exists on the local filesystem, regardless of the trust_remote_code=False argument. Attackers who can control or influence the contents of a model directory on disk can place malicious Python files such as modeling_*.py referenced via modules.json, causing the code to execute at import time when an application loads the model with SentenceTransformer(path, trust_remote_code=False), bypassing the documented security contract and achieving code execution within the loading process.	9.8	More Details
CVE-2026-52134	An issue in the parseGoosePayload() function (/goose/goose_receiver.c) of libiec61850 v1.6 allows attackers to bypass authentication via a captured GOOSE frame.	9.8	More Details
CVE-2026-	ComfyUI v0.23.0 contains an unsafe deserialization vulnerability in the LoadTrainingDataset node that allows unauthenticated remote attackers to execute arbitrary Python code by uploading a crafted pickle file and triggering its deserialization. Attackers can upload a		More

68771	malicious shard_*.pkl file via the unauthenticated POST /upload/image endpoint and then queue a workflow graph via POST /prompt referencing the uploaded file, causing torch.load to deserialize the attacker-controlled pickle payload using __reduce__ and execute arbitrary commands as the ComfyUI process user.	9.8	Details
CVE-2026-15964	The Single Sign On For TNG plugin for WordPress is vulnerable to Authentication Bypass via unauthenticated password reset in all versions up to, and including, 2.0.0. This is due to the `ssoprocess_ajax()` function — registered on `wp_ajax_nopriv_ssoprocess_ajax` and therefore reachable without authentication — accepting an attacker-supplied `email` parameter with the `setnewpassword` operation and calling `reset_password()` on the resolved account without any ownership token, email confirmation link, or capability check. The sole guard is a call to `check_ajax_referer()`, which provides no authorization barrier because the `ssoajaxnonce` nonce is publicly broadcast on every front-end page via `wp_localize_script()` into the `SSOPWDREQUIREMENT` JavaScript object; since WordPress computes nonces for logged-out visitors against a shared anonymous session context, any unauthenticated visitor can scrape a valid nonce from the homepage and use it to authenticate the request. This makes it possible for unauthenticated attackers to change the password of any WordPress account, including administrator accounts, enabling complete site takeover.	9.8	More Details
CVE-2026-66402	FreeRDP before 3.29.0 (affected versions <= 3.28.0) contains multiple TLS certificate identity validation weaknesses in tls_verify_certificate(), tls_match_hostname(), and x509_utils_get_dns_names(). Because FreeRDP performs custom Common Name and DNS SAN string matching instead of using OpenSSL's length-aware identity validation APIs, it (1) truncates DNS SAN values at embedded NUL bytes (accepting e.g. 'victim.example\0.attacker.example' as 'victim.example'), (2) accepts a matching Common Name even when non-matching DNS SAN entries are present, and (3) accepts IP-literal targets via DNS/CN matching without comparing iPAddress SANs. Under a trusted or misissued certificate chain, an attacker positioned to present such a certificate can bypass server identity verification, weakening TLS server authentication.	9.8	More Details
CVE-2026-67289	FreeRDP before 3.29.0 (affected versions <= 3.28.0) does not validate CRLF and control characters in the server-controlled RDP redirection TargetNetAddress field. This value is copied into the client's ServerHostname and, when the client connects through an HTTP proxy, is written directly into the proxy CONNECT request line and Host header by http_proxy_connect() without filtering. A malicious or compromised RDP server can send a crafted redirection PDU containing embedded control characters to inject arbitrary headers/requests into the HTTP proxy CONNECT request.	9.8	More Details
CVE-2026-17561	Improper Control of Generation of Code ('Code Injection') vulnerability in Innotim Software, Telecommunications and Consulting Trade Ltd. Co. Logsign SIEM allows Code Injection. This issue affects Logsign SIEM: before 6.4.108.	9.8	More Details
CVE-2026-14919	The ShopMonitor.io WordPress plugin before 1.2.0 does not properly restrict its email-rerouting test mode, gating it behind a trusted-source check that is satisfiable with client-supplied request headers, allowing unauthenticated attackers to redirect outgoing emails, including the WordPress administrator password-reset email, to an address they control and take over the administrator account.	9.8	More Details
CVE-2025-69935	CodeAstro Membership Management System 1.0 is vulnerale to SQL Injection in the report.php and revenue_report.php via the fromDate parameter.	9.8	More Details
CVE-2025-69930	CodeAstro Membership Management System 1.0 is vulnerable to SQL Injection in /print_membership_card.php?id=1.	9.8	More Details
CVE-2025-69937	CodeAstro Membership Management System 1.0 is vulnerable to SQL Injection in the edit_type.php endpoint via the Parameter id.	9.8	More Details
CVE-2025-69938	CodeAstro Membership Management System 1.0 is vulnerable to SQL Injection in renew.php via the parameter membershipType.	9.8	More Details
CVE-2025-69934	CodeAstro Membership Management System 1.0 is vulnerable to SQL Injection in /delete_members.php?id=1.	9.8	More Details
CVE-2025-69941	SourceCodester Tailor Management System 1.0 is vulnerable to SQL Injection in addmeasurement.php?id=1.	9.8	More Details
CVE-2025-	CodeAstro Membership Management System 1.0 is vulnerable to SQL Injection in	9.8	More

69933	/memberProfile.php?id=1.		Details
CVE-2025-69947	SourceCodester Tailor Management System 1.0 is vulnerable to SQL Injection in customeredit.php?id=1.	9.8	More Details
CVE-2026-35847	An issue in dnsmgr v.2.15 and before allows a local attacker to execute arbitrary code via the ping function of the CheckUils.php file	9.8	More Details
CVE-2025-69931	CodeAstro Membership Management System 1.0 is vulnerable to SQL Injection in /delete_membership.php?id=1.	9.8	More Details
CVE-2026-67324	GitPython 3.1.50 fails to recognize joined short-option forms such as -u<value> (the short form of --upload-pack=<value>) when enforcing its default unsafe-option gate. When an application passes attacker-influenced clone options into Repo.clone_from(..., multi_options=..., allow_unsafe_options=False), an attacker can supply -u<helper> to bypass the gate that blocks --upload-pack/-u, causing Git to execute the specified helper command during clone. Fixed in 3.1.51.	9.8	More Details
CVE-2026-14483	The Realtyna Organic IDX plugin + WPL Real Estate plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 5.2.0 via the upload function. This is due to missing file type validation in the upload function, combined with a publicly accessible I/O endpoint authenticated solely by static, plugin-seeded API credentials that are identical across all installations. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible. The WPL I/O service endpoint is registered on the public WordPress init hook with no WordPress capability check, and the required api_key and api_secret values are static defaults seeded by the plugin's own SQL migration files, meaning any unauthenticated attacker who knows these publicly documented defaults can reach and exploit the vulnerable upload path.	9.8	More Details
CVE-2026-68503	LazyOwn RedTeam/APT Framework is an AI-powered C2 and red-team operations framework. Prior to 0.2.154, LazyOwn ships default C2 credentials LazyOwn and LazyOwn in payload.json and core/payload_schema.py and passes them unchanged to lazyc2.py HTTP Basic authentication, allowing any network-reachable attacker who knows the defaults to authenticate to the C2 dashboard with operator-level access. This issue is fixed in 0.2.154.	9.8	More Details
CVE-2025-65336	Ecommerce-project-with-php-and-mysqli-Fruits-Bazar 1.0 is vulnerable to SQL Injection in /show_price_by_pdtId.php.	9.8	More Details
CVE-2026-13423	The Streamit WordPress theme through 4.5.0 does not perform any authorization or nonce verification on one of its unauthenticated AJAX routes, which invokes an attacker-supplied PHP function with an attacker-supplied argument array, allowing unauthenticated attackers to call arbitrary functions (for example to create an administrator account), leading to privilege escalation and remote code execution.	9.8	More Details
CVE-2026-67208	Juggle through 1.6.0 contains a remote code execution vulnerability that allows unauthenticated remote attackers to execute arbitrary OS commands by connecting to the exposed H2 database web console using default shipped credentials. Attackers can access the unprotected /h2-console endpoint, authenticate with default credentials, and leverage the H2 CREATE ALIAS Runtime.exec() technique to execute arbitrary commands, resulting in root-level code execution when running the stock Docker image.	9.8	More Details
CVE-2026-15976	SGLang contains a RCE vulnerability when attempting to load model weights from a HuggingFace repository, specifically within the /update_weights_from_disk, where torch.load(..., weights_only=False) fallback enables pickle deserialization of .bin files.	9.8	More Details
CVE-2026-38709	TR1200 v2.4.15, TR3000 v2.4.21, WR300 v2.4.25, WR1200 v2.4.23, WR1300 v2.4.22, WR1500 v2.3.10, WR3000 v2.4.19, WR3600 v2.3.16, and WR6500 v2.3.15 were discovered to contain a command injection vulnerability in the net.set_wan interface. This vulnerability allows attackers to execute arbitrary commands as root via a crafted input.	9.8	More Details
CVE-2026-43830	Full details and mitigation steps are currently restricted and will be published at a later date.	9.8	More Details
CVE-2026-	CodeIgniter is a PHP full-stack web framework. Prior to 4.7.4, the is_image and mime_in upload validation rules do not independently enforce a safe client filename extension, allowing a remote attacker to upload executable content when an application preserves the client filename and stores uploads in a web-accessible script-enabled directory. Applications are	9.8	More

63223	impacted when they validate uploads using is_image or mime_in without an independent safe extension check (such as ext_in on patched versions), save uploaded files using the client-supplied filename, and place uploads in a web-accessible directory where PHP files can execute. This issue is fixed in version 4.7.4.		Details
CVE-2026-68502	LazyOwn RedTeam/APT Framework is an AI-powered C2 and red-team operations framework. Prior to 0.2.154, LazyOwn's lazyc2.py registers an unauthenticated Socket.IO input event handler that dispatches data.get('value') to LazyOwnShell.one_cmd, reaching LazyOwnShell.do_cmd and subprocess.call(command, shell=True), allowing unauthenticated remote code execution in the C2 process. This issue is fixed in 0.2.154.	9.8	More Details
CVE-2026-18072	The Advanced Responsive Video Embedder for Rumble, Odysee, YouTube, Vimeo, Kick ... plugin for WordPress is vulnerable to Authentication Bypass via a Hardcoded Backdoor in version 10.8.7. The vulnerability exists because the `_arve_uc_init()` function — registered on WordPress's `init` hook at priority 1 so that it runs before any authentication checks on every request — reads an attacker-supplied token from the `_wplogin` (or `_wpm`) parameter and compares it against a hardcoded SHA-256 hash embedded directly in the plugin source, with no nonce verification, no capability check, and no password validation anywhere in the flow. Because this static hash constitutes a set of universal credentials that are publicly accessible in the plugin's source code, unauthenticated attackers can supply the known token to be authenticated as an arbitrarily selected existing administrator account, gaining full administrative control over the affected WordPress site. This was likely introduced by an attacker who gained commit access to the developers account.	9.8	More Details
CVE-2026-67340	ArcadeDB before 26.7.2 (arcadedb-engine) allows trigger scripts to look up host classes in java.lang.* (via Java.type) because ScriptTriggerExecutor adds java.lang.* to the allowed packages. An authenticated user with UPDATE_SCHEMA permission can create a JavaScript trigger that invokes java.lang.Runtime.getRuntime().exec() (or ProcessBuilder), achieving OS command execution when the trigger fires.	9.8	More Details
CVE-2026-63456	Multiple vulnerabilities in the REST API interface of HPE Networking SD-WAN Orchestrator could allow an unauthenticated remote attacker to bypass web authentication mechanisms and access system functions. Successful exploitation could allow an attacker to view and modify potentially sensitive information on the target system.	9.8	More Details
CVE-2026-18686	A vulnerability was detected in GL.iNet GL-MT3000 up to 4.4.5. The affected element is the function nas-web.add_user of the file /cgi-bin/glc of the component nas-web RPC Wrapper. Performing a manipulation results in command injection. The attack can be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	9.8	More Details
CVE-2026-16618	The Improve SEO WordPress plugin through 2.0.11 does not properly validate uploaded files, checking only the file content type while writing the file with the attacker-supplied extension into a publicly accessible directory, allowing unauthenticated users to upload executable PHP files and achieve remote code execution.	9.8	More Details
CVE-2026-14175	Unrestricted upload of file with dangerous type vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Upload a Web Shell to a Web Server. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	9.8	More Details
CVE-2026-15721	Cleartext storage of sensitive information vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows SQL Injection. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	9.8	More Details
CVE-2026-61514	Puwell IP Camera firmware versions 2.x through 4.x contains an authentication bypass vulnerability that allows unauthenticated attackers to access device functions by sending protocol-conforming packets over TCP port 23456 without credentials. Attackers can exploit the unvalidated Session field in the proprietary control protocol header to access live video streams, control pan and tilt motors, activate audio functions, and remotely restart the device.	9.8	More Details
CVE-2026-61515	Puwell IP Camera firmware versions 2.x through 4.x contains an unauthenticated command injection vulnerability that allows remote attackers to execute arbitrary operating system commands by sending a crafted JSON payload to the DebugShell interface exposed on TCP port 34567. Attackers can exploit the lack of authentication and input sanitization in the binary protocol service to pass arbitrary commands directly to the underlying operating system, achieving root-level code execution and complete device compromise.	9.8	More Details

CVE-2026-69098	kotaemon through 0.12.0 contains an insecure deserialization vulnerability in the check_connection endpoint that allows unauthenticated attackers to instantiate arbitrary Python classes by supplying crafted YAML/JSON input with a __type__ field. Attackers can exploit this to override the __type__ field with subprocess.check_output and arbitrary arguments, achieving remote code execution with application process privileges.	9.8	More Details
CVE-2025-29296	H3C Magic BE18000 V200R007, H3C NX400 V100R015, H3C Magic NX30 Pro V100R0011, H3C Magic R3010 V100R009, H3C Magic NX15 V100R017, H3C Magic R1510 V100R016, and H3C NE36 Pro V100R002 contain multiple command injection vulnerabilities in the /api/esps request handler. The affected object interfaces and methods are esps.dhcpd.vlan (getlist, delete), esps.filter.url (add, modify), esps.apcm.version (delete, H3C Magic NX15 only), esps.swcm.version (delete, upgrade, all affected models except H3C Magic NX15), and esps.system.ntp (set, all affected models except H3C Magic NX15). Attacker-controlled request parameters are incorporated into shell expressions executed by eval without adequate validation, allowing a remote attacker to execute arbitrary commands as root and gain complete control of the affected device.	9.8	More Details
CVE-2026-63455	Multiple vulnerabilities in the REST API interface of HPE Networking SD-WAN Orchestrator could allow an unauthenticated remote attacker to bypass web authentication mechanisms and access system functions. Successful exploitation could allow an attacker to view and modify potentially sensitive information on the target system.	9.8	More Details
CVE-2026-24254	NVIDIA Dynamo for Linux contains a vulnerability in the multimodal serving topology, where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	9.8	More Details
CVE-2026-48333	Adobe Campaign Classic (ACC) is affected by an Incorrect Authorization vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain elevated privileges. Exploitation of this issue does not require user interaction.	9.8	More Details
CVE-2017-20241	Keysight IxChariot Endpoint before 9.5.102 contains a heap-based buffer overflow. An unauthenticated remote attacker can send a specially crafted packet to crash the endpoint or potentially execute arbitrary code.	9.8	More Details
CVE-2017-20242	Keysight IxChariot Endpoint before 9.5.102 contains a stack-based buffer overflow. An unauthenticated remote attacker can send a specially crafted packet to crash the endpoint or potentially execute arbitrary code.	9.8	More Details
CVE-2026-0163	In multiple functions of vpu_ioctl.c, there is a possible use after free due to a use after free. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2026-49435	Keysight IxChariot Endpoint and associated products contain a stack-based buffer overflow. An unauthenticated remote attacker can send a specially crafted packet and execute arbitrary code with administrative privileges.	9.8	More Details
CVE-2026-69703	Atlas-Livre contains an improper access control vulnerability in the admin controllers under Espace_admin/controleur/ that allows unauthenticated attackers to bypass session-based authentication guards by sending raw HTTP requests that ignore redirects. Attackers can invoke destructive admin actions such as record deletion by requesting controller endpoints with GET parameters like supp, because the PHP header() redirect is never followed by an exit or die call, allowing all subsequent code including database operations to execute regardless of session state.	9.8	More Details
CVE-2026-70552	MaxSite CMS 109.5 and earlier contains an authentication bypass vulnerability in the AJAX dispatcher that allows unauthenticated attackers to access admin-gated endpoints by supplying any X-Requested-With header and requesting a base64-encoded path resolving to any *-ajax.php file in the codebase. Attackers can exploit this dispatcher bypass to reach privileged plugin endpoints without credentials, enabling actions such as manipulating poll states and vote counts, and amplifying the impact of any dangerous operation performed by admin-only ajax files across the plugin tree.	9.8	More Details
CVE-2026-	MaxSite CMS contains a remote code execution vulnerability that allows unauthenticated attackers to inject arbitrary PHP code into the application configuration file by submitting crafted POST requests to the install endpoint after installation is complete. Attackers can supply a malicious db_dbprefix value containing a single quote to break out of a PHP string	9.8	More

70553	literal in application/config/database.php, appending attacker-controlled PHP statements that are executed by the web server on every subsequent request, resulting in persistent unauthenticated remote code execution as the web-server process user.		Details
CVE-2026-45538	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. In versions 4.0.0 and prior, processing a SIP message with a header name longer than 255 bytes causes a stack buffer overflow when sip_to_json() is called in the routing script. Function sip_to_json() (modules/sipmsgops/sipmsgops.c) copies SIP header names into a fixed 255-byte stack buffer without bounds checking, performing a memcpy of the full header-name length even though the SIP parser imposes no such limit (a header name can be roughly 65000 bytes). As a result, when a routing script calls sip_to_json(), a SIP message with a header name longer than 255 bytes triggers a stack buffer overflow in which both the length and content of the overwrite are attacker-controlled, corrupting the saved frame pointer and return address. A single unauthenticated UDP packet to the SIP port (5060) can crash the process or, on builds without stack protections, hijack the return address to achieve remote code execution. This affects deployments whose routing script invokes sip_to_json(). This issue was not fixed at the time of publication.	9.8	More Details
CVE-2026-70554	MaxSite CMS contains a PHP object injection vulnerability that allows unauthenticated attackers to execute arbitrary code by passing attacker-controlled serialized data in the maxsite_comuser cookie directly to unserialize() without validation or class allowlisting. Attackers can craft a malicious serialized PHP object payload delivered in a single HTTP request to trigger magic methods during object graph reconstruction, enabling property-oriented programming attacks or remote code execution via available gadget chains such as those targeting SoapClient or Imagick extensions.	9.8	More Details
CVE-2026-18685	A security vulnerability has been detected in GL.iNet GL-MT3000 up to 4.4.5. Impacted is the function set_upgrade of the file /cgi-bin/glc of the component modem.so. Such manipulation leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	9.8	More Details
CVE-2026-18684	A weakness has been identified in GL.iNet GL-MT3000 up to 4.4.5. This issue affects the function remove_profile of the file /cgi-bin/glc of the component modem.so. This manipulation causes command injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	9.8	More Details
CVE-2026-67341	ArcadeDB versions before 26.7.2 fail to enforce scripting authorization checks on the SQL DEFINE FUNCTION statement with LANGUAGE js. Attackers with database access can execute arbitrary JavaScript code by submitting DEFINE FUNCTION statements, bypassing security controls intended to restrict scripting to administrators.	9.8	More Details
CVE-2026-18108	Net::SAML2 versions before 0.86 for Perl allow authentication bypass because _verify_encrypted_assertion accepts an EncryptedAssertion whose decrypted content carries no signature. _verify_encrypted_assertion decrypts the EncryptedAssertion and returns it as verified when it carries no signature, via "return $xml unless $xpath->exists('dsig:Signature', $assert);". The signature check and the trust anchor check that follow run only when a signature is present, so a decrypted assertion with no dsig:Signature element reaches new_from_xml unverified and its NameID and attributes are read into the assertion object. An SP's encryption certificate is published in its SAML metadata so the IdP can encrypt to it, so any party can encrypt an unsigned assertion to that certificate, wrap it in a samlp:Response, and post it to the assertion consumer service. Any caller that configures a decryption key_file, and so accepts EncryptedAssertions, takes identity fields from an assertion that no trust anchor covers, and an unauthenticated party can authenticate as an arbitrary user. Callers with no key_file configured do not decrypt and are unaffected.	9.8	More Details
CVE-2026-67342	ArcadeDB versions before 26.7.2 contain an authorization bypass vulnerability in HTTP handlers for time series, batch, Prometheus, and Grafana endpoints that fail to validate database access permissions. Attackers can access and modify databases they are not authorized to use by directly calling affected endpoints with arbitrary database parameters.	9.8	More Details
	The WooCommerce - Social Login plugin for WordPress is vulnerable to Authentication Bypass in all versions up to and including 2.8.7. This is due to the plugin's Apple login handler accepting the Apple id_token and decoding only its base64 payload without verifying the JWT		

CVE-2026-8457	signature against Apple's public keys or validating the issuer, audience, or expiry claims, combined with the security nonce required to invoke the login flow being publicly exposed to unauthenticated users via a localized JavaScript object on the login page. This makes it possible for unauthenticated attackers to log in as any existing WordPress user — including administrators — by supplying a forged id_token whose payload contains the target user's email address, as that email is used without any role exclusion to resolve a WordPress account and immediately issue an authenticated session for it.	9.8	More Details
CVE-2026-65321	PyAthena prior to 3.35.4 contains a sql injection vulnerability that allows unauthenticated attackers to inject arbitrary SQL by exploiting improper quote-escaping in DefaultParameterFormatter.format(), which routes DELETE and CTAS statements to the _escape_hive function that backslash-escapes single quotes rather than doubling them. Because Athena and Trino do not treat backslashes as escape characters inside string literals, attacker-supplied input such as a single quote followed by SQL syntax causes the parser to terminate the string literal prematurely, enabling data exfiltration via UNION SELECT, execution of destructive statements, and attacker-controlled CTAS destination and content.	9.8	More Details
CVE-2026-16060	The Insert or Embed Articulate Content into WordPress plugin through 4.3000000027 does not correctly validate the contents of an uploaded archive, relying on a bypassable check that lets an Editor-level user upload a server-executable file into a public directory, resulting in remote code execution on servers configured to execute it.	9.8	More Details
CVE-2026-16250	The Personal QR Message WordPress plugin through 1.0 does not restrict the file types that can be uploaded through an unauthenticated handler, allowing unauthenticated users to upload arbitrary executable PHP files that are directly reachable, leading to remote code execution.	9.8	More Details
CVE-2026-16300	The ChamaWP WordPress plugin before 1.0.13 does not properly validate a password reset request, allowing unauthenticated attackers to reset the password of arbitrary users, including administrators, which could lead to a full site takeover.	9.8	More Details
CVE-2026-12943	IBM HMC V10.3.1050.0 through 10.3.1064.0 and IBM HMC V11.1.1110.0 through 11.1.1112.0 Management systems in IBM Power environments (HMC and Novalink) could allow an unauthenticated user to execute arbitrary commands with elevated privileges on the system due to improper validation of user supplied input.	9.8	More Details
CVE-2026-18589	A vulnerability was found in Wavlink WL-NU516U1 708c073-mt7628. This impacts the function change_password of the file nas.cgi. The manipulation of the argument User1Passwd results in stack-based buffer overflow. The attack can be executed remotely. The exploit has been made public and could be used. The affected component should be upgraded. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	9.8	More Details
CVE-2026-2346	Authorization bypass through User-Controlled key vulnerability in Menulux Software Inc. Mobile App allows Software Integrity Attack. This issue affects Mobile App: through 12.05.2026.	9.8	More Details
CVE-2026-18601	A vulnerability was found in GL.iNet GL-MT3000 up to 4.4.5. This impacts the function ovpn-client.check_config of the file /cgi-bin/glc of the component ovpn-client.so Native Plugin. Performing a manipulation of the argument filename results in command injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	9.8	More Details
CVE-2026-69240	Sequelize is a Node.js ORM tool. Prior to 6.37.4, SQL injection is possible with strings only if dialect is set to oracle. The escape function defined in sql-string.js does not escape quotes if the value starts with TO_TIMESTAMP or TO_DATE. In the Oracle dialect, when val is a string and starts with TO_TIMESTAMP or TO_DATE, escape returns val directly instead of replacing single quotes. An attacker can inject arbitrary SQL expressions through an application value that reaches this escape path. This issue is fixed in version 6.37.4.	9.8	More Details
CVE-2026-64827	Telenia Software TVox 26.5.3 and prior 26.x versions, and 24.9.21 and prior 24.x versions, contain an authentication bypass vulnerability in set_env.php where the redirectToLoginAdminIRequestHaveAccessToken() function derives the current page name from PHP_SELF and skips authentication when the value matches 'login_admin.php'. Attackers can append '/login_admin.php' to the path of any target PHP script to cause the authentication check to pass and gain unauthenticated access to all PHP scripts under the manager HTML directory.	9.8	More Details

CVE-2026-18602	A vulnerability was determined in GL.iNet GL-MT3000 up to 4.4.5. Affected is the function ovpn-client.get_recommend_config of the file /cgi-bin/glc of the component ovpn-client.so Native Plugin. Executing a manipulation of the argument Hostname can lead to command injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	9.8	More Details
CVE-2026-41452	Krayin CRM 2.2.4 contains a missing authentication vulnerability in the installer middleware that allows unauthenticated remote attackers to overwrite the primary administrator account by sending a crafted HTTP POST request with the X-Requested-With: XMLHttpRequest header to bypass the CanInstall middleware redirect check. Attackers can supply arbitrary name, email, and password values to the admin-config-setup endpoint, which performs an unauthenticated updateOrInsert targeting the hardcoded administrator user ID, enabling full administrative access to all CRM data.	9.8	More Details
CVE-2026-18612	A flaw has been found in GL-iNet GL-MT3000 up to 4.4.5. This vulnerability affects the function plugins.remove_package/plugins.install_package of the file /cgi-bin/glc of the component plugins.so Native Plugin. This manipulation causes command injection. The attack can be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	9.8	More Details
CVE-2026-18613	A vulnerability has been found in GL-iNet GL-MT3000 up to 4.4.5. This issue affects the function plugins.set_config of the file /cgi-bin/glc of the component plugins.so Native Plugin. Such manipulation leads to injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	9.8	More Details
CVE-2026-18614	A vulnerability was found in GL-iNet GL-MT3000 up to 4.4.5. Impacted is the function s2s.enable_echo_server of the file /cgi-bin/glc of the component s2s.so Native Plugin. Performing a manipulation of the argument port results in command injection. The attack may be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	9.8	More Details
CVE-2026-18615	A vulnerability was determined in GL-iNet GL-MT3000 up to 4.4.5. The affected element is the function wg-server.generate_publickey of the file /cgi-bin/glc of the component wg-server.so Native Plugin. Executing a manipulation of the argument private_key can lead to command injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	9.8	More Details
CVE-2026-18616	A vulnerability was identified in GL-iNet GL-MT3000 up to 4.4.5. The impacted element is the function server.set_peer of the file /cgi-bin/glc of the component wg-server.so Native Plugin. The manipulation of the argument public_key leads to command injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	9.8	More Details
CVE-2026-38447	osTicket 1.18.3 generates API keys using a predictable construction based on MD5 hashing. The use of MD5, combined with predictable inputs such as the current timestamp and client IP address, significantly reduces entropy. An attacker can approximate the key generation time and brute-force the key space within a feasible time window.	9.8	More Details
CVE-2026-18588	A vulnerability has been found in Wavlink WL-NU516U1 708c073-mt7628. This affects the function fgets of the file nas.cgi. The manipulation of the argument CONTENT_LENGTH leads to stack-based buffer overflow. Remote exploitation of the attack is possible. You should upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	9.8	More Details
CVE-2026-67594	Spikster through commit e1cdf8c contains a missing authentication vulnerability that allows unauthenticated remote attackers to access all API routes by exploiting the unattached CipiAuth middleware, which is registered but never applied to any route in the API routing configuration. Attackers can invoke approximately 50 unprotected API endpoints to enumerate and provision servers, reset root passwords, read and write arbitrary files on the host, and create database users.	9.8	More Details
CVE-2026-	IBM webMethods Integration (on prem) 10.15, 10.11 could allow an unauthenticated remote	9.8	More

12118	attacker to execute arbitrary code on the system due to the deserialization of untrusted data.		Details
CVE-2026-44104	The firmware update process for the basemodule of the charging controller only validates the CRC32 checksum without cryptographic signature verification. This allows an unauthenticated remote attacker to install a modified firmware, resulting in full system compromise.	9.8	More Details
CVE-2025-69942	kishan0725 Hospital Management System 4.0 is vulnerable to SQL Injection in /hms/doctor/view-patient.php?viewid=1.	9.8	More Details
CVE-2025-67404	Sourcecodester CASAP Automated Enrollment System 1.0 is vulnerable to SQL Injection in save_stud.php via the parameters fname, lname, and student_class.	9.8	More Details
CVE-2026-12940	IBM Langflow OSS 1.0.0 through 1.10.1 are vulnerable to unauthenticated remote code execution via environment variable injection in the MCP (Model Context Protocol) stdio launcher. The vulnerability exists in src/lfx/src/lfx/base/mcp/util.py where the DANGEROUS_ENV_VARS blocklist fails to include SHELLOPTS , BASHOPTS , and PS4 environment variables.	9.8	More Details
CVE-2025-69943	kishan0725 Hospital Management System 4.0 is vulnerale to SQL Injection in get_doctor.php via the parameters doctor and specilizationid.	9.8	More Details
CVE-2025-67403	Sourcecodester CASAP Automated Enrollment System 1.0 is vulnerable to SQL Injection in update_class.php via the parameter class_name.	9.8	More Details
CVE-2025-65340	kishan0725 Hospital Management System 4.0 is vulnerable to SQL Injection in /betweendates-detailsreports.php.	9.8	More Details
CVE-2026-16610	The Admin and Site Enhancements (ASE) Pro plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 8.9.0 via the recursive_html function. This is due to the frontend save handler enforces only a publicly emitted nonce with no authentication check, CAPTCHA validation is bypassable by omitting an attacker-supplied key, and repeater row keys from cfgroup[input] are stored verbatim and later spliced into an eval() call in recursive_html without any sanitization or identifier validation. This makes it possible for unauthenticated attackers to execute code on the server. This requires the [post_cf_form] shortcode to be present on at least one publicly accessible page, as the nonce and session ID needed to reach the vulnerable save handler are emitted to unauthenticated visitors by that shortcode.	9.8	More Details
CVE-2026-44090	Due to missing authentication, an unauthenticated remote attacker may access the MQTT broker, which is only protected from external access by a firewall. This may lead to the device being fully compromised.	9.8	More Details
CVE-2026-67191	Xlight FTP Server before 3.9.5 contains a pre-authentication heap buffer overflow vulnerability that allows remote unauthenticated attackers to write past the end of a heap buffer by sending a malformed SSH client identification string. A logic error in the recv loop's termination condition uses an incorrect OR operator where an AND operator is required, enabling exploitation on any SSH or SFTP connection before authentication occurs.	9.8	More Details
CVE-2026-60113	AMMOS Instrument Toolkit (AIT) Deep Space Network (DSN) Interface before 2.2.2 contains a missing authentication vulnerability in the Space Link Extension (SLE) interface manager that allows unauthenticated network attackers to access seven unprotected API routes by sending direct HTTP requests with no credentials. Attackers can reach the exposed SLE endpoints to start or stop Deep Space Network communication sessions, retrieve telemetry frame data, and inject arbitrary frames into active spacecraft links.	9.8	More Details
CVE-2026-60112	AMMOS Instrument Toolkit (AIT) GUI before 2.5.1 contains a missing authentication vulnerability that allows any unauthenticated network attacker to obtain a valid session and issue arbitrary spacecraft commands by calling Sessions.create() without any credential check. Attackers can exploit the unauthenticated session issuance in Sessions.create() and subsequently invoke handle_cmd() to forward arbitrary commands directly to the AIT command bus without any authentication gate between session creation and command dispatch.	9.8	More Details
CVE-2026-44101	Due to missing authentication the CHARX OCPP Agent service allows an unauthenticated remote attacker to reconfigure the backend connection. This can lead to Denial-of-Service and confidential data being disclosed to the attacker.	9.8	More Details
	Care Everywhere Gateway 14.3.10 contains a hard-coded credentials vulnerability in the		

CVE-2026-41939	bundled WildFly 8.2.0.Final management interface that allows unauthenticated remote attackers to gain administrative access by using default credentials identical across all installations. Attackers can authenticate to the exposed WildFly management console on port 20990 and deploy a malicious Web Application Archive file through the Deployments interface to achieve remote code execution as the Windows machine account. Version 14.x.x was declared end-of-life (EOL) in 2017 and future releases have addressed the vulnerable finding.	9.8	More Details
CVE-2026-44108	Due to a flaw in the execution order of scripts during shutdown, the firewall is terminated prematurely during system shutdown. This creates a temporary window in which internal services may become externally accessible, potentially allowing an unauthenticated remote attacker to connect to these services, resulting in full system compromise.	9.8	More Details
CVE-2025-10656	The Spreadsheet Price Changer for WooCommerce and WP E-commerce – Light plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 2.4.37 vi the user_filter function. This makes it possible for unauthenticated attackers to create admin accounts.	9.8	More Details
CVE-2026-52680	Apache Kyuubi REST batch multipart upload handling uses the client-supplied multipart filename when creating a temporary uploaded resource. A remote attacker who can access the REST batch upload endpoint can provide path traversal sequences in the filename and cause the Kyuubi server process to write controlled content outside the intended upload directory, subject to filesystem permissions. This issue affects Apache Kyuubi: from 1.7.0 through 1.11.1. Users are recommended to upgrade to version 1.12.0, which fixes the issue.	9.8	More Details
CVE-2026-4978	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in UMAI Vision Traffic Analysis System allows SQL Injection. This issue affects Traffic Analysis System: from 30 before 34.	9.8	More Details
CVE-2026-18191	VIN-DS783E-E6 developed by Vacron has a Hidden Functionality vulnerability, allowing unauthenticated remote attackers to exploit a specific hidden function to obtain the administrator credentials of the device.	9.8	More Details
CVE-2026-28812	UserManager lack of checks allows impersonation in Apache JSPWiki up to 2.12.3 which may allow attackers to escalate privileges. Users are recommended to upgrade to version 2.12.4 or newer which fixes this issue.	9.8	More Details
CVE-2026-7849	Due to improper neutralization of special elements, an unauthenticated remote attacker is able to inject a command into the system configuration which is subsequently executed as root.	9.8	More Details
CVE-2026-15435	IBM App Connect Enterprise 13.0.1.0 through 13.0.7.2, and 12.0.1.0 through 12.0.12.27 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to write arbitrary files on the system.	9.8	More Details
CVE-2026-28323	SolarWinds Web Help Desk is found to be affected by a SAML authentication bypass vulnerability. This requires the SAML 2.0 authentication method to be enabled.	9.8	More Details
CVE-2026-59243	The FAB auth manager's Azure AD OAuth login defaulted `verify_signature=False` when decoding the ID token, so an attacker able to present a forged or unsigned (`alg:none`) ID token to the OAuth callback could bypass authentication and log in as an arbitrary user, including one holding the Admin role (CWE-347). Deployments running the FAB auth manager with the Azure AD OAuth login path under its default configuration are affected; the Authentik path already defaulted to `True`. This issue affects `apache-airflow-providers-fab` before 3.7.3. Users are advised to upgrade to `apache-airflow-providers-fab` 3.7.3, which defaults `verify_signature=True`.	9.8	More Details
CVE-2026-59310	VMware vCenter contains a directory traversal vulnerability in the Syslog server. A malicious actor with network access to vCenter may exploit this issue to execute arbitrary code.	9.8	More Details
CVE-2026-14900	The Cost Calculator Builder PRO plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.0.3 via the js_to_php function. This is due to insufficient sanitization of the orderDetails[*].originalValue field, which is injected verbatim into a calculator formula string passed to PHP eval() inside js_to_php(), with the regex allow-list in evaluateFormula() only filtering alphanumeric tokens and leaving non-word punctuation characters intact. This makes it possible for unauthenticated attackers to execute code on the server. The only authentication barrier is a nonce check, but the required nonce is publicly emitted on every front-end page via the wp_head hook, making it freely obtainable by	9.8	More Details

	unauthenticated visitors. Payloads must be non-word XOR gadgets to bypass sanitization.		
CVE-2026-59309	VMware vCenter contains an authentication bypass vulnerability in the VMware Directory Service. A malicious actor with network access to vCenter may exploit this issue to bypass authentication and gain unauthorized access to the system.	9.8	More Details
CVE-2026-68579	FreeRDP before 3.30.0 (<= 3.29.0) contains a heap-based buffer overflow in the Windows clipboard client's CliprdrStream_Read function (client/Windows/wf_cliprdr.c). When an OLE paste consumer (e.g. explorer.exe) calls IStream::Read with a fixed-size buffer of cb bytes, CliprdrStream_Read requests file contents from the RDP server and then copies the response into the caller's buffer using the server-supplied length (req_fsize) instead of cb. A malicious or compromised RDP server can return an oversized CB_FILECONTENTS_RESPONSE, causing an out-of-bounds write of attacker-controlled data into the paste consumer's heap buffer when a user pastes server-offered clipboard file contents.	9.6	More Details
CVE-2026-17704	Use after free in ANGLE in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-48317	Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') vulnerability that could result in arbitrary code execution in the context of the current user. A low-privileged attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	9.6	More Details
CVE-2026-17656	Use after free in Ozone in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-17708	Use after free in Audio in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17710	Inappropriate implementation in MHTML in Google Chrome on Mac prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17709	Race in Downloads in Google Chrome on Mac prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17711	Race in Downloads in Google Chrome on Mac prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17697	Type Confusion in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-17655	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-17713	Insufficient validation of untrusted input in Accessibility in Google Chrome on Android prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17652	Use after free in Views in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17701	Insufficient validation of untrusted input in ANGLE in Google Chrome on Mac prior to 151.0.7922.72 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)	9.6	More Details
	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 151.0.7922.72		

CVE-2026-17671	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)	9.6	More Details
CVE-2026-17695	Inappropriate implementation in ANGLE in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-17692	Use after free in DataTransfer in Google Chrome on Windows prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17691	Out of bounds write in ANGLE in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-17688	Use after free in Input in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17687	Type Confusion in ANGLE in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17684	Insufficient validation of untrusted input in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17669	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-18667	A vulnerability in Tenable Sensor Proxy allows a remote attacker to execute code with elevated privileges by inducing an operator to connect the sensor to an attacker-controlled host.	9.6	More Details
CVE-2026-17670	Use after free in Views in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17682	Integer overflow in ANGLE in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17718	Use after free in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-17681	Insufficient validation of untrusted input in Web Authentication in Google Chrome on Android prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17680	Heap buffer overflow in Color in Google Chrome on ChromeOS prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17676	Inappropriate implementation in ANGLE in Google Chrome on Android prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17675	Out of bounds write in ANGLE in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17717	Integer overflow in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details

CVE-2026-17834	Insufficient validation of untrusted input in Passwords in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17721	Out of bounds write in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-17726	Integer overflow in WebGL in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-25289	Memory Corruption when processing Device Capability Extended attributes in certain NAN Service Discovery Frames with invalid length values.	9.6	More Details
CVE-2026-18015	Inappropriate implementation in Tint in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	9.6	More Details
CVE-2026-18002	Insufficient validation of untrusted input in Google Lens in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	9.6	More Details
CVE-2026-17991	Insufficient validation of untrusted input in AI in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	9.6	More Details
CVE-2026-17990	Insufficient validation of untrusted input in WebAuthn in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted PDF file. (Chromium security severity: Low)	9.6	More Details
CVE-2026-17987	Insufficient validation of untrusted input in Notifications in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted PDF file. (Chromium security severity: Low)	9.6	More Details
CVE-2026-17947	Use after free in WebSockets in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	9.6	More Details
CVE-2026-17940	Insufficient validation of untrusted input in Picture-in-Picture in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	9.6	More Details
CVE-2026-17924	Use after free in DNS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	9.6	More Details
CVE-2026-17349	/misc/workspace/adhoc_connect_server, part of the Workspaces feature introduced in pgAdmin 4 9.0, when passed the id of an existing server, clones that server via Server.clone(), which copies every column from the source row, including user_id, shared, shared_username, and the stored credential fields password, save_password, and tunnel_password. When a non-owner triggered an adhoc connect against another user's (in practice, typically an administrator's) shared server, the clone inherited that user's ownership, shared flag, and stored database credentials verbatim. pgAdmin persisted this cross-tenant, credential-bearing server row before the connection was even attempted, so it survived even when the connection subsequently failed. The non-owner could then open the newly-owned clone and pgAdmin would connect using the source user's stored database password on the non-owner's behalf, granting the non-owner use of database credentials -- and whatever database privileges they confer -- that were never their own. Fix forces the cloned adhoc record's ownership fields (user_id, shared, shared_username) and stored credential fields (password, save_password, tunnel_password) to belong to the calling user and be cleared/private before committing, regardless of the source server's ownership, sharing state, or stored credentials. A regression test asserts that an adhoc connect triggered by a non-owner against another user's shared server persists a row owned by the caller, not shared, and without the source's stored credentials. This issue affects	9.6	More Details

	pgAdmin 4: from 9.0 before 9.17.		
CVE-2026-17865	Inappropriate implementation in Crypto in Google Chrome on Mac prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17856	Inappropriate implementation in Network in Google Chrome on Mac prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17855	Race in DevTools in Google Chrome on Mac prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-54725	vault-secrets-webhook is a Kubernetes mutating webhook that makes direct secret injection into Pods possible. Prior to 1.23.1, parseVaultConfig() in pkg/webhook/config.go accepts the vault.security.banzaicloud.io/vault-addr annotation, MutateConfigMap and MutateSecret call newVaultClient in pkg/webhook/webhook.go, and vault.security.banzaicloud.io/vault-serviceaccount can cause a ServiceAccount JWT to be sent to an attacker-controlled Vault address. This issue is fixed in version 1.23.1.	9.6	More Details
CVE-2026-17848	Integer overflow in Codecs in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-17847	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-17837	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17672	Insufficient validation of untrusted input in Chromecast in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17832	Use after free in ANGLE in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17804	Use after free in Media in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17803	Insufficient validation of untrusted input in Save to Drive in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted PDF file. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-17801	Out of bounds read and write in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-17768	Insufficient validation of untrusted input in WebSockets in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17651	Insufficient validation of untrusted input in Dawn in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-17758	Heap buffer overflow in Dawn in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details

CVE-2026-17749	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-17738	Insufficient validation of untrusted input in Payments in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-17727	Out of bounds write in WebGL in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-17673	Integer overflow in QUIC in Google Chrome prior to 151.0.7922.72 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)	9.6	More Details
CVE-2026-14529	IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 traditional is vulnerable to server-side request forgery (SSRF) when the SIP container feature (sipServlet-1.1) is enabled.	9.4	More Details
CVE-2026-15930	The Simple Membership WordPress plugin before 4.7.8 does not verify whether user creation failed during registration before using the returned value as a user ID to update an account, allowing unauthenticated attackers to overwrite the primary administrator's account data (including the email address) and take over that account through the password reset flow.	9.4	More Details
CVE-2026-63221	CodeIgniter is a PHP full-stack web framework. From 4.3.0 through 4.7.3, Query Builder deleteBatch() substitutes bound values from where() conditions into generated SQL while ignoring their escape flags, allowing user-controlled condition values to be interpreted as SQL. This affects only the deleteBatch() code path. Regular delete() operations escape where() binds correctly. This issue is fixed in version 4.7.4.	9.4	More Details
CVE-2026-44100	The CHARX JupiCore service allows an unauthenticated remote attacker to reconfigure charging points. This can lead to disclosure of charging point UIDs, Denial-of-Service and files tampering.	9.4	More Details
CVE-2026-67426	Flyto2 Core is an execution kernel for automation and AI-agent workflows. Prior to 2.26.7, the standalone flyto-verification service in src/core/verification_service.py exposes unauthenticated POST /run on 0.0.0.0:8344 and uses client-supplied callback_url for an outbound POST with X-Internal-Key: $FLYTO_RUNNER_SECRET while bypassing target_allowed, allowing unauthenticated SSRF and runner secret exfiltration. This issue is fixed in version 2.26.7.	9.3	More Details
CVE-2026-11707	IBM Tivoli System Automation Application Manager 4.1 and IBM WebSphere Application Server is affected by a cross-site scripting vulnerability in the administrative console login page.	9.3	More Details
CVE-2026-15958	The Easy Integration for Dropbox WordPress plugin before 2.2.0 does not perform authorization checks on several of its file-management AJAX actions that it also registers for unauthenticated users, allowing an unauthenticated attacker to list, download and upload arbitrary files across the connected Dropbox account and to read the connected account and administrator email addresses.	9.3	More Details
CVE-2026-66418	OpenClaw Dashboard v3.0.0 contains a stored cross-site scripting vulnerability that allows unauthenticated remote attackers to inject arbitrary HTML and script payloads by submitting a crafted username in a failed login POST request, which is recorded verbatim in the audit log. When an administrator opens the notification panel, the unescaped log entry is rendered via innerHTML with a permissive Content-Security-Policy allowing inline event handlers, enabling the attacker-supplied payload to execute in the administrator's session and interact with authenticated endpoints including agent instruction file editing and configuration changes.	9.3	More Details
CVE-2026-47876	VMware ESX contains an out-of-bounds write vulnerability in the VMXNET3 virtual network adapter. A malicious actor with local administrative privileges on a virtual machine with VMXNET3 virtual network adapter may exploit this issue to execute code on the host. Non VMXNET3 virtual adapters are not affected by this issue.	9.3	More Details
CVE-2026-58155	Apache Traffic Server truncates over-long header names, allowing header aliasing, request smuggling, and policy bypass. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	9.3	More Details

CVE-2026-41920	Improper Access Control vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 9.0.0 through 9.1.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.1.15 or 10.1.4, which fixes the issue.	9.3	More Details
CVE-2026-66421	OpenClaw Dashboard contains a stored cross-site scripting vulnerability that allows unauthenticated remote attackers to execute arbitrary JavaScript in the administrator's browser session by injecting HTML markup into agent transcript messages processed through the sessions API. Attackers can craft a message containing inline event handler payloads such as an img tag with an onerror attribute within the 60-character rendering budget, which is stored in the session transcript and interpolated unsanitized into innerHTML on the default landing page, allowing theft of session tokens and unauthorized calls to authenticated administrative endpoints including agent instruction file modification.	9.3	More Details
CVE-2026-54363	CentreStack before 17.5 contains a hardcoded cryptographic key vulnerability that allows unauthenticated attackers to forge arbitrary encrypted tokens by exploiting a static SysNumber value used as entropy for AccessTicket.Encrypt() and AccessTicket.Decrypt() across all installations. Attackers can use the hardcoded key to craft valid x-glad-auth headers and call privileged API endpoints such as acquiretenantbackuptoken to obtain a domain administrator IdentityTicket, enabling a complete unauthenticated remote code execution chain.	9.1	More Details
CVE-2026-14488	The Meta Box AIO plugin for WordPress is vulnerable to Missing Authorization via the template_redirect dispatcher in the MB Frontend Submission extension in versions up to, and including, 3.8.0. This is due to the handle_request() function routing the mbfs_delete action without any capability or ownership check, and the nonce verification in check_ajax() being gated behind is_ajax() which is false for template_redirect requests, making it bypassable. This makes it possible for unauthenticated attackers to delete arbitrary posts and pages by supplying an attacker-controlled post ID via the rwmb_frontend_field_object_id GET parameter on any page that hosts a frontend submission form regardless of whether allow_delete is enabled.	9.1	More Details
CVE-2026-63230	A pre-authentication error-based SQL injection vulnerability in Koollab LMS allowed an unauthenticated attacker to read sensitive database contents, including personally identifiable information, credentials, and valid JWT tokens that may enable account takeover, via the SCORM report endpoint.	9.1	More Details
CVE-2026-44092	An unauthenticated remote attacker can inject malicious input into the ModbusServer application because it does not validate the input it fetches from MQTT. This may lead to integrity and availability loss.	9.1	More Details
CVE-2026-63229	A pre-authentication blind SQL injection vulnerability in Koollab LMS allowed an unauthenticated attacker to use a time-based SQL oracle via the SSO OAuth endpoint to read sensitive database contents, including personally identifiable information, credentials, and valid JWT tokens that may enable account takeover.	9.1	More Details
CVE-2026-44091	An unauthenticated remote attacker can post a malicious ID to the MQTT Broker results in the creation of a new configuration entry in the system configuration. This may lead to integrity and availability loss.	9.1	More Details
CVE-2026-51992	SQL Injection vulnerability in ClickHouse Server Versions <= 26.3.9.8 allows a remote attacker to execute arbitrary code via the create dictionaries function.	9.1	More Details
CVE-2026-69110	OpenCode Studio before 2.4.4 contains a missing authentication vulnerability that allows unauthenticated remote attackers to read arbitrary files within the temp and static/music directories by directly accessing the GET /api/tmp/:tmpFile and GET /api/music/:fileName endpoints. Attackers can retrieve intermediate audio, video artifacts, and subtitles belonging to other users' jobs, and additionally delete any video by ID through the unauthenticated DELETE /api/short-video/:videoId endpoint.	9.1	More Details
CVE-2026-45100	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Versions 3.4.0-beta through 3.6.5 and 4.0.0-beta contain a buffer overflow in the {s.b64encode} string transformation. The size check for {s.b64encode} only verifies that the input fits within the 64 KB transformation buffer, but base64 encoding expands the data by roughly a third, so an input between about 49,153 and 65,535 bytes produces more output than the buffer can hold and overflows it by up to 21,844 bytes. Because these transformation buffers sit next to each other in memory and are reused for chained transformations, the overflow writes attacker-controlled data into the adjacent buffer and corrupts values used by later transformations processing the same SIP message. A remote attacker can trigger this by sending a SIP message with a large	9.1	More Details

	header value (roughly 50,000 bytes or more) when the routing script applies {s.b64encode} to attacker-controlled input, making exploitability dependent on the deployment's routing configuration. This issue has been fixed in versions 3.6.6 and 4.0.0-rc1.		
CVE-2026-52539	Outstatic CMS <= 2.1.9 contains a hardcoded JWT signing secret. When the OST_TOKEN_SECRET environment variable is not set, the application falls back to the default value which is publicly visible in the source code repository. An unauthenticated remote attacker can exploit this by forging JWT session tokens with arbitrary user data and full administrative permissions.	9.1	More Details
CVE-2026-39932	OpenEMR through 8.2.0 contains a remote code execution vulnerability in the document category tree component (library/classes/Tree.class.php) that allows authenticated administrators to execute arbitrary operating system commands by injecting PHP payloads into the categories database table. Attackers can chain arbitrary SQL execution to alter the id column type to VARCHAR and insert a malicious PHP payload, which is then executed via an unsanitized eval() call whenever any page instantiates CategoryTree, including unauthenticated and low-privilege pages, resulting in command execution as the web server user.	9.1	More Details
CVE-2026-12965	The Super Store Finder WordPress plugin through 7.8 does not sanitize a parameter of an unauthenticated AJAX action before using it in a SQL query, allowing unauthenticated attackers to perform SQL injection and extract data from the database.	9.1	More Details
CVE-2026-48031	go-base is a Go RESTful API Boilerplate template with JWT Authentication, backed by PostgreSQL. In versions prior to 2026-05-18, the JWT signing secret is hardcoded to the known string "random", letting any attacker who reads the public repository forge tokens for arbitrary users, including admin roles, and completely bypass authentication on all protected endpoints. This value is set in two places: the dev.env template (line 10) and a programmatic fallback in cmd/serve.go (line 35), so the application uses it even when no .env file is present. The original mitigation in auth/jwt/tokenauth.go (lines 22 to 25) only caught the exact string "random", letting other weak secrets through, and replaced it with an in-memory key that was not persisted, invalidating all tokens on every restart and effectively causing a denial-of-service. This issue has been fixed in version 2026-05-18.	9.1	More Details
CVE-2026-18248	@fastify/aws-lambda version 6.4.0 decorates each Fastify request with request.awsLambda.event and request.awsLambda.context, values that applications are documented to use for authorization decisions such as reading API Gateway authorizer claims. In the default configuration, the getter that populates this decoration reads the client-controlled x-apigateway-event and x-apigateway-context HTTP headers before falling back to the trusted internal request token, and those reserved headers are not stripped from the incoming event. An unauthenticated attacker who can set a single HTTP header can therefore forge the entire Lambda proxy event, including the authorizer context, and override the genuine one. This results in a full authentication and authorization bypass and privilege escalation for any application that trusts request.awsLambda.event for identity or access control. Only version 6.4.0 is affected. Patches: upgrade to @fastify/aws-lambda 6.4.1, which resolves the decoration only through the internal per-invocation token and strips the reserved headers before the request is processed.	9.1	More Details
CVE-2026-9487	XML::Sig versions before 0.71 for Perl allow signature wrapping via duplicate ID. _get_signed_xml() in lib/XML/Sig.pm, called from verify(), resolves the SignedInfo Reference/@URI to a node with the XPath expression "//*[@ID='$id']" and returns the first node of the resulting node set. A document in which two elements share that ID value is accepted: the digest and signature are checked against whichever element comes first in document order, and the duplicate is not detected. Such a document verifies successfully while an application that resolves the same ID independently can read the second, attacker supplied element; in a SAML2 context this places the contents of an Assertion under attacker control.	9.1	More Details
CVE-2026-9390	XML::Sig versions before 0.71 for Perl allow XPath injection in ID lookup. verify() and _get_signed_xml() in lib/XML/Sig.pm build XPath expressions by concatenating the SignedInfo/Reference/@URI value read from the document being verified. The value is neither escaped nor checked against the NCName grammar that XML requires of an ID, so a URI containing a single quote closes the string literal in the generated expression and appends arbitrary XPath operators. A crafted URI can make the lookup match elements the reference does not name, or every element in the document, so which node is selected for digest verification is decided by the injected expression rather than by the reference.	9.1	More Details

CVE-2026-16534	The Import and export users and customers WordPress plugin before 2.4.2 does not enforce WordPress's role-assignment and per-user edit permissions during CSV import, allowing a user holding only the user-creation capability to create an administrator account and to overwrite an existing administrator's password or email.	9.1	More Details
CVE-2026-17666	Cryptographic Flaw in Enterprise in Google Chrome prior to 151.0.7922.72 allowed an attacker in a privileged network position to bypass discretionary access control via malicious network traffic. (Chromium security severity: High)	9.1	More Details
CVE-2026-16532	The Link Library WordPress plugin before 7.9.3 does not properly sanitise and escape a user-supplied value before using it in a SQL query, allowing unauthenticated users to perform SQL injection attacks.	9.1	More Details
CVE-2026-14557	The SoftMarket — Digital Marketplace WordPress plugin through 1.0.0 does not properly validate an authentication token in one branch of its email-verification flow, allowing unauthenticated attackers to obtain a valid session as any verified user by supplying only that user's ID.	9.1	More Details
CVE-2026-45537	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. In versions prior to 3.6.6 and 4.0.0-rc1, the construct_uri() function concatenates multiple URI components (protocol, username, domain, port, params) into a fixed 1024-byte global BSS buffer without any bounds checking. When a routing script calls construct_uri() with an attacker-controlled username, a combined component length exceeding 1024 bytes overflows the buffer, corrupting adjacent global data with attacker-controlled content. The overflow reaches disable_503_translation, a global flag controlling SIP 503 response handling, allowing an attacker to deterministically set the flag via the URI username and alter the server's routing behavior for subsequent messages. Because the same buffer is shared with contact_builder(), the overflow also corrupts that function's data, and without a memory sanitizer the adjacent globals are silently overwritten on every request containing a long username. This issue has been fixed in versions 3.6.6 and 4.0.0-rc1.	9.1	More Details
CVE-2026-13596	The Participants Database WordPress plugin before 2.7.8.4 does not properly sanitize and escape a user-supplied parameter before using it in a SQL query, allowing unauthenticated attackers to perform SQL injection attacks.	9.1	More Details
CVE-2026-3141	The FormGent plugin for WordPress is vulnerable to unauthorized arbitrary file deletion due to a missing capability check on the /wp-json/formgent/responses/attachments REST API endpoint in all versions up to, and including, 1.9.2 This is due to the REST API route being registered without any authentication middleware in routes/rest/api.php. This makes it possible for unauthenticated attackers to delete arbitrary files within the formgent uploads directory. Additionally, on Linux servers where the wp-content/uploads/formgent directory does not yet exist (the default state after plugin installation), the path traversal protection can be bypassed, enabling deletion of arbitrary files including wp-config.php which can lead to complete site takeover via a fresh WordPress installation.	9.1	More Details
CVE-2026-16503	Deployment of the VPS.org one-click Supabase template deploys a PostgreSQL instance that is published on all interfaces (0.0.0.0:5432) with a default database password set to "postgres". Because Docker installs its own iptables rules, this exposure bypasses a standard host UFW configuration.	9.1	More Details
CVE-2026-18753	The product firmware contains an embedded, static RSA private key utilized by the Lighttpd web server for TLS termination. Exposure of this private key allows malicious actors to breach the confidentiality and integrity of HTTPS communications, enabling traffic decryption and server spoofing.	9.1	More Details
CVE-2026-18754	The product firmware contains an embedded, static RSA private key utilized by the Lighttpd web server for TLS termination. Exposure of this private key allows malicious actors to breach the confidentiality and integrity of HTTPS communications, enabling traffic decryption and server spoofing.	9.1	More Details
CVE-2026-14804	Use of hard-coded cryptographic key vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Read Sensitive Constants Within an Executable. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	9.1	More Details
	The fix for CVE-2026-12045 in pgAdmin 4 9.16 required the LLM-supplied query passed to the AI Assistant's execute_sql_query tool to parse, via sqlparse, as exactly one non-transaction-		

CVE-2026-17351	control statement before running it inside a BEGIN TRANSACTION READ ONLY wrapper. sqlparse's string-literal lexing can disagree with PostgreSQL's own parser: under standard_conforming_strings = on (PostgreSQL's default since 9.1), a backslash immediately before a quote is an ordinary character to PostgreSQL, but sqlparse treats it as escaping the quote. A payload such as SELECT '\';COMMIT;CREATE TABLE pwn(x int);SELECT 1 --' therefore parses as a single SELECT to sqlparse's validator, while PostgreSQL executes it as four statements: the smuggled COMMIT ends the wrapping read-only transaction, and the trailing ROLLBACK becomes a no-op. This reintroduces the same write/RCE bypass CVE-2026-12045 was meant to close, reachable via the same indirect prompt-injection delivery (an attacker plants the payload in any object the AI Assistant may read; the LLM emits it as a tool call). An initial candidate fix ran the query with psycopg's execute(..., prepare=True), intending to force PostgreSQL's own Parse step (extended query protocol) to reject multi-statement text regardless of sqlparse's classification. This candidate fix does not work as submitted: psycopg3's PrepareManager silently ignores the prepare argument whenever the connection's prepare_threshold is None, which is pgAdmin's default for every server connection (the per-server "Prepare threshold" field is blank unless an administrator explicitly sets it) -- psycopg3 falls back to the simple query protocol, the same multi-statement-capable path the bypass exploits, so the candidate fix closes nothing on any real-world default configuration. The corrected fix sets conn.prepare_threshold = 0 directly on the dedicated, single-use read-only connection the AI Assistant tool opens, structurally forcing the extended query protocol independent of any server-level configuration. Verified against a live PostgreSQL 18 instance: the payload executes successfully under the prepare_threshold=None (default) behavior, and is rejected with "cannot insert multiple commands into a prepared statement" once prepare_threshold=0 is set on that connection. This issue affects pgAdmin 4: from 9.13 before 9.17.	9.0	More Details
CVE-2026-18245	Improper control of code generation in Amazon @aws-amplify/codegen-ui-react before 2.20.6 might allow a remote authenticated user to execute arbitrary code in end-user browsers, developer machines, CI/CD environments, and server-side rendering contexts via crafted Studio component or theme schema values due to insufficient coverage and effectiveness of the input validation introduced for CVE-2025-4318. To remediate this issue, users should upgrade to version 2.20.6	9.0	More Details
CVE-2026-14602	The Remote API WordPress plugin through 0.2 does not authenticate a request before deserializing user-supplied input, allowing unauthenticated attackers to inject arbitrary PHP objects, which can lead to remote code execution when a suitable gadget chain is present through another installed Remote API WordPress plugin through 0.2.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-58154	Apache Traffic Server can write out of bounds or overflow integers while parsing MIME and HTTP headers. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	8.9	More Details
CVE-2026-65423	An integer overflow in the UA_Variant arrayDimensions product computation in open62541 may allow a remote attacker to trigger an out-of-bounds write.	8.8	More Details
CVE-2026-17920	Use after free in V8 in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code inside a sandbox via a crafted Chrome Extension. (Chromium security severity: Low)	8.8	More Details
CVE-2026-67206	Wolf CMS through 0.8.3.1 contains a remote code execution vulnerability in FileManagerController that allows authenticated attackers to create arbitrary PHP files by exploiting missing file extension validation in the create_file() and save() functions. Attackers with the file_manager_mkfile capability can write malicious PHP content into the web-accessible FILES_DIR directory and trigger execution by requesting the file over HTTP.	8.8	More Details
CVE-2026-	Wolf CMS through 0.8.3.1 contains an authorization bypass vulnerability in BackupRestoreController that allows authenticated non-administrative users to access restricted backup functionality due to a PHP operator precedence flaw in the permission check expression.	8.8	More

67207	Attackers can exploit the incorrect evaluation of the access control expression to create, download, and restore backups without administrative privileges.		Details
CVE-2026-12562	The RCU II+ and Multiload II+ are vulnerable to an unauthenticated service that exposes a debug interface granting full root-level access to the embedded system. This vulnerability stems from a network-accessible port running a Target Communications Framework (TCF) service that does not require any authentication, allowing an attacker to directly interact with the Linux environment that powers the device. Once connected, an attacker can freely view and modify the filesystem, manipulate running processes, and control network interfaces, enabling deep alteration of system behavior.	8.8	More Details
CVE-2026-17935	Heap buffer overflow in Codecs in Google Chrome prior to 151.0.7922.72 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-2026-62870	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2026-17922	Inappropriate implementation in Enterprise in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-18733	A prompt injection vulnerability in the shell tool in Amazon Strands Agents Tools before 0.8.0 might allow remote actors to execute arbitrary operating system commands on the agent's host via a crafted prompt that sets the non_interactive parameter to true, bypassing the human consent gate. To remediate this issue, users should upgrade to version 0.8.0.	8.8	More Details
CVE-2026-69096	OpenWrt luci-app-dockerman (LuCI master and openwrt-25.12 snapshots containing the ucode docker_rpc.uc RPC backend after the JS/ucode conversion) contains an OS command injection vulnerability. The package's read ACL grants broad ubus access to docker.* / docker.container.*, which exposes the docker.container.ttyd_start method even though it performs mutating operations. The run_ttyd handler builds a shell command from the request-controlled id, cmd, and uid fields and passes it to system() without quoting or argv-style execution in the rpcd root context. An authenticated attacker holding only the luci-app-dockerman read ACL can inject shell metacharacters (e.g., in id) to execute arbitrary commands as root via an HTTP POST to /ubus. openwrt-24.10 and openwrt-23.05 do not contain this backend and are not affected; no patched version was known as of the advisory.	8.8	More Details
CVE-2026-17918	Use after free in Sync in Google Chrome prior to 151.0.7922.72 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-2026-66420	MeshCentral 1.1.21 contains a cross-site WebSocket hijacking protection bypass vulnerability that allows unauthenticated remote attackers to hijack authenticated administrator sessions by exploiting an unconditional early return in the CheckWebServerOriginName() function within webserver.js when self-signed certificates are in use. Attackers can open cross-origin WebSocket connections to any of the twelve WebSocket endpoints, send crafted action commands to exfiltrate the server sessionKey used to sign session cookies, forge session tokens as arbitrary users, and gain full remote control of all managed devices governed by the MeshCentral instance.	8.8	More Details
CVE-2026-17899	Insufficient policy enforcement in DevTools in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to perform privilege escalation via a crafted Chrome Extension. (Chromium security severity: Low)	8.8	More Details
CVE-2026-18022	Integer wraparound in IVFFlat index build in pgvector before 0.8.6 allows a database user to write data out-of-bounds, which could lead to arbitrary code execution. Only 32-bit systems are affected.	8.8	More Details
CVE-2026-41453	Krayin CRM before 2.2.4 contains a blind SQL injection vulnerability in the leads DataGrid that allows authenticated users with leads access to inject arbitrary SQL into a HAVING clause by manipulating the rotten_lead[in] query parameter, which is concatenated without parameterized binding directly into a havingRaw() call in LeadDataGrid.php. Attackers can exploit this flaw using time-based and boolean-based blind injection techniques to extract the entire database contents, including user credential hashes, CRM records, and application configuration data.	8.8	More Details

CVE-2026-18607	A security vulnerability has been detected in Wavlink WN572, WN570H, WN573, WN529, WN530, WN531, WN535, etc. WN529, WN530, WN531, WN535, WN536, WN551, WN557 and NU516 up to 20260609. Affected by this issue is the function strcpy of the file upload.cgi of the component lighttpd. The manipulation of the argument HTTP_COOKIE leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-66416	Leantime 3.6.2 contains a cross-site request forgery vulnerability that allows unauthenticated attackers to perform state-changing actions on behalf of authenticated users by excluding the Laravel VerifyCsrfToken middleware from the global middleware stack in app/Http/Kernel.php. Attackers can craft malicious pages delivered via phishing emails or malicious websites to trigger unauthorized POST, PUT, and DELETE requests that create or delete projects, modify settings, and change permissions as any authenticated user.	8.8	More Details
CVE-2026-17950	Inappropriate implementation in Safebrowsing in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code via a malicious file. (Chromium security severity: Low)	8.8	More Details
CVE-2026-17951	Heap buffer overflow in WebRTC in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-67195	Perspective 5.0.0 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary operating system commands by submitting crafted expression strings to the PolarsVirtualServer backend, which passes client-supplied input directly to Python's eval() with only __builtins__={} cleared. Attackers can exploit Python object attribute traversal through the interpreter's loaded class list to reach subprocess.Popen via a TableValidateExprReq or TableMakeViewReq protobuf message, achieving arbitrary command execution in the Perspective host process.	8.8	More Details
CVE-2026-18787	A vulnerability was identified in GL.iNet AX1800 up to 4.8.3. The affected element is the function remove_rule of the file /usr/share/gl-ngx/oui-rpc.lua of the component RPC Endpoint. The manipulation of the argument args.id leads to command injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure.	8.8	More Details
CVE-2026-15307	An issue was discovered in Django 5.2 before 5.2.17 and 6.0 before 6.0.8. GeoDjango spatial lookups optimistically parse the right-hand-side value as a raster by passing it to the `django.contrib.gis.gdal.GDALRaster` constructor. Any value used in a spatial lookup against a `GeometryField` or `RasterField` reaches this constructor, including untrusted input, for example a spatial-field filter submitted through the Django admin changelist query string by a staff user with view permission. A `dict`, or a `str` holding its JSON representation, is opened in write mode regardless of the constructor's `write=False` default, allowing a file with an attacker-chosen name and contents to be written through a file-backed GDAL driver. Any other `str` is treated as a datasource, allowing an outbound network request through a GDAL virtual filesystem handler. Writing a file to a location later imported by the application can result in remote code execution. Earlier, unsupported Django series (such as 5.1.x, 5.0.x, and 4.2.x) were not evaluated and may also be affected. Django would like to thank Bence Nagy, localhost-detect, and kimchunbok_ for reporting this issue.	8.8	More Details
CVE-2026-69100	LAMP Rapid Development Platform through 5.6.2, fixed in commit 84b0c27, contains a remote code execution vulnerability in GlueFactory that executes unsandboxed Groovy scripts from database template fields without compilation restrictions or whitelisting. Attackers can write or influence the script field via message template endpoints to execute arbitrary Groovy code and OS commands on the backend server.	8.8	More Details
CVE-2026-14270	The Extra Checkout Options (addon for Extra Product Options & Add-Ons for WooCommerce) plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 2.3.2. This is due to missing authorization and nonce validation in the eco_save_settings() function, which allows low-privileged authenticated users to modify the tc_eco_custom_file_types upload allowlist setting, combined with insufficient authorization on the wc_eco_upload_file AJAX action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to allow PHP uploads, upload a PHP file using the frontend upload nonce exposed on cart and checkout pages, and achieve remote code execution. NOTE: This vulnerability was partially fixed in version 2.3.2.	8.8	More Details
CVE-	Type Confusion in V8 in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to		

2026-17989	execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-65944	Joomla Extension - rolandd.com - CSRF vectors in AJAX endpoint handlers RO CSVI < 9.11.0	8.8	More Details
CVE-2026-18650	Missing Authorization vulnerability in HAVELSAN Inc. Liman MYS allows Privilege Escalation. This issue affects Liman MYS: from 2.2.3 before 2.3.1.	8.8	More Details
CVE-2026-17956	Inappropriate implementation in Scheduling in Google Chrome prior to 151.0.7922.72 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-2026-28813	Apache JSPWiki, up to 2.12.3, is vulnerable to JSON Hijacking, which leads to csrf vulnerabilities. Users are recommended to upgrade to version 2.12.4, which fixes this issue.	8.8	More Details
CVE-2026-17070	Missing Authorization vulnerability in HAVELSAN Inc. Liman MYS allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Liman MYS: from 2.2.3 before 2.3.1.	8.8	More Details
CVE-2026-58222	A security flaw combining LDAP filter injection and improper authorization checks was found in Samba Active Directory Domain Controller (AD DC). When processing LDAP Compare requests, Samba fails to properly validate user-supplied attribute names and executes the resulting internal database search in a trusted context, bypassing normal Access Control List (ACL) enforcement. An authenticated low-privilege domain user can exploit these flaws to disclose confidential Active Directory attributes that would normally be inaccessible. The disclosed information may be leveraged to derive sensitive authentication material, potentially leading to privilege escalation and complete domain compromise. For example: In deployments configured with Group Managed Service Accounts (gMSAs), an attacker can extract the "msKds-RootKeyData" attribute and derive gMSA passwords offline, potentially leading to complete domain compromise if privileged gMSAs are present.	8.8	More Details
CVE-2026-17971	Inappropriate implementation in Frame in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-17969	Inappropriate implementation in Passwords in Google Chrome prior to 151.0.7922.72 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-2026-17967	Use after free in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-17894	Use after free in Views in Google Chrome on Linux prior to 151.0.7922.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-13609	The Frontend Admin by DynamiApps WordPress plugin before 3.29.9 decodes HTML entities in a submitted form field value after sanitizing it, which restores HTML tags that the sanitizer had neutralized. A double-encoded payload submitted by an unauthenticated visitor is therefore stored as a live tag and later output without escaping on the Frontend Admin by DynamiApps WordPress plugin before 3.29.9's front-end display surfaces, resulting in stored cross-site scripting that executes in the browser of any user, including an administrator, who views a page displaying the submitted value.	8.8	More Details
CVE-2026-67351	Serendipity before 2.6.1 contains an authentication context confusion vulnerability where password validation and session loading operate independently without ensuring both use the same user record. An authenticated Editor can create a username collision with an Administrator account and obtain administrative privileges by logging in with their own password while the session loads the Administrator's account data.	8.8	More Details
CVE-2026-	Use after free in Enterprise in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity:	8.8	More

17886	Medium)		Details
CVE-2026-17719	Use after free in Input in Google Chrome prior to 151.0.7922.72 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-2026-17725	Type Confusion in V8 in Google Chrome prior to 151.0.7922.72 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-2026-17729	Use after free in V8 in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-50986	PrestaShop module, totadministrativemandate <1.8.1 is vulnerable to Cross Site Request Forgery (CSRF). The payment validation controller has no CSRF token. An attacker can confirm an order in an awaiting status by hijacking a link.	8.8	More Details
CVE-2026-67356	ArcadeDB before 26.7.3 binds the real LocalDatabase object into JavaScript trigger contexts with HostAccess.ALL, allowing schema-admins to call getSecurity().createUser() without permission checks. Attackers with UPDATE_SCHEMA permission can create triggers that execute JavaScript to create server-wide admin users, escalating privileges beyond their authorization level.	8.8	More Details
CVE-2026-15414	The Subscriptions for WooCommerce plugin for WordPress is vulnerable to Privilege Escalation in versions up to, and including, 2.0.0. This is due to the `save_meta_boxes()` function persisting the `_wps_plan_user_role` membership plan meta from `$_POST` without an allowlist that excludes privileged roles — the only validations applied, `sanitize_key()` and `wp_roles()->is_role()`, both accept `'administrator'` as a valid value, and the UI's `disabled` attribute on the role dropdown is a client-side-only control trivially bypassed via DevTools or a direct POST request; additionally, because the `wps_membership_plan` custom post type is registered with `capability_type => 'post'`, any user who can edit posts satisfies the `current_user_can('edit_post', $post_id)` guard in `save_meta_boxes()`. This makes it possible for authenticated attackers, with Contributor-level access and above, to escalate their privileges to Administrator by storing `'administrator'` as the role granted on membership acquisition, which the Pro companion plugin then applies via `add_role()` during membership lifecycle events. Successful exploitation requires the Subscriptions for WooCommerce Pro companion plugin to be active, as it is the component that reads the stored `_wps_plan_user_role` meta via `get_post_meta()` and calls `add_role()` to apply the role during membership lifecycle events.	8.8	More Details
CVE-2026-17807	Use after free in V8 in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-15988	The AI Engine – The Chatbot, AI Framework & MCP for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.6.5 This is due to missing or incorrect nonce validation on the reauth_for_authorize function. This makes it possible for unauthenticated attackers to create new administrator accounts with attacker-supplied credentials via a CSRF-based REST authentication bypass, granted they can trick a site administrator into performing an action such as clicking on a link. This bypass can be combined with WordPress's ?_method=POST method-override support to convert a top-navigation GET request into an authenticated POST to the REST users endpoint, requiring no existing account on the attacker's part.	8.8	More Details
CVE-2026-16635	The Pronamic Pay plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 10.1.0 This is due to the `maybe_update_user_role()` function passing an attacker-controlled Gravity Forms field value (`$lead[$feed->user_role_field_id]`) directly into `WP_User::set_role()` without any allowlist validation, capability comparison, or permission check to constrain which roles can be assigned. This makes it possible for authenticated attackers, with Subscriber-level access and above, to escalate their own WordPress account to Administrator by tampering with the role field value in a form submission. Exploitation requires that an administrator has already configured a Pronamic Pay payment feed in Gravity Forms with the **Update User Role** option enabled and mapped to a form field; once that configuration is in place, no further preconditions exist to prevent an authenticated attacker from exploiting this vulnerability.	8.8	More Details
CVE-	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72		More

2026-17786	allowed an attacker who convinced a user to install a malicious extension to perform privilege escalation via a crafted Chrome Extension. (Chromium security severity: Medium)	8.8	Details
CVE-2026-17751	Inappropriate implementation in AdFilter in Google Chrome prior to 151.0.7922.72 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-2026-17752	Use after free in Views in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-17784	Use after free in Audio in Google Chrome on Mac prior to 151.0.7922.72 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)	8.8	More Details
CVE-2026-67343	ArcadeDB versions before 26.7.2 fail to properly redact the cluster token in the GET /api/v1/server endpoint, allowing authenticated users to retrieve the arcadedb.ha.clusterToken value in cleartext. Attackers can use the leaked token with X-ArcadeDB-Cluster-Token and X-ArcadeDB-Forwarded-User headers to impersonate root and execute administrative actions including user creation, database operations, and server shutdown.	8.8	More Details
CVE-2026-17778	Use after free in Extensions in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted Chrome Extension. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-17712	Race in Skia in Google Chrome on Mac prior to 151.0.7922.72 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-2026-17705	Integer overflow in libxml in Google Chrome prior to 151.0.7922.72 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-2026-17694	Use after free in DOM in Google Chrome prior to 151.0.7922.72 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-2026-18598	A vulnerability was detected in GL.iNet GL-MT3000 up to 4.4.5. The affected element is the function logread.get_system_log of the file /usr/lib/oui-httpd/rpc/logread of the component Logread Lua RPC plugin. The manipulation of the argument module results in command injection. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	8.8	More Details
CVE-2026-17884	Object lifecycle issue in WebRTC in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-18600	A vulnerability has been found in GL.iNet GL-MT3000 up to 4.4.5. This affects the function network.switch_info/network.switch_status of the file /usr/lib/oui-httpd/rpc/network of the component Network Lua RPC Plugin. Such manipulation of the argument switch leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	8.8	More Details
CVE-2026-17881	Integer overflow in WebXR in Google Chrome prior to 151.0.7922.72 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-2026-17875	Use after free in PDFium in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-16236	The Realtyna Organic IDX plugin for WordPress is vulnerable to Arbitrary File Upload in versions up to, and including, 5.3.0. This is due to missing file extension and content validation in the saveLiveImages() function combined with an insufficient authorization check on the get_keys() AJAX handler and a missing authentication check on the REST API import endpoint. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details

CVE-2026-17868	Insufficient policy enforcement in USB in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform privilege escalation via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-17658	Use after free in V8 in Google Chrome prior to 151.0.7922.72 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-2026-17836	Use after free in V8 in Google Chrome prior to 151.0.7922.72 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-2026-17661	Use after free in Loader in Google Chrome prior to 151.0.7922.72 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-2026-17665	Use after free in V8 in Google Chrome prior to 151.0.7922.72 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-2026-17346	The fix for CVE-2026-12044 in pgAdmin 4 9.16 hardened qtLiteral and switched sixteen COMMENT ON / pgstattuple / pgstatindex templates to it, but missed several sinks that had been placed in test_sql_string_literal_lint.py's ALLOWLIST on the incorrect assumption that schema, table, publication, and subscription names sourced from pg_catalog via the browser tree could never contain an apostrophe. PostgreSQL permits arbitrary characters in quoted identifiers, so a low-privileged user able to CREATE TABLE, CREATE PUBLICATION, or CREATE SUBSCRIPTION can plant an apostrophe'd object name that breaks out of the unescaped '{{ name }}' template interpolation the moment any user (including a higher-privileged one) opens that object's Statistics or Dependencies tab, allowing arbitrary SQL statement injection in the viewing user's database session. Affected sinks: the Index Statistics query for all-indexes listing (coll_stats.sql, both the 16_plus and default PostgreSQL-version template variants -- distinct from the single-index stats.sql path already fixed in CVE-2026-12044), and the publication and subscription dependencies.sql / get_position.sql templates (both the pg and ppas/EPAS dialect variants for publications). Fix switches all of these templates to qtLiteral(conn) for name interpolation, and updates publications/__init__.py and subscriptions/__init__.py to pass conn=self.conn into the dependencies.sql render_template call so the qtLiteral filter has a connection to quote against. The corresponding ALLOWLIST entries in test_sql_string_literal_lint.py are removed now that these sinks are properly escaped rather than merely assumed safe. A behavioral regression test renders each fixed template with a stacked-statement apostrophe payload and asserts both that the object name appears exactly as qtLiteral-escaped and that the rendered SQL parses as exactly one statement, verifying the assertion genuinely fails against the pre-patch raw-interpolation form. This issue affects pgAdmin 4: the Index Statistics sink from 1.0, and the Publications/Subscriptions sinks from 5.0, both before 9.17.	8.8	More Details
CVE-2026-17677	Inappropriate implementation in ANGLE in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-17678	Out of bounds read in ANGLE in Google Chrome prior to 151.0.7922.72 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)	8.8	More Details
CVE-2026-17685	Use after free in Autofill in Google Chrome prior to 151.0.7922.72 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-2026-14522	IBM App Connect Enterprise 13.0.1.0 through 13.0.7.2, and 12.0.1.0 through 12.0.12.27 could allow a remote attacker to execute arbitrary commands due to improper neutralization of CRLF characters.	8.8	More Details
CVE-2026-67325	GitPython before 3.1.51 contains an incomplete command injection blocklist that fails to account for git's long-option prefix abbreviation feature. Attackers can bypass the unsafe options guard by using abbreviated option names like upload_p instead of upload_pack, which git resolves to dangerous options and executes arbitrary commands.	8.8	More Details

CVE-2026-22622	Improper input validation in one of the session management interface of Eaton's Tripp Lite series PADM firmware could allow an authenticated user to elevate privileges resulting in unrestricted access to the device.	8.8	More Details
CVE-2026-16793	An improper neutralization of special elements used in an operating system command vulnerability was reported in Lenovo XClarity Orchestrator (LXCO) 2.2.0 that could allow an authenticated attacker to execute arbitrary operating system commands as a privileged user under a specific circumstance.	8.8	More Details
CVE-2026-50622	Description: Missing Authorization in Apache Atlas. A missing authorization vulnerability in Apache Atlas's admin endpoints allows any authenticated user, regardless of their assigned role, to perform administrative operations. Affect Version: This issue affects Apache Atlas: from 0.8 through 2.5.0. Mitigation: Users are recommended to upgrade to version 2.6.0, which fixes the issue.	8.8	More Details
CVE-2026-18017	Use after free in Dawn in Google Chrome prior to 151.0.7922.72 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-2026-70619	Odysseus before commit bf325f6 contains a missing authorization vulnerability that allows authenticated non-admin users to manage server-wide embedding backend configuration by invoking endpoint management routes that verify session authentication but omit the admin authorization guard. Attackers can supply an attacker-controlled URL to overwrite the embedding backend persisted in the endpoint configuration file and process environment, causing all subsequent embedding operations including chat messages, RAG queries, memory entries, and vault text to be transmitted in plaintext to the attacker-controlled destination, or delete the endpoint configuration to deny embedding service to all users.	8.8	More Details
CVE-2026-12144	The Wholesale for WooCommerce plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.0.5. This is due to the `save_requests_meta()` function applying only `sanitize_text_field()` to the `user_role_set` POST parameter before passing it directly to `WP_User::add_role()`, with no allowlist validation against permitted wholesale roles and no capability check such as `current_user_can('promote_users')` or `current_user_can('manage_options')`. This makes it possible for authenticated attackers with author-level access and above to escalate their privileges to administrator by supplying `administrator` as the `user_role_set` value in a crafted request. The function is gated only by a nonce (`request_user_role_nonce`) that is rendered in the meta box on the `wwp_requests` post edit screen; because the post type is registered with `capability_type => 'post'`, any author-level user who has authored a `wwp_requests` post — such as one created via the wholesale registration form — can access this nonce and submit the role-assignment request.	8.8	More Details
CVE-2026-14356	The FleekDash V2 plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.6.2.2. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to overwrite the email address and password of any WordPress user, including administrators, enabling full account takeover and complete site compromise. The public /wp-json/fleekdash/v1/register endpoint auto-provisions a Subscriber-role account and returns a valid REST nonce regardless of the site's users_can_register setting, enabling unauthenticated attackers to self-provision the required credentials and nonce in a single prior request.	8.8	More Details
CVE-2026-67248	A stack-based buffer overflow vulnerability was found in the File Explorer on the ADM. The vulnerability occurs because user-controlled input is not properly validated before being decoded and copied into a fixed-size stack buffer. An authenticated attacker can exploit this issue to cause denial of service of the affected CGI process. Further impact may be possible depending on exploitability and runtime protections. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.RUN1 as well as from ADM 5.0.0 through ADM 5.1.3.RI81.	8.8	More Details
CVE-2026-54368	CentreStack before 17.4 contains a SQL injection vulnerability in GladDBFiles.SearchEx() and SearchExUnder() that allows authenticated attackers to execute arbitrary SQL statements by supplying a crafted x-glad-filter request header through the jsondir API endpoint. Attackers can exploit unsanitized interpolation of the Field parameter directly into SQL query strings to write arbitrary files to the server filesystem via PostgreSQL lo_from_bytea() and lo_export() functions, enabling remote code execution.	8.8	More Details
CVE-2026-16526	A flaw in the PCP linux_sockets module exposes an unsecured internal connection. An attacker with initial code execution can exploit this to escalate privileges and execute arbitrary commands as root.	8.8	More Details

CVE-2026-64557	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix use-after-free in l2cap_sock_new_connection_cb() l2cap_sock_new_connection_cb() returned l2cap_pi(sk)->chan after release_sock(parent). Once the parent lock is dropped the newly enqueued child socket sk is reachable via the accept queue, so another task can accept and free it before the callback dereferences sk, resulting in a use-after-free. Rework the ->new_connection() op so the core, rather than the callback, owns the child channel's lifetime. The op now receives a pre-allocated new_chan and returns an errno instead of allocating and returning a channel. l2cap_new_connection() allocates the child channel and links it into the conn list via __l2cap_chan_add() before invoking the callback, so the conn-list reference keeps the channel alive once release_sock(parent) exposes the socket to other tasks. Channel configuration that was duplicated in l2cap_sock_init() and the various new_connection callbacks is consolidated into l2cap_chan_set_defaults(), which now inherits from the parent channel when one is supplied.	8.8	More Details
CVE-2026-18012	Use after free in PDFium in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: Low)	8.8	More Details
CVE-2026-67336	better-auth versions before 1.6.11 contain insecure cryptographic defaults in the oidcProvider and mcp plugins that advertise the none algorithm and accept plain PKCE by default. Attackers can exploit algorithm negotiation to accept unsigned tokens or intercept authorization codes when PKCE plain is used instead of the required S256 method.	8.7	More Details
CVE-2026-70492	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.10.0 until 0.11.0, src/lib/components/chat/Messages/Markdown/KatexRenderer.svelte could store and render a chat message whose math block makes KaTeX fail with a stack overflow instead of a parse error. The catch branch fell back to inserting the original math source into the page as HTML through {@html} rather than as text, so script in the message runs in the browser of whoever views it, including shared chats and channels. The viewer's session token in localStorage can be stolen, and an administrator viewer can have their account taken over. This issue is fixed in 0.11.0.	8.7	More Details
CVE-2026-58157	Apache Traffic Server can reuse server sessions and tunnels improperly, exposing data across client connections. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	8.7	More Details
CVE-2026-22620	Improper input validation in the authentication component of Eaton's Tripp Lite series PADM firmware could allow an unauthenticated remote attacker to bypass authentication and gain a privileged user access to the device.	8.6	More Details
CVE-2026-44094	An unauthenticated remote attacker can enforce the system to fall back to a firmware partition with an insecure configuration including default credentials. This could allow the attacker to gain SSH access to the system as an unprivileged user "user-app". Charging could be interrupted.	8.6	More Details
CVE-2026-67201	V through 0.5.2, fixed in commit 85859f0, contains a server-side request forgery (SSRF) bypass vulnerability that allows attackers to circumvent host-based allowlists by exploiting a parser differential between net.urllib and net.http. Attackers can craft a URL containing a backslash in the authority section such that net.urllib.parse() extracts the trusted host for allowlist validation while net.http.get() normalizes the backslash and connects to the internal host, enabling access to internal network services that the allowlist was intended to block.	8.6	More Details
CVE-2026-17699	Use after free in Views in Google Chrome prior to 151.0.7922.72 allowed a local attacker to potentially perform a sandbox escape via a malicious file. (Chromium security severity: High)	8.6	More Details
CVE-2026-16572	The LogMyTrip WordPress plugin through 1.9 does not sanitize and escape a value taken from a cookie before using it in a SQL query, allowing unauthenticated users to perform SQL injection attacks on any page that renders one of the LogMyTrip WordPress plugin through 1.9's shortcodes.	8.6	More Details
CVE-2026-54367	CentreStack before 17.2 contains an authentication bypass vulnerability that allows unauthenticated attackers to read, write, or delete arbitrary account settings by exploiting exposed API endpoints that lack authorization checks. Attackers can generate valid encrypted EntAcctId values using the static shared encryption key to forge identifiers for any user GUID, including the system-wide cluster settings account, enabling enumeration of hosted tenant domains and administrator identities.	8.6	More Details

CVE-2025-71399	Better Auth relies on better-call, which uses the rou3 router library. In affected versions of rou3, paths are normalized by removing empty segments, so /path, //path, and ///path resolve to the same route. In Better Auth versions prior to 1.4.5 (which bundles the fixed rou3), this can allow attackers to bypass disabledPaths configuration and path-based rate limits by submitting requests with extra slashes in the URL path. The issue does not apply in deployments where the proxy or platform normalizes URLs by collapsing multiple slashes.	8.6	More Details
CVE-2026-58182	The Apache Traffic Server ts_lua plugin mishandles initialization, transform context, and per-instance state. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	8.6	More Details
CVE-2026-44098	This vulnerability allows an unauthenticated remote attacker with control over the OCPP backend via firewall-bypass to perform an OS command injection, resulting in the execution of arbitrary commands as the limited user charx-oa. Charging could be interrupted.	8.6	More Details
CVE-2026-48448	Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to gain file system read access. Exploitation of this issue does not require user interaction. Scope is changed.	8.6	More Details
CVE-2026-13395	The Online Scheduling and Appointment Booking System WordPress plugin before 27.8 does not sanitize or properly cast a user-supplied parameter from its unauthenticated front-end booking requests before using it in a SQL query, allowing unauthenticated attackers to perform SQL injection attacks and extract sensitive data such as password hashes from the database.	8.6	More Details
CVE-2026-67425	Flyto2 Core is an execution kernel for automation and AI-agent workflows. Prior to 2.26.6, llm.chat reads provider keys such as OPENAI_API_KEY and ANTHROPIC_API_KEY from the environment and sends them in the Authorization: Bearer header to caller-controlled base_url, allowing an attacker to receive the operator's key on a public host that passes the SSRF guard. This issue is fixed in version 2.26.6.	8.6	More Details
CVE-2026-12721	The Kirki WordPress plugin before 6.0.13 does not properly sanitise and escape a value taken from the request before using it in a SQL statement, allowing unauthenticated attackers to perform SQL injection attacks.	8.6	More Details
CVE-2026-16328	In consul-mcp-server, versions 0.1.0 up to 0.1.3 did not restrict how the Consul backend address was supplied, allowing a connected client to override the server's configured Consul address via a request header. This may allow a malicious client to redirect the server's Consul API traffic to an attacker-controlled endpoint, potentially exfiltrating the Consul token configured on the server. This vulnerability, CVE-2026-16328, is fixed in consul-mcp-server 0.1.4.	8.6	More Details
CVE-2026-68587	SiYuan versions before v3.7.3 contain an information disclosure vulnerability in the getHeadingDeleteTransaction, getHeadingLevelTransaction, and getHeadingInsertTransaction endpoints that return rendered block DOM without publish-access checks. Anonymous readers or publish RoleReader tokens can supply a heading block ID to read full rendered content of publish-disabled documents that should be restricted.	8.6	More Details
CVE-2026-67346	Swarms through 6.8.1, fixed in commit 8b0fc9e, contains a server-side request forgery vulnerability in the _is_safe_url function that fails to validate hostnames through DNS resolution, allowing attackers to bypass the blocklist. Attackers can supply user-controlled image or audio URLs that resolve to private, loopback, or metadata addresses to reach internal services and exfiltrate credentials.	8.6	More Details
CVE-2026-68584	SiYuan versions before v3.7.3 contain an authentication bypass vulnerability in publish mode where content-returning endpoints getHeadingChildrenDOM, getHeading*Transaction, and getBacklinkDoc perform no password check despite protecting the primary getDoc endpoint. Anonymous attackers can retrieve full content of password-protected documents by obtaining internal block IDs from reader-accessible endpoints and calling unprotected content endpoints to bypass the password gate.	8.6	More Details
CVE-2026-67427	Flyto2 Core is an execution kernel for automation and AI-agent workflows. Prior to 2.26.6, the workflow engine variable resolver expands ${env.VAR} for any host environment variable without an allowlist or capability policy check, allowing a workflow parameter to bypass the default capability policy denylist for env.get and env.load_dotenv and exfiltrate secrets through allowed modules. This issue is fixed in version 2.26.6.	8.6	More Details

CVE-2026-11974	The wp-media-folder-addon WordPress plugin through 4.1.6 does not validate a user-supplied parameter before using it in a file read operation in two AJAX actions available to unauthenticated users, leading to Arbitrary File Disclosure and Server-Side Request Forgery on sites where a cloud storage connection has been configured. This is an incomplete fix of CVE-2026-9690, whose patch hardened only one of the affected cloud-storage handlers and left the others unpatched.	8.6	More Details
CVE-2026-68586	SiYuan before v3.7.3 fails to apply publish-access filters to the getBacklinkDoc and getBackmentionDoc content endpoints (/api/ref/getBacklinkDoc and /api/ref/getBackmentionDoc). While the corresponding backlink list endpoints filter publish-forbidden documents, the content endpoints (gated only by CheckAuth) do not. A publish-mode reader — including an anonymous reader when publish Basic Auth is disabled — can call these endpoints directly with a publish-forbidden document's ID to retrieve its rendered DOM content and to determine whether the document references a given block (a reference-existence oracle).	8.6	More Details
CVE-2026-66415	Leantime 3.6.2 contains a server-side request forgery and local file inclusion vulnerability that allows authenticated attackers to read internal resources by passing unsanitized user-supplied filenames to file_get_contents() in the Blueprints::import() method without path validation. Attackers can submit crafted filenames containing URL wrappers or path traversal sequences through the JSON-RPC API endpoint to access cloud metadata services or read arbitrary files from the server filesystem.	8.5	More Details
CVE-2026-62246	Kamaji is the Hosted Control Plane Manager for Kubernetes. Prior to 26.7.4-edge, Kamaji derives a TenantControlPlane datastore schema, database user, and etcd key prefix from a lossy namespace-and-name normalization in GetDefaultDatastoreSchema() and GetDefaultDatastoreUsername(), allowing distinct tenants with colliding normalized identifiers to share control-plane state and read, modify, or destroy another tenant's Kubernetes data. This issue is fixed in version 26.7.4-edge.	8.5	More Details
CVE-2026-67424	Flyto2 Core is an execution kernel for automation and AI-agent workflows. Prior to 2.26.7, the HTTP modules http.get, http.request, and http.batch in src/core/modules/atomic/http/get.py, src/core/modules/atomic/http/request.py, and src/core/modules/atomic/http/batch.py validate only the initial URL, then follow redirects with allow_redirects=True and without per-hop Location revalidation, allowing a public URL to redirect into internal address space and return the internal response body. This issue is fixed in version 2.26.7.	8.5	More Details
CVE-2026-11536	IBM WebSphere Application Server 9.0, and 8.5 is affected by a remote code execution vulnerability in the SOAP/JMX connector.	8.5	More Details
CVE-2026-10079	A flaw was found in Red Hat Advanced Cluster Security for Kubernetes (RHACS). When processing Kubernetes Deployments, ACS replaces deployment identity metadata based on the openshift.io/encoded-deployment-config label. A user with permission to create Deployments can set this label to "null", causing ACS to treat the workload as having empty UID, name and labels and namespace "default". This bypasses deploy-time policy detection and enforcement visibility, prevents correct persistence in Central and breaks violation reporting and compliance correlation for the affected deployment.	8.5	More Details
CVE-2026-57862	Kanboard 1.2.52 and prior contains a server-side request forgery vulnerability that allows authenticated users to bypass SSRF protections by supplying hexadecimal IP address notation in user-controlled URLs. Attackers can submit hexadecimal-encoded internal IP addresses through the web link creation feature, causing cURL to resolve and connect to internal network resources such as cloud instance metadata services, localhost services, and RFC1918 addresses while the isPrivateURL() filter in app/Core/Http/Client.php incorrectly treats the input as safe due to FILTER_VALIDATE_IP rejecting non-dotted-decimal notation.	8.5	More Details
CVE-2026-67428	Flyto2 Core is an execution kernel for automation and AI-agent workflows. Prior to 2.26.7, HTTP-emitting modules including src/core/modules/third_party/developer/http/requests.py, core.api.http_get, core.api.http_post, graphql.query, graphql.mutation, monitor.http_check, communication.slack_send, notification.discord.send_message, notification.slack.send_message, notification.teams.send_message, ai.vision_analyze, verify.visual_diff, browser.proxy_rotate, and the agent and llm inline base_url branch fetch caller-controlled URLs without validate_url_with_env_config, allowing SSRF to internal or metadata endpoints. This issue is fixed in version 2.26.7.	8.5	More Details
CVE-	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 10.1.0 before 19.0.5,		

2026-6267	19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user with Developer role to access unauthorized information due to insufficient access controls on internal request handling.	8.5	More Details
CVE-2026-11885	IBM PowerVM Hypervisor FW1110.00 through FW1110.20, FW1060.00 through FW1060.71, and FW950.00 through FW950.H1 A carefully crafted OS hypervisor call can cause the PowerVM hypervisor to crash or compromise OS memory integrity.	8.4	More Details
CVE-2026-67323	GitPython before 3.1.51 fails to guard against dangerous Git options passed as keyword arguments in Repo.archive() and git.ls_remote(), allowing command injection via options such as --exec/--upload-pack (leading to arbitrary command execution). Additionally, Repo.iter_commits() and Repo.blame() do not check for leading-dash revision arguments, so a revision like --output=<path> can cause Git to open and truncate an arbitrary file. Exploitation requires an application that passes attacker-controlled arguments to these methods.	8.4	More Details
CVE-2026-17716	Use after free in Updater in Google Chrome on Mac prior to 151.0.7922.72 allowed a local attacker to perform privilege escalation via malicious network traffic. (Chromium security severity: High)	8.4	More Details
CVE-2026-10535	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 is vulnerable to buffer overflow in setgid helper db2flacc.	8.4	More Details
CVE-2026-17877	Inappropriate implementation in Chromoting in Google Chrome on Linux prior to 151.0.7922.72 allowed a local attacker to perform OS-level privilege escalation via malicious network traffic. (Chromium security severity: Medium)	8.4	More Details
CVE-2026-12436	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.0 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user to modify CI/CD configuration belonging to another user due to improper validation of user-supplied attributes when processing pipeline schedule inputs.	8.4	More Details
CVE-2026-5219	Cross-Site request forgery (CSRF) vulnerability in Softtr Information Technology Trade Ltd. Co. E-Commerce Pack allows Cross Site Request Forgery. This issue affects E-Commerce Pack: before 5.03.01.49.	8.3	More Details
CVE-2026-17723	Use after free in Media in Google Chrome on Windows prior to 151.0.7922.72 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-2026-67327	better-auth versions >= 1.1.3 and < 1.6.22 (and pre-release versions >= 1.7.0-beta.0 and < 1.7.0-beta.10) are vulnerable to account takeover via pre-account hijacking on magic-link and email-OTP sign-in when open email/password registration is enabled. An attacker registers an account with the victim's email address and an attacker-chosen password; the account remains unverified. When the legitimate owner later signs in via the magic-link or email-OTP passwordless flow, the account is marked verified without removing the pre-existing password or revoking existing sessions, so the attacker's password remains valid, granting persistent access to the victim's account. Fixed in 1.6.22 and 1.7.0-beta.10.	8.3	More Details
CVE-2026-22621	Improper input validation in one of the session management interface of Eaton's Tripp Lite Series PADM firmware could allow an authenticated administrator to execute arbitrary commands within a restricted environment.	8.3	More Details
CVE-2026-14980	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 is vulnerable to cross-site request forgery which could allow an attacker to perform SSRF attacks with elevated privileges when the collectiveController-1.0 feature is enabled.	8.3	More Details
CVE-2026-47882	When enabling Spring Boot DevTools support for a remote application target (for example a Docker container or Cloud Foundry app) from the Spring Tools Boot Dashboard, Spring Tools generates a shared secret that authenticates DevTools remote-restart uploads to the deployed application. This secret was generated using a non-cryptographic pseudo-random number generator rather than a cryptographically secure source of randomness. Affected Spring Products and Versions: Spring Tools for Eclipse: 5.2.0 and earlier	8.3	More Details
CVE-2026-67331	better-auth SCIM versions from 1.5.0 before 1.7.0-beta.4 fail to bind non-organization SCIM providers to their creator by default, allowing authenticated users to manage other users' providers. Attackers can regenerate SCIM bearer tokens, invalidate legitimate tokens, and	8.3	More Details

	authenticate to SCIM API routes with the attacker-controlled token.		
CVE-2026-58153	Apache Traffic Server forwards HTTP/2 origin trailers to HTTP/1 clients without proper chunked framing when converting HTTP/2 to HTTP/1. This issue affects Apache Traffic Server: from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	8.3	More Details
CVE-2026-17722	Object lifecycle issue in WebView in Google Chrome on Android prior to 151.0.7922.72 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-2026-17650	Use after free in Compositing in Google Chrome prior to 151.0.7922.72 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-2026-54666	swagger-typescript-api generates API clients for Fetch or Axios from an OpenAPI Specification. Prior to 13.12.2, src/schema-routes/schema-routes.ts passes OpenAPI path keys through parseRouteName to templates/default/procedure-call.ejs and templates/modular/procedure-call.ejs without escaping JavaScript template literal interpolation, allowing an attacker-controlled path containing ${...} to execute when the generated method is called. This issue is fixed in version 13.12.2.	8.3	More Details
CVE-2026-17663	Insufficient validation of untrusted input in GPU in Google Chrome on Android prior to 151.0.7922.72 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-2026-54661	swagger-typescript-api generates API clients for Fetch or Axios from an OpenAPI Specification. Prior to 13.12.2, templates/base/http-clients/axios-http-client.ejs interpolates servers[0].url from src/code-gen-process.ts into the HttpClient constructor without escaping, allowing an attacker-controlled OpenAPI spec to inject code that executes when new HttpClient() or new Api() is constructed. This issue is fixed in version 13.12.2.	8.3	More Details
CVE-2026-54662	swagger-typescript-api generates API clients for Fetch or Axios from OpenAPI specifications. Prior to 13.12.2, src/code-gen-process.ts createApiConfig copies servers[0].url into apiConfig.baseUrl, and templates/base/http-clients/fetch-http-client.ejs interpolates apiConfig.baseUrl into the generated HttpClient baseUrl field without escaping, allowing an attacker-controlled OpenAPI spec to inject TypeScript static field code that executes when the generated fetch client module is imported. This issue is fixed in version 13.12.2.	8.3	More Details
CVE-2026-54664	swagger-typescript-api generates API clients for Fetch or Axios from an OpenAPI Specification. Prior to 13.12.2, src/schema-parser/base-schema-parsers/enum.ts passes components.schemas.*.enum[i] values to Ts.StringValue in src/configuration.ts without escaping before templates/base/enum-data-contract.ejs renders TypeScript enum declarations, allowing an attacker-controlled OpenAPI spec to inject code that executes when the generated module is imported. This issue is fixed in version 13.12.2.	8.3	More Details
CVE-2026-17660	Insufficient validation of untrusted input in Network in Google Chrome prior to 151.0.7922.72 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-2026-17657	Use after free in Navigation in Google Chrome prior to 151.0.7922.72 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-2026-17653	Use after free in Skia in Google Chrome prior to 151.0.7922.72 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-2026-56670	ComfyUI is a modular diffusion model GUI, api and backend with a graph/nodes interface. Prior to 0.28.0, the /view endpoint served uploaded SVG files inline because image/svg+xml and related XML content types were absent from the dangerous-content-type handling, allowing stored cross-site scripting in the ComfyUI origin. This issue is fixed in version 0.28.0.	8.2	More Details
CVE-2026-47623	NVIDIA Dynamo for Linux contains a vulnerability where an attacker could cause deserialization of untrusted data. A successful exploit of this vulnerability might lead to denial of service and data tampering.	8.2	More Details

CVE-2026-56672	ComfyUI is a node-based diffusion model GUI, API, and backend. Prior to 0.28.0, GET /userdata/{file} served user-controlled HTML and SVG files with extension-derived content types, allowing stored cross-site scripting in the ComfyUI origin and access to browser-stored API tokens, settings, workflows, and authenticated-equivalent API calls. The handler used web.FileResponse(path), so an uploaded .html/.svg was served as text/html/image/svg+xml. POST /userdata stores arbitrary request bodies (confined to the user's userdata directory). When a victim navigated to the file URL, the embedded script executed same-origin. The /view endpoint already forced dangerous MIME types to download; that protection had never been applied to /userdata. This issue is fixed in version 0.28.0.	8.2	More Details
CVE-2026-10849	The hawkBit device management client in subsys/mgmt/hawkbit accumulates the body of an HTTP response from the update server into a heap buffer in response_json_cb() (subsys/mgmt/hawkbit/hawkbit.c). The buffer is sized to hold the received body bytes but reserves no space for a terminating NUL. When the full response has arrived, the code writes response_data[downloaded_size] = '\0' — and whenever the accumulated body length equals the allocation, that terminator lands one byte past the end of the heap object (a heap-based out-of-bounds write, CWE-122 / CWE-787). The body length and fragmentation are taken directly from the parsed HTTP response (rsp->body_frag_start / rsp->body_frag_len) and are fully controlled by the remote hawkBit server, which chooses its own response length. The precise trigger depends on how the buffer grows, and both forms are remotely reachable. Since v4.0.0 the reallocation is sized to exactly downloaded_size + body_len, so any response body larger than the 1100-byte initial buffer makes the out-of-bounds write deterministic; such response sizes are normal for hawkBit deployment metadata. Before v4.0.0 the buffer grew by doubling and the growth check ((downloaded_size + body_len) > response_buffer_size) is false at equality, so a response body whose length is exactly the current allocation — 1100 bytes with the default initial buffer — skips the reallocation entirely and writes the terminator at response_data[1100] of an 1100-byte object. The HTTP length-mismatch check does not catch this, because the declared and received lengths genuinely agree. Either form is reachable by a malicious, compromised, or man-in-the-middle update server (TLS is optional and, when enabled, does not protect against a hostile server), with no authentication of response content and no client-side length cap protecting the write. The out-of-bounds write is a fixed single NUL byte immediately following the allocation, corrupting adjacent allocator metadata or the next allocation. The practical impact is heap corruption leading to denial of service (fault on a subsequent allocation or free), with the bounded, allocator-dependent possibility of further corruption. The fix sizes the buffer to the body length plus one and copies with memcpy, ensuring the terminator always lands within the allocation.	8.2	More Details
CVE-2026-70486	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.0 until 0.11.0, the terminal file-preview serveUrl iframe branch always granted allow-same-origin together with allow-scripts for HTML files served from the application origin. Any authenticated user with access to a configured terminal server could cause script in a previewed file to run in the Open WebUI origin, read the victim's session token from localStorage, and take over the account, with possible server-side code execution if the victim was an admin or held workspace.functions. This issue is fixed in 0.11.0.	8.2	More Details
CVE-2026-54727	proot-distro is a utility for managing proot containers. Prior to version 5.1.6, proot-distro restore accepted hardlink entries whose linkname referenced another installed container and did not verify that the hardlink source container matched the destination container being restored, allowing a crafted restore archive to copy files between otherwise isolated containers. This issue is fixed in version 5.1.6.	8.2	More Details
CVE-2026-54574	proot-distro is a utility for managing proot containers. Prior to version 5.1.5, proot-distro install extracted plain tarball root filesystems through _extract_plain_tar() in proot_distro/commands/install.py and Docker layers through _apply_layer() in proot_distro/helpers/docker.py without validating archive-controlled symlink targets in member.linkname, allowing a malicious archive to plant an absolute host-path symlink and write files through it onto the host filesystem. This issue is fixed in version 5.1.5.	8.2	More Details
CVE-2026-22068	Regular Expression without Anchors vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 10.0.X through 10.1.3, from 9.0.X through 9.2.14. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fixes the issue.	8.2	More Details
CVE-2026-58159	Apache Traffic Server can bypass IP access controls on UDS listeners and through ACL matching errors. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	8.2	More Details

CVE-2026-14920	## Summary	8.2	More Details
CVE-2026-53500	Thumbor is an open-source photo thumbnail service by globo.com. Prior to 7.8.0, the ALLOWED_SOURCES configuration passes plain strings to re.match() without escaping dots, so a hostname differing at dot positions can match the allowlist. This issue is fixed in 7.8.0.	8.2	More Details
CVE-2026-24253	NVIDIA Dynamo for Linux contains a vulnerability where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to denial of service and data tampering.	8.2	More Details
CVE-2026-18141	A flaw was found in aap-gateway, a component of Ansible Automation Platform's Event-Driven Ansible (EDA). An unauthenticated remote attacker can bypass mutual Transport Layer Security (mTLS) authentication for event streams. This is achieved by manipulating the event stream URL and forging the HTTP Subject header. The system also inadvertently discloses the expected certificate subject in error messages, which simplifies the attack. This vulnerability allows an attacker to inject arbitrary events into EDA, potentially triggering automated workflows.	8.2	More Details
CVE-2026-53501	Thumbor is an open-source photo thumbnail service by globo.com. Prior to 7.8.0, Thumbor’s HMAC validation can be bypassed due to the use of Python’s .replace() when removing the signature from the URL before validation. Since .replace() removes all occurrences of the substring, an attacker can insert the same signature multiple times in the URL and manipulate the final URL used for validation. This allows crafting URLs where the validated string differs from the actual requested resource, enabling loading images from unintended domains or paths. This issue is fixed in 7.8.0.	8.2	More Details
CVE-2026-58188	Several Apache Traffic Server experimental plugins have memory-safety and limit-bypass errors. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	8.2	More Details
CVE-2026-12722	Missing authentication for critical function vulnerability in FTC Software IT Services FTC E-Commerce Management Panel allows Authentication Bypass. This issue affects FTC E-Commerce Management Panel: before 1.0.2.	8.2	More Details
CVE-2026-58184	The Apache Traffic Server header_rewrite plugin can crash or corrupt memory during cookie operations and CIDR condition matching. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	8.2	More Details
CVE-2026-67348	Julep contains an insecure direct object reference vulnerability in the get_execution_details endpoint that allows authenticated tenants to read another tenant's execution data. Attackers can supply arbitrary execution_id values to retrieve sensitive execution records including task inputs, outputs, metadata, and temporal task tokens from other tenants.	8.1	More Details
CVE-2026-12251	The Ultimate Member WordPress plugin before 2.12.1 does not filter administrator-level capabilities from the roles it makes selectable on its registration forms, and its post-registration safeguard against elevated accounts is disabled by default, allowing unauthenticated users to register with a site-defined role that carries administrator capabilities and gain administrative access, when such a role exists and a role-selection field is present on a published registration form.	8.1	More Details
CVE-2026-18092	Net::SAML2 versions before 0.86 for Perl allow SAML authentication bypass via XML signature wrapping because new_from_xml reads assertion identity with document-wide XPath instead of the signed subtree. new_from_xml reads the NameID, attribute values, SessionIndex, audience and other identity fields with document-wide XPath, such as //saml:Assertion/saml:AttributeStatement/saml:Attribute and //saml:Subject/saml:NameID, which select the first matching element in document order rather than the element covered by the verified signature. handle_response confirms that a signature is present and, when a cacert is configured, that it chains to the CA, but XML::Sig verifies only the element named by the signature's Reference URI, so unsigned sibling assertions in the same document are not covered. An attacker who holds any one IdP-signed assertion can add an unsigned attacker-authored assertion earlier in document order; the signature still verifies and the document-order XPath returns the attacker's NameID and attributes. Any caller that passes an untrusted Response to new_from_xml can accept identity fields from an assertion the IdP never signed, even when a	8.1	More Details

	cacert trust anchor is configured, so a party holding one valid IdP-signed assertion can authenticate as an arbitrary user.		
CVE-2026-58179	The Apache Traffic Server regex_remap plugin overflows the stack and integers from substitution input. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	8.1	More Details
CVE-2026-15658	A vulnerability in the foreUP customer REST API allows any authenticated, low-privilege customer to access an endpoint that returns the records of other users without checking that the caller owns the data associated with that record.	8.1	More Details
CVE-2026-67611	OpenEMR through 8.2.0 contains an authentication bypass vulnerability that allows attackers with valid credentials to circumvent multi-factor authentication by exploiting the exposed OAuth2 password grant flow through an unauthenticated client registration endpoint. Attackers can register an OAuth2 client via the unauthenticated registration endpoint and use the password grant to exchange credentials for an API access token, bypassing the normal web interface authentication and any enforced multi-factor authentication controls.	8.1	More Details
CVE-2026-58177	The Apache Traffic Server Cripts framework has out-of-bounds writes, path traversal, and use-after-free errors. This issue affects Apache Traffic Server: from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 10.1.4, which fix the issue.	8.1	More Details
CVE-2026-20465	In wlan AP driver, there is a possible out of bounds write due to a missing bounds check. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00489200; Issue ID: MSV-7834.	8.1	More Details
CVE-2026-17995	Out of bounds read in Dawn in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Low)	8.1	More Details
CVE-2026-66318	Origin validation error in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	8.1	More Details
CVE-2026-67345	MaxKey through 4.1.12, fixed in commit ddbb72f, contains an insufficient redirect URI validation vulnerability in DefaultRedirectResolver.hostMatches() that allows remote attackers to hijack OAuth 2.0 authorization codes by supplying a crafted redirect_uri whose hostname suffix matches a registered URI without proper dot-boundary anchoring. Attackers who control a domain ending with the registered redirect URI hostname can social-engineer victims into clicking a crafted authorization URL, causing the authorization code to be issued to the attacker-controlled URI and exchanged for an access token granting access to the victim's identity.	8.1	More Details
CVE-2026-67610	OpenEMR through 8.2.0 contains an improper authentication vulnerability in the OAuth2 dynamic client registration endpoint that allows unauthenticated attackers to register a malicious client with system-level FHIR scopes by supplying a self-generated RSA keypair via the jwks field. Once an administrator approves the registered client, attackers can use the client_credentials grant with a self-signed JWT assertion to obtain access tokens granting read access to all FHIR resources across all patients in the system.	8.1	More Details
CVE-2026-18577	An incomplete patch for CVE-2026-18556 allows for authentication bypass and account takeover in N-central Versions through 2026.3.1	8.1	More Details
CVE-2026-12695	The miniOrange 2FA WordPress plugin before 6.2.6 does not validate the submitted one-time password against the targeted user's stored secret, instead verifying it against an attacker-supplied value, allowing an unauthenticated attacker who knows a victim's password to bypass two-factor authentication and gain access to the victim's account, including administrators.	8.1	More Details
CVE-2026-16539	The sm page duplicator WordPress plugin through 1.0.0 does not sanitise and escape a stored value before using it in a SQL statement when duplicating a page, allowing users with the Editor role and above to perform SQL Injection attacks.	8.1	More Details
CVE-2026-63231	A post-authentication SQL injection vulnerability in Koollab LMS allowed an authenticated attacker to use an error-based SQL oracle via the face-to-face runs update endpoint to read the entire application database and obtain valid JWT tokens for account takeover.	8.1	More Details

CVE-2026-68581	Vikunja versions 0.22.0 through 2.3.0 fail to validate the principal type in API token management. Because user IDs and link-share IDs are independent numeric sequences and both resolve through a generic web.Auth.GetID() interface, a link-share JWT whose numeric ID equals a target user's ID is treated as that user by the /api/v1/tokens endpoints. An authenticated attacker can obtain a target's numeric user ID via authenticated user search, then create link shares on an attacker-writable project until the link-share sequence reaches that value, and use the resulting link-share JWT to list, create, and delete the target user's API tokens (including issuing a new token with attacker-chosen scopes under the target's permissions). Fixed in version 2.4.0.	8.1	More Details
CVE-2026-56428	The SSH service on BSH ELP (Electronic Platform) modules contains a platform-specific vulnerability due to an improperly secured default configuration. An insecure, non-revocable SSH public key is included in the firmware's authorized_keys file for the root user. An attacker in possession of the corresponding private key could leverage it to bypass authentication and gain root-level access to the appliance.	8.1	More Details
CVE-2026-17686	Insufficient validation of untrusted input in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	8.1	More Details
CVE-2026-67328	@better-auth/sso versions before 1.6.21 contain multiple authentication bypass vulnerabilities in SSO provider handling that allow attackers to sign in as arbitrary users. Attackers can exploit domain verification parsing mismatches, orphaned provider accounts, unbound SAML assertions, or reflected XSS on logout endpoints to gain unauthorized session access and account takeover.	8.1	More Details
CVE-2026-18830	Insufficient input validation in Amazon Bedrock AgentCore harness might allow an authenticated remote user to execute configured tools bypassing model invocation and security controls via crafted content blocks in conversation messages. AWS has addressed this issue. No customer action is required.	8.1	More Details
CVE-2026-24079	Cryptographic Issue while processing registration requests with malformed or missing authentication parameters.	8.1	More Details
CVE-2026-12586	The Lenxel WP WordPress theme through 1.0.31 does not perform any authorization or ownership check on its password-reset action, validating only a CSRF nonce, allowing unauthenticated attackers to reset the password of any user (including an administrator) and take over the account.	8.1	More Details
CVE-2026-15450	The Nex Forms – Ultimate Form Builder – Lite plugin for WordPress is vulnerable to arbitrary file deletion via path traversal in versions up to, and including, 9.2.3. This is due to the delete_file() AJAX handler retrieving a file path from the database and passing it directly to unlink() with no validation (no realpath(), basename(), or allowlist check), combined with the insert_record() AJAX handler that lets the same authenticated user store an arbitrary value in the target 'location' column (wp_kses() only strips HTML tags and does not neutralize path traversal or absolute paths). This makes it possible for authenticated attackers, with admin-level access and above, to delete arbitrary files on the affected site's server, including wp-config. When the plugin's user-level option is configured to something else, this may be exploitable with lower privileges.	8.1	More Details
CVE-2026-70482	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.8.0 until 0.11.0, when ENABLE_OAUTH_TOKEN_EXCHANGE=True, /oauth/{provider}/token/exchange accepts a raw provider access token and validates it by calling the provider userinfo endpoint without confirming which OAuth client the token was issued to. Anyone holding an access token minted for any client registered with the same provider could exchange it for an Open WebUI session as that token user, including applications the operator does not control and has never authorized. This issue is fixed in 0.11.0.	8.1	More Details
CVE-2026-18187	A format string vulnerability was found in the Internal Backup on the ADM. The vulnerability occurs because user-controlled task input may be included in an error response and processed through an unsafe format string operation. An authenticated attacker can exploit this issue to disclose memory information or cause denial of service of the affected CGI process. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.RUN1 as well as from ADM 5.0.0 through ADM 5.1.3.RI81.	8.1	More Details
CVE-2026-53510	Savon is a Ruby SOAP client. From 0.9.8 until 2.17.2, Savon::Model .all_operations interpolates attacker-controlled WSDL operation names into Ruby source passed to module_eval, allowing Ruby code execution in the application process. This issue is fixed in version 2.17.2.	8.1	More Details

CVE-2026-69088	Grav CMS versions 2.0.7 through 2.0.10 fail to validate fully-qualified static method calls (Class::method) in blueprint dynamic-field directives because Blueprint::isSafeDynamicCall() only applies its dangerous-callable denylist to strings that do not contain '::'. An account with only page-editing rights (admin.pages, not super-admin or admin.pages_twig) can plant a directive in a page's form-field frontmatter that invokes an arbitrary public static PHP method with attacker-controlled arguments. Using built-in gadget methods this allows reading of any server-readable file (disclosed to anonymous visitors of the crafted page) and arbitrary creation/copying of files and directories under the web-server account. Fixed in 2.0.11.	8.1	More Details
CVE-2026-18188	A format string vulnerability was found in the Rsync Backup on the ADM. The vulnerability occurs because user-controlled rsync backup configuration or log data may be processed through an unsafe format string operation. An authenticated attacker can exploit this issue to disclose memory information or cause denial of service of the affected backup component. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.RUN1 as well as from ADM 5.0.0 through ADM 5.1.3.RI81.	8.1	More Details
CVE-2026-17869	Out of bounds read in WebXR in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	8.1	More Details
CVE-2026-67192	Xlight FTP Server before 3.9.5 contains a pre-authentication stack buffer overflow vulnerability that allows unauthenticated attackers to corrupt stack memory by sending malformed SSH packets when a GCM cipher is negotiated. Attackers can craft packets with an unvalidated length field passed directly to the GCM decrypt function, overwriting the stack cookie and return address to potentially achieve remote code execution before any authentication occurs.	8.1	More Details
CVE-2026-18186	A stored format string vulnerability was found in the FTP Backup on the ADM. The vulnerability occurs because user-controlled backup configuration data may be written into a task log and later processed through an unsafe format string operation. An authenticated attacker can exploit this issue to disclose memory information or cause denial of service of the affected CGI process. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.RUN1 as well as from ADM 5.0.0 through ADM 5.1.3.RI81.	8.1	More Details
CVE-2026-16144	The Kali Forms — Contact Form & Drag-and-Drop Builder plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.4.20 via the _save_data function. This is due to insufficient validation of the 'thisPermalink' field value before it overwrites a trusted callable placeholder, allowing attacker-controlled strings to reach call_user_func() in _save_data(). This makes it possible for unauthenticated attackers to execute code on the server. Exploitation requires the target form to define a field with a name matching one of the reserved placeholder keys ('thisPermalink', 'entryCounter', or 'submission_link'), as check_if_placeholders_changed() only processes POST keys present in the form's field_type_map.	8.1	More Details
CVE-2026-63035	A heap use-after-free vulnerability in the TransferSubscriptions service in open62541 may allow an authenticated attacker to cause a denial of service or potentially execute arbitrary code.	8.1	More Details
CVE-2026-67595	VaahCMS versions 2.0.0 through 2.3.4 contain a malicious obfuscated JavaScript payload embedded in the Blade template responsible for rendering security OTP emails, allowing remote attackers to execute unauthorized code in any browser that renders the affected email template with JavaScript enabled. The payload establishes a WebSocket connection to a hardcoded command-and-control endpoint, installs a password-field keylogger using MutationObserver to capture dynamically added inputs, scrapes WhatsApp Web DOM content, and accepts remote commands to redirect or overwrite the rendered page.	8.1	More Details
CVE-2026-65313	A provisioning script used when installing HIPASE-250 (formerly 250 SCALA) engineering workstations sets a fixed, hard-coded x11vnc password. Because the same credential is applied to every workstation provisioned this way, an attacker with adjacent-network access who knows the password can gain VNC access to affected workstations.	8.1	More Details
CVE-2025-15672	The ChamaWP WordPress plugin before 1.0.13 does not properly validate user input before passing it to a PHP deserialization function, allowing unauthenticated attackers to inject arbitrary PHP objects, which could lead to remote code execution when a suitable gadget chain is present via other installed code.	8.1	More Details
CVE-	The security fix for CVE-2025-66518 is incomplete. Any client who can access to Apache Kyuubi Server via Kyuubi frontend protocols can bypass server-side		

2026-62391	config kyuubi.session.local.dir.allowlist via unprefixed Spark config aliases. This issue affects Apache Kyuubi: from 1.6.0 before 1.12.0. Users are recommended to upgrade to version 1.12.0, which fixes the issue.	8.1	More Details
CVE-2026-13444	IBM Langflow OSS 1.0.0 through 1.10.1 can allow an attacker to access another user's private vector documents by creating their own flow with matching Chroma persist_directory and collection_name values. The attacker receives exact victim content in their workflow output despite having no authorization to read the victim's flow. Additionally, the attacker can pollute the victim's collection by inserting their own documents into the shared namespace.	8.1	More Details
CVE-2026-70494	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.10.0 until 0.11.0, the DELETE /api/v1/folders/{id} handler in backend/open_webui/routers/folders.py allowed a user granted write access to a shared chat folder to permanently delete chats and messages belonging to the folder owner. The cascade following the authorization check is bound to the folder owner's id, but the subfolder check accepted any inherited write grant instead of requiring ownership or administrator status. A collaborator can destroy the owner's subtree or force-move chats out of it when delete_contents=false. This issue is fixed in 0.11.0.	8.1	More Details
CVE-2026-67245	A path traversal vulnerability was found in the VPN Clients on the ADM. The vulnerability occurs because user-controlled certificate name input is not sufficiently validated before being used to construct the upload destination path. An authenticated attacker can exploit this issue to write an uploaded certificate file outside the intended VPN certificate directory, subject to process privileges and filesystem permissions. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.RUN1 as well as from ADM 5.0.0 through ADM 5.1.3.RI81.	8.1	More Details
CVE-2026-14300	The miniOrange Social Login and Register (Discord, Google, Twitter, LinkedIn) WordPress plugin before 7.8.0 does not bind the one-time code used by its optional email-verification (Profile Completion) feature to the account it was issued for, allowing unauthenticated attackers to obtain a valid session for any account, including administrators, by requesting a code for an email address they control and replaying it against the victim's email address. Exploitation requires the Profile Completion feature to be enabled and social login to be configured.	8.1	More Details
CVE-2026-15258	The Product Feed Manager For WooCommerce WordPress plugin before 7.6.1 does not properly sanitise and escape product-feed custom filter rules before using them in a SQL query, allowing users with the Contributor role and above to perform SQL injection attacks.	8.1	More Details
CVE-2026-12703	TeamViewer Full Client and Host for macOS before version 15.80 contain a business logic error that can allow an authenticated attacker to bypass a configured 2FA for Connections approval flow via Unattended Access and establish a remote connection to an affected macOS host.	8.0	More Details
CVE-2026-16623	The Create Block WordPress plugin before 2.10.0 does not correctly escape user-supplied text before writing it into a generated PHP pattern file, allowing a multisite subsite administrator (who holds the capability gating this action but is denied the capability that normally gates PHP file editing) to inject and execute arbitrary PHP code on the server.	8.0	More Details
CVE-2026-47858	Starting Spring Boot applications in the Spring Tools with the live information mode enabled makes the running application vulnerable against JMX-based remote code execution. Affected Spring Products and Versions: Spring Tools for Eclipse: 5.2.0 and earlier Spring Tools for VSCode / Cursor / Theia: 2.2.0 and earlier	8.0	More Details
CVE-2026-18599	A flaw has been found in GL.iNet GL-MT3000 up to 4.4.5. The impacted element is the function logread.set_config of the file /usr/lib/oui-httpd/rpc/logread of the component Logread Lua RPC Plugin. This manipulation of the argument record_size causes command injection. The exploit has been published and may be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	8.0	More Details
CVE-2026-47873	The Boot Dashboard Docker integration in Spring Tools publishes container control ports on all of the host's network interfaces (0.0.0.0) rather than restricting them to loopback. Affected Spring Products and Versions: Spring Tools for Eclipse: 5.2.0 and earlier	8.0	More Details
CVE-2026-18642	Deserialization of untrusted data vulnerability in TUBITAK BILGEM Software Technologies Research Institute eta-otp-lock allows Object Injection. This issue affects eta-otp-lock: before 1.0.4.	7.8	More Details
CVE-2026-44106	A privilege escalation vulnerability in the init-script for user-applications allows a low-privileged local user to execute arbitrary commands as root, resulting in full system compromise.	7.8	More Details

CVE-2026-17864	Inappropriate implementation in Updater in Google Chrome on Mac prior to 151.0.7922.72 allowed a local attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: Medium)	7.8	More Details
CVE-2026-17863	Inappropriate implementation in Browser in Google Chrome on Windows prior to 151.0.7922.72 allowed a local attacker to perform privilege escalation via a malicious file. (Chromium security severity: Medium)	7.8	More Details
CVE-2026-17862	Use after free in Tracing in Google Chrome on Windows prior to 151.0.7922.72 allowed a local attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: Medium)	7.8	More Details
CVE-2026-17861	Insufficient validation of untrusted input in Updater in Google Chrome prior to 151.0.7922.72 allowed a local attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: Medium)	7.8	More Details
CVE-2026-17654	Race in Updater in Google Chrome on Mac prior to 151.0.7922.72 allowed a local attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: Critical)	7.8	More Details
CVE-2026-44099	A privilege escalation vulnerability in the system configuration allows a low-privileged local user to execute arbitrary commands as root, resulting in full system compromise.	7.8	More Details
CVE-2026-18606	A weakness has been identified in Razer RzUpdateService 1.10.14.0. Affected by this vulnerability is an unknown functionality of the file C:\Program Files (x86)\Razer\RzUpdateEngineService\RzUpdateService.exe of the component Named Pipe Handler. Executing a manipulation of the argument lpThreadParameter can lead to improper privilege management. The attack requires local access. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure.	7.8	More Details
CVE-2026-18657	An uncontrolled search path element in Kiro CLI before version 2.10.0 on Windows might allow a remote unauthenticated actor to execute arbitrary code via a maliciously crafted project directory containing an executable that bypasses workspace trust protections when a local user starts Kiro CLI in the directory. To remediate this issue, users should upgrade to version 2.10.0 or higher.	7.8	More Details
CVE-2026-18157	A flaw was found in yggdrasil-worker-package-manager. A local attacker with existing access to the system could exploit an argument injection vulnerability in the APT backend. This allows specially crafted package names, which begin with a hyphen, to be misinterpreted as command options by apt-get. Successful exploitation could lead to remote code execution (RCE) with root privileges, enabling the attacker to fully compromise the system's integrity, confidentiality, and availability.	7.8	More Details
CVE-2026-18220	An out-of-bounds write vulnerability was found in the BFD library's DLX ELF backend (bfd/elf32-dlx.c) in GNU binutils. The dlx_rtype_to_howto() function maps ELF relocation types to internal howto structures but fails to perform adequate bounds checking on attacker-controlled relocation type values (via ELF32_R_TYPE(r_info)) before indexing into the dlx_elf_howto_table[] array. The DLX relocation type number space is non-contiguous (basic types 0-6, extended types at 0x10000+), but the default case in the switch statement allows arbitrary index values to reach the array access. A specially crafted ELF/DLX object file can trigger this out-of-bounds write when processed by any BFD-consuming tool (objdump, readelf, strip, ld, nm, objcopy). The vulnerability has been demonstrated to achieve arbitrary code execution via a File Stream Oriented Programming (FSOP) attack against glibc FILE structures (stderr), redirecting control flow to system(). Attack scenarios include CI/CD pipelines performing automated binary analysis, developer workstations running objdump/readelf on untrusted binaries, automated security scanning or malware analysis tools invoking binutils, and package build systems processing third-party code. Note: This vulnerability is only exploitable when binutils is built with the DLX backend enabled (typically via --enable-targets=all).	7.8	More Details
CVE-2026-24083	Memory Corruption while processing IOCTL device driver requests with invalid arguments.	7.8	More Details
CVE-2026-24080	Memory Corruption when handling malformed request parameters in the fingerprint TA.	7.8	More Details

CVE-2026-21366	Memory corruption while processing a packet with a size close to the maximum allowed value.	7.8	More Details
CVE-2026-16524	A command injection flaw in PCP's linux_sockets PMDA allows malicious shell metacharacters via the network.persocket.filter metric. This failed validation lets attackers execute arbitrary commands as the PMDA user when metrics refresh.	7.8	More Details
CVE-2026-10710	A maliciously crafted FBX file, when parsed through Autodesk FBX SDK, can trigger a stack-based buffer overflow vulnerability in fbxsdk::ExtractDrive. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2026-10709	A maliciously crafted FBX file, when parsed through Autodesk FBX SDK, can trigger a stack-based buffer overflow vulnerability in fbxsdk::FbxIO::BinaryReadSectionHeader. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2026-16463	A maliciously crafted DXF file, when parsed through Autodesk AutoCAD, can force a Heap-Based Overflow vulnerability. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2026-64558	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Check length in pkey_pckmo handler implementation Explicitly check the length of the target buffer in the pkey_pckmo implementation of the key_to_protkey() handler function. The handler function fails, if the generated output data exceeds the length of the provided target buffer.	7.8	More Details
CVE-2026-64559	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Check length in PKEY_VERIFYPROTK ioctl Explicitly check the buffer length request structure provided by user-space and fail, if it exceeds the buffer size.	7.8	More Details
CVE-2026-64560	In the Linux kernel, the following vulnerability has been resolved: posix-cpu-timers: Prevent UAF caused by non-leader exec() race Wongi and Jungwoo decoded and reported a non-leader exec() related race which can result in an UAF: sys_timer_delete() exec() posix_cpu_timer_del() // Observes old leader p = pid_task(pid, pid_type); de_thread() switch_leader(); release_task(old_leader) __exit_signal(old_leader) sighand = lock(old_leader, sighand); posix_cpu_timers*_exit(); sighand = lock_task_sighand(p) unhash_task(old_leader); sh = lock(p, sighand) old_leader->sighand = NULL; unlock(sighand); (p->sighand == NULL) unlock(sh) return NULL; // Returns without action if(!sighand) return 0; free_posix_timer(); This is "harmless" unless the deleted timer was armed and enqueued in p->signal because on exec() a TGID targeted timer is inherited. As sys_timer_delete() freed the underlying posix timer object run_posix_cpu_timers() or any timerqueue related add/delete operations on other timers will access the freed object's timerqueue node, which results in an UAF. There is a similar problem vs. posix_cpu_timer_set(). For regular posix timers it just transiently returns -ESRCH to user space, but for the use case in do_cpu_nanosleep() it's the same UAF just that the k_itimer is allocated on the stack. Also posix_cpu_timer_rearm() fails to rearm the timer, which means it stops to expire. While debating solutions Frederic pointed out another problem: posix_cpu_timer_del(tmr) __exit_signal(p) posix_cpu_timers*_exit(p); unhash_task(p); p->sighand = NULL; sh = lock_task_sighand(p) sighand = p->sighand; if (!sighand) return NULL; lock(sighand); if (!sh) WARN_ON_ONCE(timer_queued(tmr)); On weakly ordered architectures it is not guaranteed that posix_cpu_timer_del() will observe the stores in posix_cpu_timers*_exit() when p->sighand is observed as NULL, which means the WARN() can be a false positive. Solve these issues by: 1) Changing the store in __exit_signal() to smp_store_release(). 2) Adding a smp_acquire__after_ctrl_dep() into the !sighand path of lock_task_sighand(). 3) Creating a helper function for looking up the task and locking sighand which does not return when sighand == NULL. Instead it retries the task lookup and only if that fails it gives up. 4) Using that helper in the three affected functions. #1/#2 ensures that the reader side which observes sighand == NULL also observes all preceeding stores, i.e. the stores in posix_cpu_timers*_exit() and the ones in unhash_task(). #3 ensures that the above described non-leader exec() situation is handled gracefully. When the task lookup returns the old leader, but sighand == NULL then it retries. In the non-leader exec() case the subsequent task lookup will observe the new leader due to #1/#2. In normal exit() scenarios the subsequent lookup fails. When the task lookup fails, the function also checks whether the timer is still enqueued and issues a warning if that's the case. Unfortunately there is nothing which can be done about it, but as the task is already not longer visible the timer should not be accessed anymore. This check also requires memory ordering, which is not provided when the first lookup fails. To achieve that the check is preceeded by a smp_rmb() which pairs with the smp_wmb() in write_seqlock() in __exit_signal(). That ensures that the stores in posix_cpu_timers*_exit() are visible. The history of the non-leader exec() issue goes	7.8	More Details

	back to the early days of posix CPU timers, which stored a pointer to the group leader task in the timer. That obviously fails when a non-leader exec() switches the leader. commit e0a70217107e ("posix-cpu-timers: workaround to suppress the problems with mt exec") added a temporary workaround for that in 2010 which surv ---truncated---		
CVE-2026-41447	FirmaCheck for Windows before 1.3.16 contains a dll hijacking vulnerability that allows local attackers to execute arbitrary code by placing a crafted openssl.cnf file in the unvalidated C:\Program Files (x86)\Common Files\SSL\ directory path. Attackers can write a malicious OpenSSL configuration file referencing an attacker-controlled DLL to achieve code execution at startup process privilege level when FirmaCheck.exe runs automatically at system startup.	7.8	More Details
CVE-2026-44093	A local privilege escalation vulnerability in the init-script for user-applications allows a low-privileged local user to execute arbitrary commands as root, resulting in full system compromise.	7.8	More Details
CVE-2026-67609	Telenia Software TVox 26.5.3 and prior 26.x versions, and 24.9.21 and prior 24.x versions, contain a privilege escalation vulnerability that allows attackers with access to the apache account to execute arbitrary commands as root by exploiting an insecure sudoers configuration in /etc/sudoers.d/telenia. The configuration grants the apache user NOPASSWD execution of /bin/nice, which can be leveraged to invoke arbitrary commands, enabling full root-level command execution without supplying a password.	7.8	More Details
CVE-2026-64556	In the Linux kernel, the following vulnerability has been resolved: perf/core: Detach event groups during remove_on_exec perf_event_remove_on_exec() removes events by calling perf_event_exit_event(). For top-level events, this removes the event from the context with DETACH_EXIT only. This can leave inconsistent group state when a removed event is a group leader and the group contains siblings without remove_on_exec. If the group was active, the surviving siblings can remain active and attached to the removed leader's sibling list, but are no longer represented by a valid group leader on the PMU context active lists. A later close of the removed leader uses DETACH_GROUP and can promote the still-active siblings from this stale group state. The next schedule-in can then add an already-linked active_list entry again, corrupting the PMU context active list. With DEBUG_LIST enabled, this is caught as a list_add double-add in merge_sched_in(). Fix this by detaching group relationships when remove_on_exec removes an event. This preserves the existing task-exit and revoke behavior, while ensuring surviving siblings are ungrouped before the removed event leaves the context.	7.8	More Details
CVE-2026-59913	Dell Display and Peripheral Manager (DDPM Mac), versions prior to 2.3.0.1005, contain a Missing Authentication for Critical Function vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.8	More Details
CVE-2026-59912	Dell Display and Peripheral Manager (DDPM Mac), versions prior to 2.3.0.1005, contain an Improper Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges and arbitrary code execution.	7.8	More Details
CVE-2026-44095	A privilege escalation vulnerability in a script used for network configuration allows a low-privileged local user to execute arbitrary commands as root, resulting in full system compromise.	7.8	More Details
CVE-2026-18656	An uncontrolled search path element in Kiro IDE before version 1.0.228 on Windows might allow a remote unauthenticated actor to execute arbitrary code via a maliciously crafted project directory containing an executable that bypasses workspace trust protections when a local user opens the directory. To remediate this issue, users should upgrade to version 1.0.228 or higher.	7.8	More Details
CVE-2026-34641	Premiere Pro is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-44096	A privilege escalation vulnerability in udhcpc allows a local user "charx-web" to execute arbitrary commands as root, resulting in full system compromise.	7.8	More Details
CVE-2026-20483	In Telephony, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS11087526; Issue ID: MSV-8243.	7.7	More Details
CVE-2026-	External control of file name or path in Microsoft Edge for Android allows an unauthorized attacker	7.7	More

66310	to disclose information locally.		Details
CVE-2026-70479	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.6 until 0.11.0, with WEB_LOADER_ENGINE=playwright, the Playwright web loader validates only the top-level page request and lets sub-resource requests pass unvalidated. A page supplied by an authenticated user can use JavaScript to reach blocked internal addresses, and returned DOM can include data read from those addresses in web-search or RAG output. This issue is fixed in 0.11.0.	7.7	More Details
CVE-2026-69086	SiYuan versions before v3.7.3 fail to validate the avID parameter on all code branches in attribute-view read endpoints, allowing attackers to construct traversal paths that escape the storage directory. Authenticated users with RoleReader permissions or anonymous clients when publish authentication is disabled can read JSON files outside the attribute-view directory to disclose cross-scope database content.	7.7	More Details
CVE-2026-41703	VMware ESX, Workstation, and Fusion contain an out-of-bounds read vulnerability. A malicious actor with VM deployment privileges could trigger an out-of-bounds read, potentially leading to information disclosure or more likely a Denial-of-Service (DoS) condition of the host process. On Workstation and Fusion, the impact of this vulnerability is restricted to information disclosure.	7.6	More Details
CVE-2026-16969	The IRIS web application in version 2.4.26 and possibly others is vulnerable to stored cross-site scripting (XSS) in the assets function.	7.6	More Details
CVE-2026-67352	luci-app-https-dns-proxy contains a stored cross-site scripting vulnerability in the resolver_url parameter that allows authenticated users to inject active HTML. When an administrator views the HTTPS DNS Proxy status page, the resolver URL is rendered as raw HTML and executes JavaScript in the administrator's browser origin.	7.6	More Details
CVE-2026-18361	The IRIS web application in version 2.4.26 and possibly others is vulnerable to stored cross-site scripting (XSS) in the datastore upload function.	7.6	More Details
CVE-2026-10685	The Zephyr Bluetooth GATT client CCC-write response handler gatt_write_ccc_rsp() in subsys/bluetooth/host/gatt.c invoked the application's params->subscribe() callback after it had already called params->notify(conn, params, NULL, 0). Per the public GATT API, a notify callback with NULL data is the documented signal that the subscription has terminated and the bt_gatt_subscribe_params struct may be freed or reused by the application; calling subscribe() on the struct afterwards is a use-after-free, including an indirect call through the freed params->subscribe function pointer. The error branch is remotely (adjacent) reachable: a Zephyr device acting as a GATT client that calls bt_gatt_subscribe() can be driven into this ordering when a connected GATT server peer answers the CCC write with an ATT Error Response (the peer-supplied error code flows through att_error_rsp -> att_handle_rsp into gatt_write_ccc_rsp). For applications that free or recycle subscription parameters in their notification-termination handler, this results in memory corruption, a crash (denial of service), or potentially attacker-influenced control flow. The fix reorders the handler so the subscribe() callback runs before the terminating notify(NULL) in both the error and unsubscribe paths.	7.6	More Details
CVE-2026-18381	A flaw was found in the koku-metrics-operator for Red Hat OpenShift. The operator's CostManagementMetricsConfig custom resource allows a user able to edit the CR to specify an arbitrary upload URL. The operator attaches its own Kubernetes service-account bearer token to queries sent to this user-controlled URL, allowing the attacker to obtain the token.	7.6	More Details
CVE-2026-18378	A flaw was found in koku-metrics-operator. The operator's CostManagementMetricsConfig custom resource allows user able to edit the CR to specify an arbitrary upload URL. When authentication.type is set to token (the default), the cluster-global Red Hat Cloud pull-secret bearer token is attached to HTTP requests sent to this user-controlled URL, allowing the attacker to obtain the token.	7.6	More Details
CVE-2026-67527	OpenProject is open-source, web-based project management software. Prior to 17.6.0, PATCH /api/v3/work_packages/{id} accepted _links.fileLinks and allowed authenticated users with edit_work_packages but without manage_file_links to resolve Storages::FileLink records by raw id, detach or hard-delete existing FileLinks, and re-parent FileLinks from other projects to an attacker-controlled work package, exposing origin filename, origin id, and MIME type metadata. This issue is fixed in 17.6.0.	7.6	More Details
CVE-	Memory Corruption when processing untrusted user input in the fastboot command handler for		More

2026-25292	audio framework configuration.	7.6	Details
CVE-2026-18360	The IRIS web application in version 2.4.26 and possibly others is vulnerable to stored cross-site scripting (XSS) in the custom attributes function.	7.6	More Details
CVE-2026-67304	FreeRDP before 3.29.0 contains a null pointer dereference vulnerability in smartcard device control request cleanup when reader-state decoding fails. Attackers can send malformed smartcard IRP requests with non-zero cReaders and truncated reader-state data to crash the process via null pointer access in free_reader_states functions.	7.5	More Details
CVE-2026-67300	FreeRDP before 3.29.0 contains client-side heap use-after-free vulnerabilities in the async update message proxy for RAIL WINDOW_STATE_ORDER and NOTIFY_ICON_STATE_ORDER when AsyncUpdate is enabled. When a malicious or compromised RDP server sends crafted update orders, the message proxy shallow-copies structures containing nested parser-owned pointers (e.g., titleInfo.string, windowRects, visibilityRects, icon buffers). The parser frees those nested buffers after the callback returns, so the queued async message later dispatches stale pointers, potentially causing memory corruption or a client crash.	7.5	More Details
CVE-2026-67322	GitPython before 3.1.52 is vulnerable to environment-variable exfiltration in Repo.clone_from(). The caller-supplied remote URL is passed through Git.polish_url(), which on non-Cygwin platforms calls os.path.expandvars() on the URL before invoking git clone. An attacker who controls the clone URL can embed $NAME or ${NAME} tokens that are expanded to the values of the hosting process's environment variables (e.g., AWS_SECRET_ACCESS_KEY or GITHUB_TOKEN). The resulting URL, now containing the secret, is transmitted over the network to an attacker-controlled host during the clone attempt, disclosing the secret.	7.5	More Details
CVE-2026-67301	FreeRDP before 3.29.0 contains out-of-bounds read vulnerabilities in the async update message proxy for the PolygonSC and PolygonCB primary drawing orders. When AsyncUpdate is enabled (e.g., xfreerdp /async-update), update_message_PolygonSC() and update_message_PolygonCB() allocate a fresh points array but copy point data from the address of the order structure instead of from polygonSC->points / polygonCB->points, resulting in a client-side out-of-bounds read. A malicious or compromised RDP server sending crafted PolygonSC/PolygonCB update orders can trigger memory disclosure or a client crash.	7.5	More Details
CVE-2026-53503	Thumbor is an open-source photo thumbnail service by globo.com. Prior to 7.8.0, Thumbor's filters:convolution(<matrix>, <columns>, <should_normalize>) filter passes the user-controlled <columns> value to a C extension (thumbor/ext/filters/_convolution.c) where it is used as a divisor (for % and /) without validating columns > 0. When columns=0, the C code triggers undefined behavior; on x86_64 this reliably results in a fatal divide-by-zero trap (SIGFPE) and crashes the Thumbor process, causing a remote denial of service. This issue is fixed in 7.8.0.	7.5	More Details
CVE-2026-15006	The Bit integrations – Form Integration, Webhook, Spreadsheets, CRM, LMS & Email Automation plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.9.0 via the processAttachment function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.	7.5	More Details
CVE-2026-67298	FreeRDP versions 3.28.0 and earlier contain a heap buffer overflow in the server-side RAIL channel handler (rail_server_handle_messages() in channels/rail/server/rail_main.c). When processing a RAIL PDU header, the code subtracts RAIL_PDU_HEADER_LENGTH from the peer-controlled orderLength field without first verifying orderLength is at least the header length. For orderLength values 0..3 this causes an unsigned integer underflow to a very large size, which bypasses the Stream_EnsureRemainingCapacity() capacity check (due to pointer arithmetic wraparound) and is then passed to WTSVirtualChannelRead(), resulting in an out-of-bounds heap write. A malicious or compromised RDP client can exploit this to corrupt the heap and crash the server. Fixed in FreeRDP 3.29.0.	7.5	More Details
CVE-2026-67299	FreeRDP before 3.29.0 contains a client-side heap use-after-free in the async update message proxy for WINDOW_ICON_ORDER when AsyncUpdate is enabled (e.g. xfreerdp /async-update). In update_message_WindowIcon() a shallow CopyMemory() overwrites a freshly allocated lParam->iconInfo with the parser-owned windowIcon->iconInfo pointer. After the parser callback returns, update_recv_window_info_order() frees window_icon.iconInfo, but the queued async message still retains and later dispatches that stale pointer. A malicious or compromised RDP server sending a crafted RAIL Window Alternate Secondary Order with WINDOW_ORDER_ICON can trigger use-after-free, leading to memory corruption and client crash.	7.5	More Details

CVE-2026-53599	REDAXO is a PHP-based content management system. From 5.18.2 until 5.21.1, rex_mediapool::isAllowedExtension in redaxo/src/addons/mediapool/lib/mediapool.php lets an authenticated backend user with media[upload] permission upload a JPEG/PHP polyglot named shell.php.any.jpg, which web servers with multi-extension PHP handlers can execute as the web-server user. This issue is fixed in version 5.21.1.	7.5	More Details
CVE-2026-53504	Thumbor is an open-source photo thumbnail service by globo.com. Prior to 7.8.0, the convolution filter regular expression performs exponential backtracking on crafted repeated numeric input, allowing a URL request to exhaust processing time. This issue is fixed in 7.8.0.	7.5	More Details
CVE-2026-67297	FreeRDP before 3.29.0 fails to enforce the RESPONSE_SIZE_LIMIT when processing Transfer-Encoding: chunked HTTP responses in http_response_recv_body(). Attackers controlling a malicious RD Gateway endpoint can send oversized chunked response bodies to exhaust client memory resources without triggering the configured size limit.	7.5	More Details
CVE-2026-16529	A signed integer overflow in the PCP __pmGetPDU() function can be exploited via crafted network packets during PDU processing or SASL negotiation. This permanently blinds the affected daemon, resulting in a total denial of service (DoS) for subsequent packet reads.	7.5	More Details
CVE-2026-53505	Thumbor is an open-source photo thumbnail service by globo.com. Prior to 7.8.0, Thumbor's filters:proportion(<value>) filter does not enforce an upper bound on <value> and runs in the post-transform phase. An attacker can trigger extremely large resizes (CPU/memory exhaustion) and cause denial of service. This issue is fixed in 7.8.0.	7.5	More Details
CVE-2026-67296	FreeRDP before 3.29.0 contains a denial of service vulnerability in the RDPEI server channel handler that fails to validate maximum PDU body length before stream allocation. A malicious RDP client can send a header-only RDPEI message with a large declared body length to force excessive memory allocation on the server.	7.5	More Details
CVE-2026-62999	Copier is a library and CLI app for rendering project templates. From 9.5.0 through 9.16.0, percent-encoded parent-directory segments or encoded path separators in a template URL can match a configured trusted repository prefix before an HTTP server or Git transport decodes the path, allowing unsafe template features from a repository outside the trusted prefix to run after user interaction. This issue is fixed in version 9.17.0.	7.5	More Details
CVE-2026-67290	FreeRDP before 3.29.0 contains a heap out-of-bounds read vulnerability in the TSMF FFmpeg decoder when parsing AVC1 MPEG2VIDEOINFO media types with insufficient ExtraData. Attackers can send malformed media format data from a server to trigger a crash by reading fixed offsets without validating source buffer length.	7.5	More Details
CVE-2026-67288	FreeRDP before 3.29.0 contains a null pointer dereference vulnerability in smartcard cache request decoders that accept NULL NDR pointers for LookupName in SCARD_IOCTL_READCACHEA and SCARD_IOCTL_WRITECACHEA operations. When smartcard emulation is enabled, attackers can send crafted smartcard cache requests with NULL lookup-name pointers to trigger strlen() on a null pointer, causing client process termination.	7.5	More Details
CVE-2026-18536	Data::Entropy versions before 0.010 for Perl read remote entropy sources over plain HTTP. The Data::Entropy::RawSource::RandomOrg and Data::Entropy::RawSource::RandomnumbersInfo remote sources are accessed over plain HTTP. The Data::Entropy::RawSource::RandomOrg integrity check trivially matches any non-empty byte string. Any on-path attacker, such as open WiFi, a compromised ISP, captive portal, or a hostile egress proxy substitutes the response and thereby chooses the bytes returned by rand_bits and rand_int for every application that selected one of these sources via with_entropy_source. The _checkbuf method response is equally attacker-controlled, so the retry/sleep behaviour is steerable too.	7.5	More Details
CVE-2026-17816	Insufficient policy enforcement in Speech in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: Medium)	7.5	More Details
CVE-2026-14839	The Mapster WP Maps WordPress plugin before 1.24.0 does not perform any authorization or post-status check on a public REST endpoint, allowing unauthenticated users to retrieve the title and full content of any post regardless of its status, including unpublished (draft, pending, private, and trashed) posts.	7.5	More Details
	FreeRDP before 3.29.0 (affected versions <= 3.28.0) contains a heap out-of-bounds read in update_process_glyph_fragments()/glyph_cache_fragment_put() in libfreerdp/cache/glyph.c. When		

CVE-2026-67291	handling a GLYPH_FRAGMENT_ADD update, the code reads a one-byte server-controlled declared fragment size but does not verify it fits within the remaining received buffer before allocating and copying that many bytes. A malicious RDP server can send a short fragment with an oversized declared size, causing the client to read beyond the allocated buffer, resulting in an out-of-bounds read and client crash.	7.5	More Details
CVE-2026-60074	Date::Manip versions through 6.99 for Perl return corrupted dates via non-ASCII decimal digits that pass the numeric range tests in check. The parse regexes capture year, month and day with the `\d` shorthand, which on a character string matches the whole Unicode decimal digit property `\p{Nd}` and not just `[0-9]`. Date::Manip::Base::check then validates the captured fields with numeric comparisons alone (`$y<1 || $y>9999`, `$m<1 || $m>12`, `$d<1 || $d>$days`), and _parse_check stores the numified fields (`$y+0`). Perl truncates a string at the first character that is not an ASCII digit, so a field whose leading characters are ASCII digits numifies to an in-range prefix and satisfies every test: a year field of three ASCII digits followed by U+0664 ARABIC-INDIC DIGIT FOUR numifies to 202, giving the year 0202, and one non-ASCII digit in the month or day field shifts those fields the same way. The hour, minute and second fields match explicit ASCII character classes (`0?[0-9]`, `[0-5][0-9]`) and do not shift, though a non-ASCII digit in a fractional hour or minute field truncates the fraction. Any caller that passes an untrusted character string to ParseDate() or Date::Manip::Date->parse() can get back a date that differs from the string it parsed, with no parse error. Where the parsed date gates logic such as an expiry check or a retention window, the shift goes unnoticed.	7.5	More Details
CVE-2026-13178	The Eventin WordPress plugin before 4.1.16 does not properly authorize order creation and accepts an attacker-supplied order status, allowing unauthenticated users to create orders marked as paid without completing any payment.	7.5	More Details
CVE-2026-17774	Insufficient validation of untrusted input in Variations in Google Chrome prior to 151.0.7922.72 allowed an attacker in a privileged network position to potentially exploit heap corruption via malicious network traffic. (Chromium security severity: Medium)	7.5	More Details
CVE-2026-63559	An integer overflow in the UA_Variant arrayDimensions product computation in open62541 may allow a remote attacker to read out-of-bounds heap memory, potentially disclosing sensitive information.	7.5	More Details
CVE-2026-18064	An incomplete fix for CVE-2026-15352 in the NASA core Flight System (cFS) Health and Safety (HS) application leaves a separate NULL pointer dereference reachable in versions through 7.0.1. An attacker who can trigger the affected command under specific conditions could cause the HS application to crash, resulting in a denial-of-service condition and processor reset.	7.5	More Details
CVE-2026-68500	Sylius Mollie Plugin provides Mollie payment integration for Sylius applications. Prior to 2.2.8, 3.2.4, and 3.3.1, Sylius Mollie Plugin's POST /{_locale}/update-payment payment webhook accepts attacker-controlled id and orderId parameters but does not verify that the Mollie payment belongs to the referenced Sylius order, allowing an unauthenticated attacker with any valid paid Mollie payment ID to mark a victim order as paid without transferring funds for that order. This issue is fixed in 2.2.8, 3.2.4, and 3.3.1.	7.5	More Details
CVE-2026-17948	Type Confusion in V8 in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code inside a sandbox via a crafted Chrome Extension. (Chromium security severity: Low)	7.5	More Details
CVE-2026-17952	Inappropriate implementation in V8 in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code inside a sandbox via a crafted Chrome Extension. (Chromium security severity: Low)	7.5	More Details
CVE-2026-61536	Banks generates meaningful LLM prompts using a simple template language. In versions prior to 2.4.3, banks parses Tool JSON objects from the rendered body of {% completion %} blocks and later resolves their import_path field through importlib.import_module(...) + getattr(...) to obtain the callable that handles a tool call. There is no allowlist or sanitization on import_path, so any importable Python attribute (e.g. os.system, subprocess.getoutput) can be selected. When the LLM emits a tool_calls entry whose function.name matches the attacker-supplied tool name, the resolved callable is invoked with kwargs decoded from tool_call.function.arguments, yielding arbitrary code execution in the banks-hosting process. This is distinct from GHSA-gphh-9q3h-jgpp / CVE-2026-44209. That advisory was fixed in 2.4.2 by switching src/banks/env.py from Environment to SandboxedEnvironment. The fix does not touch src/banks/extensions/completion.py, and the unsafe import + getattr chain still executes on 2.4.2. The malicious Tool JSON is plain text in the rendered template body — it requires no Jinja attribute access, so the sandbox is irrelevant. This issue has been fixed in version 2.4.3.	7.5	More Details

CVE-2026-18140	Uncontrolled recursion in the unknown-key skip path of the aws-smithy-json runtime crate before 0.62.7, which the smithy-rs code generator invokes from every generated struct deserializer, might allow remote unauthenticated users to cause a denial of service (process abort via stack exhaustion) via a single small HTTP request containing deeply nested JSON to a smithy-rs generated server. To remediate this issue, users should upgrade to aws-smithy-json 0.62.7 or later and rebuild.	7.5	More Details
CVE-2026-15978	SGLang contains a model weight exfiltration vulnerability when no API keys are configured, as SGLang will expose two endpoints that allow a remote attacker to trigger distributed weight broadcasting using NCCL and then triggering data transfer, attackers can exfiltrate all model weights.	7.5	More Details
CVE-2026-15977	SGLang contains a credential leakage vulnerability in the /server_info endpoint, which will return API keys and SSL keyfile information when only the --admin-api-key is configured.	7.5	More Details
CVE-2026-12942	IBM Langflow OSS 1.0.0 through 1.10.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot " sequences (/.. /) to view arbitrary files on the system.	7.5	More Details
CVE-2026-12733	IBM DataPower Gateway could allow a remote attacker to cause a denial of service due to improper resource limitations.	7.5	More Details
CVE-2026-10545	IBM Planning Analytics Local 2.1.0 through 2.1.21 is vulnerable to an open redirect that allows an attacker to redirect users to arbitrary external websites via a crafted URL. If used in SSO authentication flows, this could result in exposure of session tokens and allow attackers to hijack user sessions.	7.5	More Details
CVE-2024-25039	IBM Engineering Requirements Management DOORS and DOORS Web Access 9.7.2.1 through 9.7.2.11, and 9.6.1.1 through 9.6.1.13 do not limit the length of a connection which could allow for a Slowloris HTTP denial of service attack to take place. This can cause the web server to become unresponsive.	7.5	More Details
CVE-2026-9322	IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 are vulnerable to a denial of service via a crafted HTTP request.	7.5	More Details
CVE-2026-54365	CentreStack before 17.3 contains an unauthenticated deserialization vulnerability in GSNamespace.dll that allows unauthenticated attackers to create arbitrary local OS user accounts by supplying a crafted base64-encoded XML string to exposed API endpoints. Attackers can send a malicious StorageConfigure parameter to the jsonimportuserbyupn, jsonimportuserbyupnex, or japiimportuserbyupn endpoints to trigger InternalImportAdUserByUPN(), causing GladinetCloudMonitor.exe to invoke the NetUserAdd Windows API with attacker-controlled credentials and create arbitrary directories on the server filesystem.	7.5	More Details
CVE-2026-62663	Banks generates meaningful LLM prompts using a simple template language. In versions prior to 2.4.4, all four media filters (image, audio, video, document) in banks accept untrusted user input as file paths via Path(value) and pass them directly to open(file_path, "rb") without any path sanitization, canonicalization, or directory restriction. An attacker who controls template variables passed to a banks Prompt can use path traversal (../) to read arbitrary files accessible to the Python process—including .env files, SSH keys, cloud credentials, source code, /etc/passwd, and /etc/shadow—with the content returned base64-encoded in the rendered prompt output, making exfiltration trivial. This is particularly dangerous for applications that use banks to process user-provided template variables before sending prompts to an LLM. This issue has been fixed in version 2.4.4.	7.5	More Details
CVE-2026-17979	Race in V8 in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	7.5	More Details
CVE-2026-28814	Arbitrary Wiki Markup rendering due to lack of authentication in Apache JSPWiki up to 2.12.3 allows attacker to obtain sensitive data stored in JSPWiki variables. Users are recommended to upgrade to version 2.12.4 or 3.0.0, which fixes this issue.	7.5	More Details

CVE-2026-54366	CentreStack before 17.4 contains an XML external entity (XXE) injection vulnerability that allows unauthenticated attackers to exfiltrate arbitrary files by supplying a malicious URL to the SharePoint storage configuration handler. Attackers can send a crafted request to the unauthenticated StorageConfig endpoint causing the server to fetch and parse attacker-controlled XML containing external DTD references, resulting in out-of-band file exfiltration of sensitive files such as Web.config, which may contain database credentials and cryptographic key material.	7.5	More Details
CVE-2026-28811	Debug Messages Revealing Unnecessary Information in Apache JSPWiki up to 2.12.3. Users are recommended to upgrade to version 2.12.4, which fixes this issue.	7.5	More Details
CVE-2026-10842	IBM WebSphere Application Server 8.5, and 9.0 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 Traditional and Liberty could allow a remote attacker to bypass security constraints.	7.5	More Details
CVE-2026-67349	OpenCost before 1.121.0 fails to authenticate the GET /helmValues endpoint, exposing base64-decoded HELM_VALUES environment variable containing cloud provider credentials. Additionally, adminAuthMiddleware fails open when ADMIN_TOKEN is unset, allowing unauthenticated attackers to modify GCP service account keys via POST /serviceKey to redirect billing calls.	7.5	More Details
CVE-2026-16308	IBM Enterprise Build of Quarkus 3.27.1 through 3.27.4.SP2, and 3.33.1 through 3.33.2.SP2 Quarkus REST could allow a remote attacker to cause a denial of service due to unbounded accumulation of multipart MIME part-header bytes.	7.5	More Details
CVE-2026-57859	e107 prior to version 2.3.8 contains a code execution vulnerability in the e_array deserialization handler that allows an attacker with out-of-band database write access to execute arbitrary PHP code by storing a crafted payload in the user_prefs column. The e_array::unserialize() function in e107_handlers/core_functions.php performs only a prefix check for the string 'array' before passing the stored value to eval(), causing automatic PHP execution whenever the affected user's preferences are materialized through e_user_pref::load().	7.5	More Details
CVE-2026-14519	IBM App Connect Enterprise 13.0.1.0 through 13.0.7.2, and 12.0.1.0 through 12.0.12.27 could allow a remote attacker to read arbitrary files due to a path traversal vulnerability.	7.5	More Details
CVE-2026-12947	IBM App Connect Enterprise 13.0.1.0 through 13.0.7.2, and 12.0.1.0 through 12.0.12.27 stores potentially sensitive information in log files that could be read by a local user.	7.5	More Details
CVE-2026-11897	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 is vulnerable to a denial of service, caused by sending a specially crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources.	7.5	More Details
CVE-2026-17930	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)	7.5	More Details
CVE-2026-1360	The BuddyPress plugin for WordPress is vulnerable to Deserialization of Untrusted Data in all versions up to, and including, 14.5.0 This is due to the `bp_unserialize_profile_field()` function using `@unserialize()` without the `allowed_classes` parameter on user-controlled XProfile field data. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary PHP objects via XProfile textbox fields, which could lead to remote code execution if a suitable POP chain is available in the WordPress environment.	7.5	More Details
CVE-2026-52856	Wings is the server control plane for Pterodactyl, a free, open-source game server management panel. Prior to 1.13.0, a malformed packet received during the SFTP connection handshake causes a Go panic. This issue is fixed in version 1.13.0.	7.5	More Details
CVE-2026-66360	The ISO Presentation layer contains a flaw in the handling of specific parameters during normal mode negotiation. A missing length check in the processing of the encoded presentation data allows an attacker controlled field with a zero length value to trigger a bounded heap over read. This condition occurs before MMS session establishment, a crafted TCP/102 connection attempt can trigger the issue. The resulting over read causes the process to terminate, leading to a denial of service condition.	7.5	More Details
	The MASTER_PASSWORD_HOOK setting, introduced in pgAdmin 4 7.2, lets an administrator configure an external command that returns a per-user encryption key, with %u in the configured		

CVE-2026-17347	string replaced by the current user's name. The previous implementation substituted the username directly into the command string and executed the result with subprocess.Popen(..., shell=True). Because the username can originate from an external authentication source (OAuth/OIDC claims, Kerberos, webserver auth) rather than a value pgAdmin fully controls, a username containing shell metacharacters (';', '$()', backticks, pipes, '&&', newlines) allowed an authenticated user to execute arbitrary commands as the pgAdmin service account in any deployment where the configured hook string uses %u. Fix tokenises the trusted, administrator-configured hook string into an argument vector first (using shlex in POSIX-quoting mode, with backslash-escaping disabled so Windows-style paths are not mis-parsed), substitutes the untrusted username into the individual argv elements, and executes with shell=False. The username is therefore always confined to a single argv element; any shell metacharacters it contains are inert. Administrators whose MASTER_PASSWORD_HOOK previously relied on shell features (pipes, redirection, environment-variable expansion, globbing) within the hook string itself must move that logic into the invoked script, since it is no longer interpreted by a shell. This issue affects pgAdmin 4: from 7.2 before 9.17.	7.5	More Details
CVE-2026-44107	A reboot of the charging controller can be triggered via Modbus TCP without authentication. Therefore, when the Modbus functionality is enabled by opening the port that CharxModbusServer is listening, an unauthenticated attacker can perform a Denial-of-Service attack.	7.5	More Details
CVE-2026-12687	The ProfileGrid WordPress plugin before 5.9.9.8 does not restrict which group an anonymous visitor may register into through its front-end registration, allowing unauthenticated users to register directly into a privileged group and be granted that group's configured role, up to Administrator when such a group exists, leading to privilege escalation.	7.5	More Details
CVE-2026-18446	fast-uri before 4.1.2, 3.1.5, and 2.4.4 requires a literal double forward slash to recognize a URI authority, so a reference that uses a backslash based introducer in place of it (backslash backslash, forward slash backslash, or backslash forward slash) is parsed with no authority and folds into the path. Node's native WHATWG URL parser instead treats a backslash as interchangeable with a forward slash for special schemes, so the two parsers extract different hosts from the same input. Applications that use fast-uri to enforce host based policy such as allowlists, SSRF filtering, or redirect validation before passing the same URL into Node's URL or fetch consumers can be steered to an unintended host. Upgrade to fast-uri 4.1.2, 3.1.5, or 2.4.4.	7.5	More Details
CVE-2026-12500	The WP Travel Engine WordPress plugin before 6.8.2 does not perform a capability check on an AJAX action that updates a WP Travel Engine WordPress plugin before 6.8.2 option, allowing unauthenticated users to overwrite a site-wide WP Travel Engine WordPress plugin before 6.8.2 option (the public nonce that gates the action is served to anonymous visitors).	7.5	More Details
CVE-2026-18358	A flaw was found in gnome-remote-desktop as shipped in Red Hat Enterprise Linux. When the daemon is running in system mode with RDP enabled, the incoming connection handler bypasses the connection throttler, allowing an unauthenticated remote attacker to open many parallel pre-authentication connections to the RDP listener. This can accumulate accepted sockets and pending routing-token operations until timeout, exhausting resources and preventing legitimate users from establishing RDP sessions. This issue does not affect the upstream version.	7.5	More Details
CVE-2026-15722	A stack buffer overflow flaw was found in 389 Directory Server (389-ds-base). The get_ruvelement_from_berval() function in repl5_ruv.c copies digit characters from a network-supplied RUV berval into a fixed 16-byte stack buffer without bounds checking. A remote unauthenticated attacker can crash the LDAP server by sending a crafted StartNSDS50ReplicationRequest extended operation containing a replica ID field with more than 16 digit characters. The overflow occurs during payload decoding, before any authorization check. Stack protectors limit impact to denial of service.	7.5	More Details
CVE-2026-11770	A flaw was found in 389 Directory Server. An unauthenticated remote attacker can inject LDAP search filters into the CleanAllRUV replication status-check extended operation. Because the handler performs the search against cn=config with elevated replication plugin privileges and returns a boolean match result, the attacker can extract sensitive server configuration metadata, including replication bind DNs and password storage scheme information.	7.5	More Details
CVE-2026-65310	ANDRITZ HIPASE-250 (formerly 250 SCALA), in the default configuration of affected versions, exposes its data and configuration endpoint without any authentication and permissive CORS on every response. An unauthenticated attacker with network access can read live process values and server configuration.	7.5	More Details
CVE-	ANDRITZ HIPASE-250 (formerly 250 SCALA) in affected versions stores and transmits user		More

2026-65309	passwords using a reversible format instead of a one-way password hash. This allows an attacker able to read the credential store or capture network traffic to recover all stored passwords.	7.5	Details
CVE-2026-15048	The Geeky Bot WordPress plugin before 1.2.8 does not perform an authorization check on one of its AJAX actions, allowing unauthenticated users to retrieve chat-history session metadata including WordPress usernames, user IDs, and timestamps.	7.5	More Details
CVE-2026-14930	The JS Help Desk WordPress plugin before 3.1.4 does not perform any authorization, nonce, or ownership check on a front-end request dispatcher, allowing unauthenticated users to upload files (limited to the JS Help Desk WordPress plugin before 3.1.4's inert allowed extensions) and attach them to arbitrary users' support tickets.	7.5	More Details
CVE-2026-14830	The FlxWoo WordPress plugin before 3.1.1 does not verify with the payment processor that a checkout session was actually paid before marking the associated order as paid, allowing unauthenticated attackers to complete WooCommerce orders without paying.	7.5	More Details
CVE-2026-17887	Use after free in TabStrip in Google Chrome prior to 151.0.7922.72 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: Medium)	7.5	More Details
CVE-2026-14333	The Demi WordPress plugin before 0.0.7 stores its full-site backup archives in a publicly accessible location under a predictable filename and without access protection, allowing unauthenticated attackers to download complete backups including the site database and its user password hashes.	7.5	More Details
CVE-2026-14319	The GiveWP WordPress plugin before 4.16.3 does not properly restrict access to a REST API endpoint that returns recurring-donation records, allowing unauthenticated users to retrieve information about anonymous recurring donors, including their name and subscription details.	7.5	More Details
CVE-2026-12720	The Kirki WordPress plugin before 6.0.13 does not restrict which classes may be instantiated when it deserialises data that unauthenticated users can store, leading to PHP Object Injection that is triggered when an administrator later reviews the stored data. With a suitable gadget chain present on the site (via another installed Kirki WordPress plugin before 6.0.13, , or an outdated WordPress version), this could be leveraged to perform a variety of attacks, such as remote code execution.	7.5	More Details
CVE-2026-60075	Date::Manip versions through 6.99 for Perl allow CPU exhaustion via quadratic backtracking in the unanchored time substitution in _parse_time. _parse_time removes a time from anywhere in the string with the unanchored substitution `s/$timerx/ /`, where $timerx is an auto-generated alternation of time patterns reached through a leading `(?:$atrx|^|\s+)`. The engine therefore retries the match at every position of an interior whitespace run: at each start position the leading `\s+` consumes the rest of the run greedily, the time alternation fails because the run holds no digits, and the engine backtracks a space at a time across the run before advancing the start position, which is quadratic in the length of the run. No time need be present in the string for this to happen, only a long run of whitespace, and the parse time rises about fourfold for each doubling of the run: a few kilobytes of whitespace costs seconds of CPU per parse and tens of kilobytes costs minutes. Any caller that passes an untrusted string of unbounded length to ParseDate(), Date::Manip::Date->parse() or ->parse_time() can be made to spend unbounded CPU in a single parse, a denial of service.	7.5	More Details
CVE-2026-17896	Use after free in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	7.5	More Details
CVE-2026-17898	Use after free in DevTools in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code inside a sandbox via a crafted Chrome Extension. (Chromium security severity: Low)	7.5	More Details
CVE-2026-63222	CodeIgniter is a PHP full-stack web framework. Prior to 4.7.4, calling UploadedFile::move() without a second argument uses the client-provided filename without sanitization, allowing a remote attacker to use path traversal sequences to write uploaded content outside the intended directory when the application exposes an upload path. This issue is fixed in version 4.7.4.	7.5	More Details
CVE-	ComfyUI is a modular diffusion model GUI, API, and backend with a graph-and-node interface. Prior to 0.28.0, folder_paths.get_annotated_filepath and exists_annotated_filepath join workflow-controlled annotated filenames to a base directory without a containment check, allowing an		

2026-56673	unauthenticated crafted POST /prompt workflow using LoadImage or sibling nodes to probe arbitrary host paths and exfiltrate image-format files through /view. LoadImage defines a VALIDATE_INPUTS method, which causes the execution engine to skip COMBO (input-directory) validation. Affected nodes include LoadImage, LoadImageMask, LoadImageOutput, LoadAudio, LoadLatent, LoadVideo, and Load3D. This issue is fixed in version 0.28.0.	7.5	More Details
CVE-2026-56671	ComfyUI is a modular diffusion model GUI, api and backend with a graph/nodes interface. Prior to 0.28.0, get_model_preview in app/model_manager.py joins an unrestricted filename route capture to a selected model directory without a containment check, allowing an unauthenticated remote attacker to use traversal, encoded traversal, absolute paths, or an unbounded path_index to read image-decodable files and enumerate host paths. get_model_preview (app/model_manager.py) built the path with os.path.join(folder, filename) where filename is an unrestricted {filename:.*} route capture. Literal ../, percent-encoded %2e%2e%2f, and absolute paths all escaped the model directory; path_index was also unbounded. The target file is piped through Pillow and re-encoded as WEBP, so disclosure is limited to image-decodable files plus a file-existence/enumeration oracle (and internal-path leakage via path_index errors). This issue is fixed in version 0.28.0.	7.5	More Details
CVE-2026-43832	Full details and mitigation steps are currently restricted and will be published at a later date.	7.5	More Details
CVE-2026-43831	Full details and mitigation steps are currently restricted and will be published at a later date.	7.5	More Details
CVE-2026-43829	Full details and mitigation steps are currently restricted and will be published at a later date.	7.5	More Details
CVE-2026-17916	Insufficient policy enforcement in Settings in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)	7.5	More Details
CVE-2026-16540	The Simply Schedule Appointments WordPress plugin before 1.6.12.6 does not correctly restrict a bulk appointment operation to the requester's own records, allowing unauthenticated users to retrieve the personal data of all appointments across the site and, on premium editions, to permanently delete them.	7.5	More Details
CVE-2026-15240	The Customer Switching WordPress plugin before 2.1.3 does not securely bind an active user-switching session to the operator who initiated it, allowing a lower-privileged account that an operator is currently switched into to be resolved as that operator and to switch into any permitted account, including an administrator, resulting in full account takeover.	7.5	More Details
CVE-2026-47617	NVIDIA Dynamo for Linux contains a vulnerability in the multimodal media fetcher where an attacker may cause server-side request forgery via DNS rebinding. A successful exploit of this vulnerability might lead to information disclosure.	7.5	More Details
CVE-2026-50782	Jinher OA C6 contains an XML External Entity (XXE) injection vulnerability in the /c6/JHSoft.Web.HrmAttendance/sp_manager_getUserlist.aspx/GetXmlHttp endpoint. An unauthenticated remote attacker can send a crafted XML payload to read arbitrary files from the server via an out-of-band attack.	7.5	More Details
CVE-2026-47618	NVIDIA Dynamo for Linux contains a vulnerability in the Rust multimodal media fetcher where an attacker could cause server-side request forgery. A successful exploit of this vulnerability might lead to information disclosure.	7.5	More Details
CVE-2026-67437	OliveTin gives access to predefined shell commands from a web interface. From 3000.0.0 until 3000.17.0, the service/internal/auth/otoauth2/restapi_auth_oauth2.go OAuth2 login handler stores per-login state in the registeredStates map on every /oauth/login request without expiring, deleting, or bounding entries, allowing an unauthenticated attacker to exhaust memory and cause a denial of service. This issue is fixed in version 3000.17.0.	7.5	More Details
CVE-	Net::SAML2 versions before 0.86 for Perl allow SAML authentication bypass by verifying responses against the response-embedded certificate in verify_xml when no trust anchor is configured. verify_xml in Net::SAML2::Role::VerifyXML runs "return if !$anchors && !$cacert;" as soon as the XML::Sig check succeeds, and that check uses the X.509 certificate taken from the response's own dsig:KeyInfo/dsig:X509Certificate element, so an unanchored response is checked only against the		More

2026-18089	key it carries. Binding::POST declares cacert as an optional Maybe[Str] with no default, so a POST binding built without one takes that path, and _verify_encrypted_assertion returns early the same way with "return $xml unless $cacert;". Any caller that constructs Binding::POST or calls Assertion->new_from_xml without a cacert, cert_text, or anchors argument accepts a response signed by an attacker generated key whose self-signed certificate is embedded in that response, authenticating an arbitrary assertion.	7.5	Details
CVE-2026-17698	Insufficient validation of untrusted input in UI in Google Chrome on Android prior to 151.0.7922.72 allowed a local attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-47614	NVIDIA Dynamo for Linux contains a vulnerability where an attacker may cause server-side request forgery. A successful exploit of this vulnerability might lead to information disclosure.	7.5	More Details
CVE-2026-20479	In Modem, there is a possible out of bounds read 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: MOLY00741071; Issue ID: MSV-7620.	7.5	More Details
CVE-2026-47613	NVIDIA Dynamo for Linux contains a vulnerability where an attacker may cause improper limitation of a pathname to a restricted directory by supplying a crafted local path in a multimodal request. A successful exploit of this vulnerability might lead to information disclosure.	7.5	More Details
CVE-2026-3245	A deserialization vulnerability in PRISMAproduction Version 6.5 or earlier that may lead to arbitrary code execution.	7.5	More Details
CVE-2026-47616	NVIDIA Dynamo for Linux contains a vulnerability in the multimodal media fetcher where an attacker may cause server-side request forgery. A successful exploit of this vulnerability might lead to information disclosure.	7.5	More Details
CVE-2026-47612	NVIDIA Dynamo for Linux contains a vulnerability in the image loading component where an attacker may cause improper limitation of a pathname to a restricted directory. A successful exploit of this vulnerability might lead to information disclosure.	7.5	More Details
CVE-2026-65324	Apache Traffic Server drops the per-stream buffer cap when dechunking HTTP/2 or HTTP/3 responses, letting a slow client exhaust server memory. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	7.5	More Details
CVE-2026-24255	NVIDIA Dynamo for Linux contains a vulnerability in the multimodal embedding cache, where an attacker could cause a hash collision by submitting images that share an identical pixel byte sequence but have different dimensions. A successful exploit of this vulnerability might lead to data tampering.	7.5	More Details
CVE-2026-68580	FreeRDP before 3.29.0 contains integer overflow vulnerabilities in the audio input redirection channel (audin) across ALSA, sndio, WinMM, and OpenSL ES backends that fail to validate the FramesPerPacket parameter from RDP servers. Attackers can supply a malicious FramesPerPacket value causing allocation size wraparound, resulting in heap-based buffer overflow on ALSA or denial of service on all platforms.	7.5	More Details
CVE-2026-69089	Grav CMS 2.0.10 contains a path traversal vulnerability in ImageMedium::watermark(), which passes its unsanitized $image argument to RocketTheme\Toolbox\ResourceLocator\UniformResourceLocator::findResource(). Because the file:// scheme branch only lexically collapses '..' segments without a realpath/containment check, an editor authoring Markdown image syntax with traversal sequences can cause arbitrary image files outside Grav's media sandbox to be composited into a carrier image, which is then cached and served from a public, unauthenticated URL — disclosing those files to anonymous visitors.	7.5	More Details
CVE-2026-69091	Admidio before 5.0.11 contains an authentication bypass vulnerability in the forum module when configured in login-only mode. The access control logic in modules/forum.php fails to validate the login-only configuration state, allowing unauthenticated attackers to read forum topics and posts by directly accessing the module with read-only parameters.	7.5	More Details
CVE-	Apache Traffic Server can be crashed or driven to resource exhaustion by abusive HTTP/2 framing and flow-control. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0		More

2026-58151	through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	7.5	Details
CVE-2026-58161	Apache Traffic Server can crash from null dereferences and dangling references in TLS and SNI handling. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	7.5	More Details
CVE-2026-58163	Apache Traffic Server mishandles on-disk cache fields and object lifetimes, corrupting state or crashing. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	7.5	More Details
CVE-2026-58164	Apache Traffic Server has use-after-free and time-of-check/time-of-use errors in remap configuration handling. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	7.5	More Details
CVE-2026-18587	A flaw has been found in Wavlink WL-NU516U1 708c073-mt7628. The impacted element is an unknown function of the component Config Import. Executing a manipulation of the argument Password can lead to os command injection. The attack may be launched remotely. This attack is characterized by high complexity. The exploitability is regarded as difficult. The exploit has been published and may be used. It is advisable to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	7.5	More Details
CVE-2026-66315	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-58181	The Apache Traffic Server uri_signing and url_sig plugins can exhaust the stack or crash on attacker input. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	7.5	More Details
CVE-2026-58180	The Apache Traffic Server txn_box plugin overflows the stack from attacker-controlled input. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	7.5	More Details
CVE-2026-21555	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2026-21554	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2026-21553	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2026-21552	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2026-21551	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2026-47615	NVIDIA Dynamo for Linux contains a vulnerability where an attacker may cause server-side request forgery by supplying a crafted URL in a multimodal request. A successful exploit of this vulnerability might lead to information disclosure.	7.5	More Details
CVE-2026-	The Apache Traffic Server ESI plugin can recurse without bound and fetch attacker-controlled URLs. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or	7.5	More Details

58178	10.1.4, which fix the issue.		
CVE-2026-21550	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2026-21549	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2026-21548	In nr modem, there is a possible improper input validation. This could lead to remote denial of service with System execution privileges needed.	7.5	More Details
CVE-2026-58175	Apache Traffic Server leaks memory when handling HostDB SRV records. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	7.5	More Details
CVE-2026-58189	Apache Traffic Server allows redirect-limit bypass when plugins reset the retry counter, enabling SSRF amplification. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	7.5	More Details
CVE-2026-68578	ArcadeDB versions before 26.7.3 fail to bind the authenticated principal in the MCP HTTP transport, causing all engine permission checks to silently pass as no-ops. Non-root MCP-allowed users can perform arbitrary database writes, DDL, schema mutations, and execute arbitrary JavaScript code via the query tool.	7.5	More Details
CVE-2026-67357	ArcadeDB versions before 26.7.3 contain an information disclosure vulnerability in the MCP get_server_settings tool that leaks the arcadedb.ha.clusterToken in cleartext. Attackers with MCP access can retrieve the cluster token and use it with X-ArcadeDB-Cluster-Token and X-ArcadeDB-Forwarded-User headers to impersonate root and achieve full server compromise.	7.5	More Details
CVE-2026-67432	MCP Ruby SDK is the official Ruby SDK for Model Context Protocol servers and clients. Prior to 0.23.0, MCP::Server::Transports::StreamableHTTPTransport in the mcp gem reads and parses an entire JSON-RPC POST body without a size limit, allowing an unauthenticated remote attacker to exhaust process memory. This issue is fixed in version 0.23.0.	7.5	More Details
CVE-2026-15206	The SMS Alert WordPress plugin before 3.9.8 does not bind its "mobile verified" session flag to the phone number that was actually verified: after an attacker verifies an OTP sent to their own phone, the signup/login handler reads a fresh, attacker-supplied phone number to select the account and logs them in. An unauthenticated attacker can therefore log in as any user, including an administrator, who has a billing phone on file.	7.5	More Details
CVE-2026-69095	OpenWrt luci-app-bmx7 before commit 5890760a454dad2cb00389dba2cdc5e779e0ffdd contains a path traversal vulnerability in the bmx7-info CGI script that allows unauthenticated attackers to read files outside the configured runtimeDir. Attackers can supply directory traversal sequences in the query string to escape the intended directory and read sensitive files accessible to the CGI process.	7.5	More Details
CVE-2026-67857	open62541 1.5.5 contains an out-of-bounds read in the client-side function responseReadNamespacesArray() in src/client/ua_client_connect.c.	7.5	More Details
CVE-2026-67858	Buffer Overflow vulnerability exists in open62541 1.5.5 when the Local Discovery Server (LDS) is built with multicast discovery enabled through the MDNSD backend. An unauthenticated remote attacker can send a RegisterServer or RegisterServer2 request containing many unique discoveryUrls. This allows remote attackers to cause a denial of service.	7.5	More Details
CVE-2026-15241	The AI ChatBot for WooCommerce WordPress plugin before 4.8.4 does not perform any authorization or nonce check on one of its AJAX actions, allowing unauthenticated users to abuse the site owner's stored third-party API key to send requests billed to the owner's account and, when an optional feature is enabled, to retrieve indexed knowledge-base content.	7.5	More Details
CVE-2026-15236	The Gallery for Google Photos WordPress plugin before 1.2.1 does not properly restrict access to the stored third-party OAuth credentials of the connected account, exposing the persistent access and refresh tokens to unauthenticated users and allowing long-term compromise of the linked	7.5	More Details

	account.		
CVE-2025-60931	An Insecure Direct Object Reference (IDOR) in the Employee Compensation View function of Infor Global HR v11.24.10.01.33 allows unauthorized attackers to arbitrarily view the compensation information of other employees via a crafted GET request.	7.5	More Details
CVE-2026-48399	Adobe Campaign Classic (ACC) is affected by a Violation of Secure Design Principles vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2026-69185	Socket.IO enables bidirectional and low-latency communication for every platform. Prior to 4.2.7, 3.4.5, and 3.3.6, a specially crafted Socket.IO packet can make the server wait for a large number of binary attachments and buffer them, which can be exploited to make the server run out of memory. This vulnerability is fixed in 4.2.7, 3.4.5, and 3.3.6.	7.5	More Details
CVE-2026-15151	The Five Star Restaurant Reservations WordPress plugin before 2.7.23 does not perform a capability check on one of its AJAX actions, allowing users with the lowest booking-management role (which by default cannot access the Five Star Restaurant Reservations WordPress plugin before 2.7.23's settings) to reset the site's configured booking notification rules.	7.5	More Details
CVE-2026-67859	Buffer Overflow vulnerability in open62541 v1.5.5 allows a remote attacker to cause a denial of service via the Discovery/LDS handling.	7.5	More Details
CVE-2026-18352	The User Access Manager plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.3.15 via the 'uamgetfile' parameter parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. This is possible because when attachment_url_to_postid() returns 0 for a traversal path, the plugin falls back to the global post set by a valid ?attachment_id parameter supplied by the attacker, causing the access check to pass against a legitimate public attachment while the file streamed is the attacker-chosen path.	7.5	More Details
CVE-2026-13339	The CubeWP Framework plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.1.30 via the 'cubewp_get_svg_content' function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. This is exploitable by unauthenticated attackers because the required nonce is publicly emitted into the markup of any page rendering the CubeWP posts shortcode or widget with AJAX loading enabled, making it harvestable by any guest visitor before submitting the AJAX request.	7.5	More Details
CVE-2026-67978	An issue in the SBN UDP interface of NASA cFS v7.0.1 allows attackers to cause a Denial of Service (DoS) via transmitting a crafted SBN frame.	7.5	More Details
CVE-2026-67861	An issue in open62541 v.1.5.5 and before allows a remote attacker to cause a denial of service via the UA_Client_getRemoteDataTypes component	7.5	More Details
CVE-2026-45103	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. In versions prior to 3.6.6 and 4.0.0-rc1, the TCP message framing layer parses the Content-Length header using unsigned int arithmetic with no overflow check. When an attacker sends a Content-Length value that overflows unsigned int (e.g., 4294967296), the framing layer computes a wrapped-around value (e.g., 0) and splits the TCP stream at the wrong boundary, causing the body of the first SIP message to be processed as a separate message and enabling SIP message smuggling. Because Content-Length is parsed in the transport layer before authentication, an unauthenticated, network-based attacker can smuggle arbitrary SIP messages over any TCP-based transport (proto_tcp, proto_tls, proto_ws, proto_wss) on any instance with TCP enabled, with no routing-script preconditions. This allows smuggled messages to bypass front-end SBC/proxy security policies, inherit the connection's authentication context, and evade rate limiting. This issue has been fixed in versions 3.6.6 and 4.0.0-rc1.	7.5	More Details
CVE-2026-58186	The Apache Traffic Server webp_transform plugin can decode unsafely and serve mislabeled, cacheable responses. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	7.5	More Details

CVE-2026-65943	Joomla Extension - rolandd.com - Unauthenticated directory creation RO CSVI < 9.11.0	7.5	More Details
CVE-2026-24084	Weak configuration when UE does not verify the consistency of its additional security capabilities with the replayed capabilities.	7.5	More Details
CVE-2026-16285	The Product Attachment for WooCommerce WordPress plugin before 2.3.3 does not perform any authorization check before streaming media library files, allowing unauthenticated users to download any attachment — including private or unlinked uploads — by enumerating its numeric ID.	7.5	More Details
CVE-2026-67215	cJSON through 1.7.19 is vulnerable to uncontrolled recursion leading to stack exhaustion when an untrusted RFC 6902 JSON Patch is applied via cJSONUtils_ApplyPatches() or cJSONUtils_ApplyPatchesCaseSensitive(). A patch containing add and copy operations grafts duplicated subtrees to amplify document depth beyond the parser's nesting limit: cJSON_Delete() recurses with no depth bound, and the cJSON_Duplicate() guard CJSON_CIRCULAR_LIMIT is set to 10000, ten times the parser's 1000-level nesting limit and high enough to overflow a default thread stack. An attacker who can supply the patch document can crash the process, resulting in denial of service.	7.5	More Details
CVE-2026-67198	Perspective 5.0.0 contains a denial-of-service vulnerability in the VirtualServer protocol dispatcher that allows unauthenticated remote attackers to crash the server process by sending malformed or incomplete protobuf messages. Attackers can send well-formed requests such as ViewToArrowReq with no viewport set or MakeTableReq with no data field to trigger unwrap() calls on None values at nine distinct sites, causing the process to abort with SIGABRT.	7.5	More Details
CVE-2026-67200	Perspective 5.0.0 contains a path traversal vulnerability that allows unauthenticated remote attackers to read arbitrary files from the server filesystem by including literal ../ segments in HTTP request URL paths. Attackers can bypass the insufficient query-string-stripping sanitization to traverse outside the configured asset root directory and retrieve sensitive files such as system credentials and application secrets, with results exposed cross-origin due to a wildcard Access-Control-Allow-Origin header set on all responses.	7.5	More Details
CVE-2026-69152	The brace-expansion library generates arbitrary strings containing a common prefix and suffix. Prior to 1.1.18, 2.1.4, 3.0.6, and 5.0.9, expand() does not apply maxLength while constructing comma-alternative intermediate arrays or padded sequences, allowing attacker-controlled input to exhaust memory or block the event loop. The fix for CVE-2026-14257 is bypassed by the vulnerability. This issue is fixed in versions 1.1.18, 2.1.4, 3.0.6, and 5.0.9.	7.5	More Details
CVE-2026-16261	The login-social WordPress plugin through 1.0.4 does not validate password-reset requests against a reset key or the requester's identity, and it issues authentication sessions from unverified third-party sign-in data, allowing unauthenticated attackers to reset any user's password or log in as any existing account, including administrators, and take over the site.	7.5	More Details
CVE-2026-15975	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 11.8 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an unauthenticated user to cause a denial of service due to insufficient resource throttling when processing merge request discussions.	7.5	More Details
CVE-2026-18568	XML::Sig versions from 0.29 before 0.72 for Perl allow signature verification bypass because verify returns true when every signature was skipped before any cryptographic check. verify in lib/XML/Sig.pm counts the `//dsig:Signature` elements into `$numsigs` and iterates over them, but two paths reach `next` before any digest or key check runs: a `SignedInfo/Reference/@URI` that resolves to no element while `$numsigs` is greater than 1, and, when `id_attr` is set, a reference that does not match the requested ID. The loop records nothing about what it checked, so when every signature takes one of those paths control reaches the unconditional `return 1` that ends verify. Two `Signature` elements whose Reference URI names an ID that no element carries is enough, as is one such element combined with `id_attr`. Any caller that passes untrusted XML to verify can receive a true return for a document in which no digest and no signature value was checked; a `cert` or `cert_text` trust anchor does not change this, because no key check runs. Versions up to 0.28 use an XML::XPath based verify that has no such skip and are not affected.	7.5	More Details
CVE-	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in		More

2026-61372	Apache Jena Fuseki. This issue affects Apache Jena Fuseki: through 6.1.0. Users are recommended to upgrade to version 6.2.0, which fixes the issue.	7.5	Details
CVE-2026-66321	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	7.4	More Details
CVE-2026-65802	External control of file name or path in Microsoft Edge for Android allows an unauthorized attacker to disclose information over a network.	7.4	More Details
CVE-2026-25288	Transient DOS when processing a short target wake time channel usage response frame with insufficient packet size.	7.4	More Details
CVE-2026-54660	swagger-typescript-api generates API clients for Fetch or Axios from OpenAPI specifications. Prior to 13.12.2, src/resolved-swagger-schema.ts getRemoteRequestHeaders forwards --authorizationToken to every URL fetched by fetchRemoteSchemaDocument while warmUpRemoteSchemasCache resolves external $ref URLs, allowing an attacker-controlled OpenAPI spec to exfiltrate the developer or CI bearer token to a cross-origin endpoint. This issue is fixed in version 13.12.2.	7.4	More Details
CVE-2026-13697	undici's cache interceptor mishandles malformed Cache-Control private directives. In undici 7.0.0 up to before 7.29.0 and 8.0.0 up to before 8.9.0, a response carrying a degenerate qualified private directive, such as private set to an empty value, can be stored in the default shared cache and later served to a different caller with the same cache key, disclosing private response bodies and headers including Set-Cookie. Separately, a Cache-Control header that combines an unqualified private directive with a qualified one triggers an uncaught TypeError in the cache-control parser, which rejects the request and, depending on the consumer's error handling, can terminate the process. Both issues affect applications using the cache interceptor in shared mode, including the default configuration. The issues are fixed in undici 7.29.0 and 8.9.0.	7.4	More Details
CVE-2026-56822	Netty is an asynchronous, event-driven network application framework. Prior to versions 4.1.136.Final and 4.2.16.Final, the OcspServerCertificateValidator forwards the SslHandshakeCompletionEvent before the asynchronous OCSP validation completes. This allows the client's downstream handlers to send sensitive application data (e.g., HTTP requests) to a revoked server before the channel is closed by the OCSP check. n io.netty.handler.ssl.ocsp.OcspServerCertificateValidator#userEventTriggered, when an SslHandshakeCompletionEvent is received, the validator immediately calls ctx.fireUserEventTriggered(evt). It then initiates an asynchronous OCSP query using OcspClient.query. Because the handshake completion event is forwarded immediately, downstream handlers in the client's pipeline are notified that the TLS handshake is successful. They may then begin reading and processing incoming application data or sending outgoing data. If the OCSP response later indicates the server's certificate is REVOKED, the validator closes the channel, but by this time, the client may have already leaked sensitive data to a revoked server or processed malicious responses from it. This issue has been fixed in versions 4.1.136.Final and 4.2.16.Final.	7.4	More Details
CVE-2026-67598	Emlog Pro through 2.6.23 contains a disabled TLS certificate validation vulnerability in include/service/ai.php that allows network-adjacent attackers to intercept outbound HTTPS requests to configured LLM providers by presenting arbitrary TLS certificates, as CURLOPT_SSL_VERIFYPEER and CURLOPT_SSL_VERIFYHOST are unconditionally disabled across sendStream(), sendImageRequest(), send(), and fetchSearchHtml() with no option to re-enable verification. Attackers can perform man-in-the-middle interception to extract Authorization Bearer API keys from every AI request and inject crafted AI responses that may be acted upon by the tool-call execution pipeline, including the query_database and update_config tool handlers.	7.4	More Details
CVE-2026-14838	Use of GET request method with sensitive query strings vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Session Hijacking. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	7.4	More Details
CVE-2026-8497	Improper certificate validation in the Devolutions Server connection handling in Devolutions Password Manager 2026.2.1.0 and earlier on Android, iOS, and macOS allows an adjacent-network attacker to intercept and modify sensitive information via a forged TLS certificate.	7.4	More Details
	Netty is an asynchronous, event-driven network application framework. Prior to versions		

CVE-2026-56821	4.1.136.Final and 4.2.16.Final, the OcspServerCertificateValidator flags an out-of-date OCSP response but does not stop processing it, so an expired GOOD response is still reported as VALID, letting an on-path attacker replay a stale GOOD response to bypass revocation of a since-revoked certificate. Exploitation can lead to certificate revocation bypass via replay of an expired OCSP response. Any application using OcspServerCertificateValidator is affected; a revoked certificate can be accepted. This issue has been fixed in versions 4.1.136.Final and 4.2.16.Final.	7.4	More Details
CVE-2026-18394	Incorrect authorization in the http_request tool in Strands Agents Tools before 0.8.2 might allow remote attackers to obtain credentials configured via HTTP_REQUEST_TOKEN_CONFIG by influencing the LLM to route requests through actor-controlled proxy infrastructure. To remediate this issue, users should upgrade to version 0.8.2.	7.4	More Details
CVE-2026-13690	The UsersWP WordPress plugin before 1.2.67 does not validate the selected authentication provider in its two-factor login handler, allowing an attacker who already knows a user's credentials to bypass the second authentication factor and log in as that user.	7.4	More Details
CVE-2026-51953	An issue in FeehiCMS v.2.1.1 allows an attacker to escalate privileges via the Session management module, authentication logic, logout handler components	7.4	More Details
CVE-2026-18556	Authentication bypass using an alternate path or channel vulnerability in N-able N-central allows Authentication Bypass. This issue affects N-central: through 2026.1.	7.4	More Details
CVE-2025-69944	kishan0725 Hospital Management System 4.0 is vulnerable to SQL Injection in the view-medhistory.php endpoint via the viewid parameter.	7.3	More Details
CVE-2026-18641	A vulnerability was determined in Sangfor Operation and Maintenance Security Management System up to 3.0.13. Affected by this vulnerability is the function com.sbr.fort.foreignDP.DpLoginController of the file /fort/portal_login of the component Login Endpoint. This manipulation causes os command injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-18770	A vulnerability has been found in vibesurf-ai VibeSurf up to cd6e519d507cdd4d63061300bf60fb176e1f57e0. Impacted is an unknown function of the file /code of the component Python Validation Handler. The manipulation leads to code injection. Remote exploitation of the attack is possible. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-18810	A security vulnerability has been detected in H3C NX15 V100R017. Impacted is an unknown function of the file /api/wizard/networkSetup. Such manipulation leads to missing authentication. The attack may be performed from remote. The vendor was contacted early about this disclosure.	7.3	More Details
CVE-2026-18788	A security flaw has been discovered in Trippo ResponsiveFilemanager up to 9.14.0. The impacted element is an unknown function of the file filemanager/dialog.php. The manipulation results in unrestricted upload. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	7.3	More Details
CVE-2026-18647	A security vulnerability has been detected in jina-ai reader up to 1574bfd380d249c86c82db4dace0d9c8fe17e2b1. This issue affects the function isValidTLD of the file /backend/functions/src/cloud-functions/crawler.ts of the component Crawler/Puppeteer. The manipulation leads to server-side request forgery. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-65947	Joomla Extension - balbooa.com - Various CSRF vectors in the admin interface in Gridbox < 2.20.2	7.3	More Details
CVE-	A DLL hijacking vulnerability in GeoVision GV-ASManager allows a local attacker with write access to an unsafe search directory to execute arbitrary code. By placing a crafted dynamic-link library		More

2026-18755	(DLL) file into the application search path prior to the legitimate library, the malicious code is loaded and executed under the security privileges of the GV-ASManager process.	7.3	Details
CVE-2026-11980	IBM Aspera Desktop App 1.0.5 through 1.0.19 can allow arbitrary code execution by loading DLL files at start-up.	7.3	More Details
CVE-2026-42169	A heap-buffer-overflow vulnerability exists in the APNG (Animated PNG) file loader of GIMP. This flaw occurs when the `fcTL` width exceeds the `IHDR` width, leading to pixel data being written past the end of a heap allocation. Additionally, a heap-based buffer overflow exists in the DDS plug-in due to a BPP mismatch in the `load_layer()` function. Both vulnerabilities can be triggered by opening a specially crafted image file, potentially leading to code execution.	7.3	More Details
CVE-2025-67408	Sourcecodester CASAP Automated Enrollment System 1.0 is vulnerable to SQL Injection in /save_user.php via the parameter status.	7.3	More Details
CVE-2026-15144	@fastify/rate-limit before 11.2.0 keys rate-limit buckets by the verbatim client IP string returned from request.ip. Because a single IPv6 client can control a large address range (a /64 holds 2^64 distinct addresses) and the same address has multiple valid textual representations, an IPv6 capable client can defeat the rate-limit boundary by rotating addresses or by rewriting the same address in different forms. Applications that use @fastify/rate-limit to protect endpoints such as authentication, password reset, OTP delivery, or expensive API calls can be bypassed by IPv6 clients behind a proxy that surfaces IPv6 to the origin when trustProxy is enabled. The issue is fixed in @fastify/rate-limit 11.2.0, where the default key generator normalizes IPv6 addresses to their canonical form, collapses IPv4 mapped IPv6 to IPv4, and applies a configurable prefix mask (default /64) via a new ipv6Subnet option.	7.3	More Details
CVE-2026-4793	An incorrect default permissions vulnerability in Synology Assistant before 7.0.7-50095 allows local users to read or write arbitrary files and conduct denial-of-service during installation.	7.3	More Details
CVE-2025-69945	kishan0725 Hospital Management System 4.0 is vulnerable to SQL Injection in /doctor/edit-patient.php?editid=1.	7.3	More Details
CVE-2026-16527	An unauthenticated remote attacker can bypass access controls by sending crafted requests to the PCP pmproxy /store endpoint. This allows the attacker to overwrite any PMDA metric, leading to arbitrary code execution and system takeover.	7.3	More Details
CVE-2025-67407	Sourcecodester CASAP Automated Enrollment System 1.0 is vulnerable to SQL Injection in update_student.php via parameters fname and student_class.	7.3	More Details
CVE-2025-67406	https://www.sourcecodester.com Advocate office management system 1.0 is affected by: SQL Injection. The impact is: execute arbitrary code (remote). The component is: control/activate_case.php,?id=1. The attack vector is: A SQL Injection vulnerability exists in the activate_case.php in parameter id endpoint of Advocate office management system. Unsanitized user input in the specified parameter is interpolated directly into an SQL query, allowing attackers to infer or extract data and, in some cases, execute stacked/time-based payloads. ¶¶ Affected Component & Parameter Affected Endpoint URL: http://localhost/advocate/kortex_lite/control/activate_case.php?id=1 HTTP Method: GET Vulnerable File: activate_case.php Parameter: id Vector Location: GET Injection Techniques (as identified by sqlmap) Type: error-based Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE) Payload: id=1 AND EXTRACTVALUE(6268,CONCAT(0x5c,0x71766b6a71,(SELECT (ELT(6268=6268,1))),0x716a7a6b71)) Type: time-based blind Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP) Payload: id=1 AND (SELECT 4464 FROM (SELECT(SLEEP(5)))aHqo) Proof of Concept (Burp Repeater)	7.3	More Details
CVE-2025-67405	Sourcecodester CASAP Automated Enrollment System 1.0 is vulnerable to SQL Injection in update_password.php via the parameter new_password.	7.3	More Details
CVE-2025-	kishan0725 Hospital Management System 4.0 is vulnerable to SQL Injection in	7.3	More

69949	check_availability.php via the parameters emailid and email.		Details
CVE-2026-54737	@phun-ky/defaults-deep is a library like lodash defaultsDeep with array preservation and no lodash dependency. Prior to 2.0.5, defaultsDeep() recursively merges user-supplied objects without filtering proto, constructor, and prototype, allowing properties to be written to Object.prototype. This issue is fixed in version 2.0.5.	7.3	More Details
CVE-2026-18481	Stored cross-site scripting in the participant URL handling in AWS Ops Wheel before PR #168 might allow an authenticated remote user to steal session tokens and escalate to full administrative control of the deployed instance via a crafted participant_url value containing a dangerous URI scheme. To remediate this issue, users should redeploy from the latest version of aws-ops-wheel.	7.3	More Details
CVE-2026-23904	Kyuubi Engine UI proxy accepts a host and port from the request path and proxies HTTP requests to that destination. A remote requester with network access to the proxy can cause the Kyuubi server to send HTTP requests to arbitrary reachable hosts, resulting in SSRF or open-proxy behavior. This issue affects Apache Kyuubi: from 1.8.0 before 1.12.0. Users are recommended to upgrade to version 1.12.0, which disables the proxy by default. To restore proxied Engine UI, set kyuubi.frontend.rest.engine.ui.proxy.enabled=true and configure allowed target hosts with kyuubi.frontend.rest.engine.ui.proxy.hosts.	7.3	More Details
CVE-2026-67333	better-auth before 1.6.13 (and pre-release builds 1.7.0-beta.0 through 1.7.0-beta.3) fail to validate the scheme of redirect_uris registered via the deprecated oidc-provider plugin and the mcp plugin (which wraps the same provider). An attacker can register an OAuth client with a javascript: redirect_uri, which the authorization server later returns unchanged in the consent response. If the deployment's consent page navigates the browser to the returned redirectURI (e.g. assigning it to window.location.href), the attacker's JavaScript executes in the authorization-server origin, exposing the victim's session and enabling account takeover.	7.2	More Details
CVE-2026-69246	Guzzle is an extensible PHP HTTP client. Prior to 7.15.2 and 8.0.1, Guzzle gives a transport the request URI as text and supplies the Host header separately. The cURL handlers set CURLOPT_URL to the URI exactly as written and push that Host into CURLOPT_HTTPHEADER; StreamHandler does the same through fopen(). libcurl then parses the authority itself, percent-decoding it and, on an IDN-capable build, applying IDNA mapping, and uses the result to resolve, connect, name the TLS peer and address a proxy CONNECT, while the supplied Host suppresses the aligned one libcurl would have generated. For a URI host written as 127.0.0.%31, filter_var() rejects the host as an IP literal, yet libcurl decodes it to 127.0.0.1 and reaches loopback with no DNS lookup while the server receives Host: 127.0.0.%31. An attacker who influences a fetched URI can therefore reach a host the application's checks excluded and read whatever the host exposes of the response. The same divergence moves Guzzle's own decisions onto a spelling the transport does not use: no_proxy selects proxy routing from the literal host, and RedirectMiddleware decides from it whether to strip Authorization and Cookie. Exploitation requires the application to build a request URI from untrusted input and to make a host decision before handing it to Guzzle. This issue is fixed in versions 7.15.2 and 8.0.1.	7.2	More Details
CVE-2026-12476	The Easy Digital Downloads plugin for WordPress is vulnerable to Arbitrary File Upload in versions up to and including 3.6.9. This is due to insufficient file type validation in the edd_do_ajax_import_file_upload() function , which only checks the client-supplied $_FILES['edd-import-file']['type'] Content-Type header against an allow-list of CSV mime types, then uses raw move_uploaded_file() (bypassing wp_handle_upload()'s core MIME enforcement) to write the file under its original extension into the web-accessible wp-content/uploads/edd/exports/ directory. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2026-67599	ClearOS 7.9 contains an OS command injection vulnerability in the Log Viewer component that allows authenticated attackers to execute arbitrary commands by submitting unsanitized input through the filter parameter, which is interpolated directly into a shell command in File.php. Attackers can inject command substitution payloads into the filter parameter to execute arbitrary commands as the webconfig user, and due to extensive NOPASSWD sudo privileges granted to that user by default, immediately escalate to root.	7.2	More Details
CVE-2026-	A vulnerability was found in H3C NX15 V100R017. This impacts the function reload.reload_config of the file /api/esps. The manipulation results in command injection. The attack can be launched remotely. The exploit has been made public and could be used. The vendor was contacted early	7.2	More Details

18814	about this disclosure.		
CVE-2026-18813	A vulnerability has been found in H3C NX15 V100R017. This affects the function delete of the file /api/esps. The manipulation of the argument esps.apcm.version leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure.	7.2	More Details
CVE-2026-15052	The MailChimp Subscribe Form, Optin Builder, PopUp Builder, Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Form Field Values in all versions up to, and including, 4.3.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-6837	A post-authentication command injection vulnerability in the "export-cgi" CGI program in Zyxel WAX650S firmware versions through 7.10(ABRM.4)C0 could allow an authenticated attacker with administrator privileges to execute OS commands on an affected device.	7.2	More Details
CVE-2026-61524	WebsiteBaker CMS before 2.13.10 contains an unrestricted file upload vulnerability in the module installation feature that allows authenticated administrators to achieve remote code execution by uploading a crafted ZIP archive containing a PHP webshell alongside a valid info.php metadata file. Attackers can place the malicious archive through the module installation interface, causing the application to extract the webshell into a web-accessible modules/ subdirectory where it becomes immediately executable by any unauthenticated user via direct HTTP request.	7.2	More Details
CVE-2026-61523	WebsiteBaker CMS before 2.13.10 contains a code injection vulnerability in the Droplets editor that allows authenticated administrators to inject arbitrary PHP code by submitting malicious content through the droplet Code field, which is written verbatim to a publicly accessible PHP file with no content sanitization. Attackers can save a PHP webshell via the save_droplet handler to a predictable path inside the modules directory, enabling unauthenticated users to achieve remote code execution by making direct HTTP requests to the written file.	7.2	More Details
CVE-2026-14818	A path traversal vulnerability in the CLI command used to execute configuration files in Zyxel ATP series firmware versions from V4.32 through V5.42 Patch 1, USG FLEX series firmware versions from V4.50 through V5.42 Patch 1, USG FLEX 50(W) series firmware versions from V4.16 through V5.42 Patch 1, and USG20(W)-VPN series firmware versions from V4.16 through V5.42 Patch 1 could allow an authenticated attacker with administrator privileges to execute a crafted malicious configuration file on an affected device.	7.2	More Details
CVE-2026-18812	A flaw has been found in H3C NX15 V100R017. The impacted element is the function esps.ipv6.wan of the file /api/esps. Executing a manipulation of the argument workMode can lead to command injection. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure.	7.2	More Details
CVE-2026-18255	A flaw was found in Quay. A user configured in GLOBAL_READONLY_SUPER_USERS is able to view robot account tokens for repositories they are not a member of, allowing an attacker with read-only superuser privileges to impersonate any robot account.	7.2	More Details
CVE-2026-16597	The GTM4WP – A Google Tag Manager (GTM) plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via WooCommerce Billing Fields in all versions up to, and including, 1.22.3 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 requires the GTM4WP WooCommerce order data integration option (GTM4WP_OPTION_INTEGRATE_WCORDERDATA) to be enabled, and is exploited by placing a guest checkout order with a JavaScript payload in a WooCommerce billing field such as the billing first name.	7.2	More Details
CVE-2026-18811	A vulnerability was detected in H3C NX15 V100R017. The affected element is the function Add of the file /api/esps. Performing a manipulation of the argument esps.filter.url results in command injection. It is possible to initiate the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure.	7.2	More Details
CVE-2026-67608	Telenia Software TVox 26.5.3 and prior 26.x versions, and 24.9.21 and prior 24.x versions, contain an OS command injection vulnerability in action_audio.php that allows authenticated attackers to execute arbitrary operating system commands by passing an unsanitized pid parameter into an exec() call when the action parameter is set to checkProcess. Attackers can inject malicious OS commands through the pid request parameter to execute arbitrary commands with the privileges	7.2	More Details

	of the apache user.		
CVE-2026-13425	The Database for CF7 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Array Form Field Values in all versions up to, and including, 1.2.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is exploitable by unauthenticated attackers because Contact Form 7 accepts array-structured input for ordinary text fields (e.g., your-name[]) via the public REST API endpoint /wp-json/contact-form-7/v1/contact-forms/{id}/feedback, and the plugin stores submitted data using $wpdb INSERT with serialize() into a custom wp_cf7db table, bypassing WordPress save-time filtering via wp_insert_post/wp_kses.	7.2	More Details
CVE-2026-67244	A format string vulnerability was found in the Notification OAuth settings of ADM. The vulnerability occurs because user-controlled notification configuration input may be processed through an unsafe format string operation. An authenticated administrator can exploit this issue to disclose memory information or cause denial of service of the affected component. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.RUN1 as well as from ADM 5.0.0 through ADM 5.1.3.RI81.	7.2	More Details
CVE-2026-16655	The Fluent Forms – Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Name Field Nested `password` Member in all versions up to, and including, 6.2.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-13392	The ElementsKit Elementor Addons WordPress plugin before 3.10.01 does not prevent a custom-widget definition saved by a user with administrative capabilities from being written verbatim into a generated PHP file that the ElementsKit Elementor Addons WordPress plugin before 3.10.01 subsequently executes, allowing arbitrary PHP code to run on the server; on a multisite network this lets a non-super subsite Administrator, who is otherwise denied code/file editing, reach host-level code execution beyond the privileges the network grants them.	7.2	More Details
CVE-2026-24033	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 10.0.0 through 10.1.3, from 9.0.0 through 9.2.14. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fixes the issue.	7.2	More Details
CVE-2026-15397	The Subscriptions for WooCommerce plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 2.0.0. This is due to the plugin not properly verifying that a user is authorized to perform an action via the wps_sfw_install_plugin_configuration AJAX handler. This makes it possible for authenticated attackers, with shop manager-level access and above, to install and activate arbitrary WordPress.org plugins.	7.2	More Details
CVE-2026-16843	Some Hikvision Networking Products are vulnerable to authenticated command execution due to insufficient input validation. Attackers with valid credentials can exploit this flaw by sending crafted packets containing malicious commands to affected devices, leading to arbitrary command execution.	7.2	More Details
CVE-2026-39931	OpenEMR through 8.2.0 contains an authenticated SQL injection vulnerability in the backup configuration import feature that allows administrators with admin or super ACL privileges to execute arbitrary DDL and DML statements against the application database by uploading a crafted SQL file at the form_step=202 parameter in backup.php. Attackers can exploit the unfiltered shell_exec invocation of the mysql command-line client to extract credential hashes, modify access control tables, inject backdoor accounts, create persistent triggers or stored procedures, and write arbitrary files to the filesystem where MySQL FILE privileges and permissive secure_file_priv settings are configured.	7.2	More Details
CVE-2026-38710	TR1200 v2.4.15 and TR3000 v2.4.21 were discovered to contain a command injection vulnerability in the system.setclock interface. This vulnerability allows attackers to execute arbitrary commands as root via a crafted input.	7.2	More Details
CVE-2026-67329	@better-auth/stripe versions >= 1.4.11 and < 1.6.21, and >= 1.7.0-beta.0 and < 1.7.0-beta.10, contain an authorization bypass in organization subscription actions. The middleware validates the organization ID taken from the request query string against the authorizeReference callback, but the handler reads the organization ID only from the request body and falls back to the caller's active organization from their session. When these differ, an authenticated member of multiple organizations can perform subscription actions (cancel, change plan, restore, billing portal access)	7.1	More Details

	against an organization they belong to but should not manage, and can access another organization's billing details including payment methods, invoices, and subscription state.		
CVE-2026-17750	Use after free in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	7.1	More Details
CVE-2026-14239	The tourmaster WordPress plugin before 5.4.8 does not perform a nonce check when storing a custom-filter label taken from a request parameter, and does not escape that label when echoing it on the filter admin page, allowing an unauthenticated attacker to trick a logged-in administrator into storing JavaScript that then executes in the admin area (stored Cross-Site Scripting via CSRF).	7.1	More Details
CVE-2026-66322	Origin validation error in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	7.1	More Details
CVE-2026-65875	BaserCMS provided by baserCMS Users Community contains a CSV file injection vulnerability. If a user downloads and opens a CSV file containing malicious code injected by an attacker, the malicious code may be executed.	7.1	More Details
CVE-2026-17867	Insufficient validation of untrusted input in Dawn in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	7.1	More Details
CVE-2026-14234	The WOLF WordPress plugin before 1.1.0 does not perform a nonce or capability check on one of its AJAX actions, allowing an unauthenticated attacker to trick a logged-in administrator into writing arbitrary content, including a malicious script, into a post via a cross-site request, resulting in stored Cross-Site Scripting.	7.1	More Details
CVE-2026-65981	Coturn is a free open source implementation of TURN and STUN Server. Prior to 4.15.0, a server using --mobility authenticates a resumed REFRESH request with the resuming user's credentials but does not verify that identity against the original allocation owner, allowing an authenticated attacker who obtains a victim MOBILITY-TICKET to receive and inject relayed traffic and consume the victim's quota. In the handle_turn_refresh resume branch, the victim allocation (orig_ss) is located solely by the attacker-controlled mobile id, and credentials are only adopted (via copy_auth_parameters) when the resuming session is unauthenticated. Because the attacker's session already has hmackey_set set to 1 from its own prior authentication (which is never reset for long-term-credential sessions), the credential copy is skipped and check_stun_auth validates the REFRESH against the attacker's own identity rather than the allocation owner's. This issue is fixed in version 4.15.0.	7.1	More Details
CVE-2026-17888	Insufficient validation of untrusted input in WebUI in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via malicious network traffic. (Chromium security severity: Medium)	7.1	More Details
CVE-2026-17744	Inappropriate implementation in File Input in Google Chrome on Linux prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	7.1	More Details
CVE-2026-44097	A low-privileged remote attacker with "operator" access can upload arbitrary files via the REST endpoint intended for firmware updates, resulting in persistent storage of attacker-controlled files and potentially exhausting resources, which might lead to Denial-of-Service.	7.1	More Details
CVE-2026-18806	External control of file name or path vulnerability in TÜBİTAK BİLGEM Software Technologies Research Institute pardus-image-writer allows Removing Important Client Functionality. This issue affects pardus-image-writer: before 1.0.4.	7.1	More Details
CVE-2025-71400	better-auth passkey versions before 1.4.0 contain an insecure direct object reference vulnerability in the passkey deletion endpoint that allows authenticated users to delete arbitrary passkeys by ID. Attackers with valid sessions can submit crafted requests to the delete-passkey endpoint with enumerated passkey IDs to remove other users' passkeys.	7.1	More Details
CVE-2026-12945	IBM Langflow OSS 1.0.0 through 1.10.1 allows authenticated users to access and manipulate other users' build jobs through improper access control on log retrieval and unauthenticated build endpoints.	7.1	More Details
CVE-2026-	Insufficient validation of untrusted input in WebView in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted	7.1	More

17741	HTML page. (Chromium security severity: Medium)		Details
CVE-2026-11368	The Bluetooth host ATT layer (subsys/bluetooth/host/att.c) associates each in-flight ATT TX buffer with its owning channel via the static tx_meta_data_storage[] array (data->att_chan = chan). When a buffer's last reference is dropped, its net-buf destroy callback defers the completion handling to the system workqueue (att_tx_destroy -> att_tx_destroy_work_handler -> att_on_sent_cb -> bt_att_sent), where bt_att_sent dereferences the channel and its ATT context (sys_slist_get(&att->reqs)). When a peer disconnects while an ATT PDU (a server notification/indication or any response) is still in flight in the controller TX path, L2CAP tears the channel down in l2cap_chan_del(): it runs the disconnected callback and then the released callback (bt_att_released), which frees the channel slab slot. Because the in-flight buffer is held by the connection TX path rather than the channel's own queue, its deferred destroy work can run after the channel has been freed. The att_on_sent_cb guard intended to drop the stale callback itself dereferences meta->att_chan, which is now a dangling pointer into a freed (and possibly reused) slab slot. A remote peer with an ATT connection can drive this by disconnecting during routine ATT traffic; no pairing or user interaction is required to reach the ATT bearer. The result is a use-after-free read/write of freed channel memory, reliably crashing the Bluetooth host (denial of service) and, because the channel slab slot may be reused, potentially corrupting live memory. The fix makes bt_att_released() NULL the att_chan field of every tx_meta_data_storage[] entry still referencing the channel before freeing it, so the deferred guard observes a NULL pointer and drops the callback. Teardown and the destroy work both run on the cooperative system workqueue, so the array update is serialized and needs no lock.	7.1	More Details
CVE-2026-17811	Use after free in ANGLE in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	7.1	More Details
CVE-2026-55502	Cloudreve is a self-hosted file management and sharing system. Prior to 4.17.0, POST /api/v4/admin/policy/oauth/signin requires only Admin.Read even though GetOauthRedirectService persists caller-supplied OneDrive secret and app_id values, allowing an OAuth token without Admin.Write to modify storage policy credentials. The route is inside the admin group that requires Admin.Read, but it does not add the local Admin.Write guard used by sibling policy mutation routes. Its handler persists attacker-supplied secret and app_id values into the selected OneDrive storage policy before returning an OAuth URL. This issue is fixed in version 4.17.0.	7.1	More Details
CVE-2026-70485	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.0 until 0.11.0, Open WebUI checked whether a user-supplied URL destination was globally routable by applying ipaddress.is_global to the literal IPv6 address without examining IPv4 addresses embedded in transition encodings. On a deployment with a NAT64 gateway, any verified user could wrap an internal or cloud-metadata IPv4 address in the NAT64 well-known prefix, pass the filter, and receive the internal response body through RAG URL ingestion, URL-to-markdown conversion, or web-search content retrieval. This issue is fixed in 0.11.0.	7.1	More Details
CVE-2025-71403	better-auth versions before 1.1.20 contain a bypass vulnerability in trustedOrigins validation logic affecting absolute URLs and wildcard domains. Attackers can construct malicious callbackURL parameters that pass origin checks and trigger open redirects to steal sensitive tokens for account takeover.	7.1	More Details
CVE-2026-17993	Race in Updater in Google Chrome on Windows prior to 151.0.7922.72 allowed a local attacker to perform privilege escalation via a malicious file. (Chromium security severity: Low)	7.0	More Details
CVE-2026-67326	GitPython before 3.1.50 fails to validate newline characters in the section parameter of config_writer(), allowing attackers to inject arbitrary section headers into .git/config. Attackers can inject newlines to create a forged [core] section with hooksPath pointing to attacker-controlled directories, achieving remote code execution when git hooks are triggered.	7.0	More Details
CVE-2026-18718	Ghidra contains an arbitrary code execution vulnerability in the Swift demangler analyzer that allows an attacker to execute arbitrary binaries by supplying a malicious Ghidra project with a crafted Swift tool directory path. When a victim opens the attacker-supplied project, SwiftDemanglerAnalyzer restores the persisted Swift binary directory from project state and SwiftNativeDemangler executes the resolved binary without integrity or signature verification, causing attacker-controlled executables to run under the Ghidra process user with no prompt or confirmation.	7.0	More Details

CVE-2026-10848	The OCPP 1.6 client in subsys/net/lib/ocpp parsed inbound WAMP RPC frames in parse_rpc_msg() (subsys/net/lib/ocpp/ocpp_j.c) using a hand-rolled helper, extract_string_field(), that copied the message's uid and action fields with strncpy(out_buf, token + 1, outlen - 1) and then scanned the result with strchr(out_buf, '"'). Because strncpy does not NUL-terminate the destination when the source is at least outlen - 1 (127) bytes long, the subsequent strchr reads past the 128-byte destination buffer into adjacent stack memory; if a " byte is found beyond the buffer, a one-byte out-of-bounds NUL write also occurs. A related defect in extract_payload() runs strchr/strrchr over the receive buffer, which may not be NUL-terminated when a maximal-length frame fills it. The parsed bytes come directly from the OCPP central-system server over a websocket: the reader thread fills recv_buf via websocket_recv_msg() and calls parse_rpc_msg() on each inbound DATA frame (subsys/net/lib/ocpp/ocpp.c). A malicious or compromised central server, or an on-path attacker (OCPP is commonly deployed over plain ws://), can send an RPC frame whose uid or action field is 127+ bytes with no closing quote, triggering the out-of-bounds access. The primary impact is a remotely triggerable denial of service: the unbounded scan can fault on an unmapped page, and the stray NUL write can corrupt adjacent stack state. The over-read data is not reflected to the peer, so disclosure is limited. The feature is EXPERIMENTAL and must be explicitly enabled (CONFIG_OCPP). The fix replaces the manual parser with the bounds-respecting json_mixed_arr_parse() and copies the extracted uid with an explicitly NUL-terminated buffer, eliminating both over-reads.	7.0	More Details
CVE-2026-69097	GitPython before 3.1.53 fails to properly escape section names in git config files, allowing attackers to inject arbitrary configuration directives through malicious submodule names. Attackers can inject core.sshCommand or other dangerous config keys into the victim's .git/config via create_submodule or clone_from operations, achieving remote code execution when git performs ssh operations.	7.0	More Details
CVE-2026-18605	A security flaw has been discovered in CheckMAL AppCheck Pro 3.1.43.10. Affected is an unknown function in the library AppCheckD.sys of the component Kernel Mini-Filter Driver. Performing a manipulation results in uncontrolled search path. The attack requires a local approach. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.0	More Details
CVE-2026-40272	Improper Input Validation in the decode() function of the traceparser library could allow an attacker with a corrupted kernel trace event log (.kev) file, to execute arbitrary code or cause a crash in processes that use libtraceparser in QNX hosts or targets.	7.0	More Details
CVE-2026-16293	The PowerPress Podcasting plugin by Blubrry WordPress plugin before 11.16.11 does not sanitise and escape some of its Podcast Episode settings, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	6.8	More Details
CVE-2026-13605	The PhotoSwipe WordPress plugin through 4.1.1.1 uses the title attribute of author-supplied link markup as a lightbox caption that is written into the page DOM without escaping. Because the title attribute survives the post-content sanitization applied to users who lack the unfiltered_html capability, an authenticated user with Author-level access can store a JavaScript payload that executes in the browser of any visitor, including an administrator, who clicks the link.	6.8	More Details
CVE-2026-17919	Insufficient policy enforcement in Enterprise in Google Chrome on Mac prior to 151.0.7922.72 allowed a local attacker to perform privilege escalation via physical access to the device. (Chromium security severity: Low)	6.8	More Details
CVE-2026-18654	Key exchange without entity authentication in the EMR SSH helper commands in Amazon AWS CLI before 1.45.28 and AWS CLI v2 before 2.35.3 might allow man-in-the-middle attackers to intercept SSHsessions and file transfers via network positioning between the client and the EMR cluster endpoint. To remediate this issue, users should upgrade to AWS CLI v1 1.45.28 or later, or AWS CLI v2 2.35.3 or later.	6.8	More Details
CVE-2026-14833	The Lightbox with PhotoSwipe WordPress plugin before 5.9.0 does not sanitise or escape a link data attribute before rendering it into the image lightbox caption in the browser, allowing users with author-level access and above (who lack the unfiltered_html capability) to store JavaScript that runs when a visitor or administrator opens the lightbox.	6.8	More Details
CVE-2026-	Vendure through 3.7.1, fixed in commit f67ef5f, contains a cross-channel authorization bypass vulnerability in stock-location.service.ts and asset.service.ts update methods that allows channel-scoped administrators to modify other tenants' data. Attackers can supply global IDs of	6.8	More Details

67347	StockLocation or Asset entities from different channels to overwrite inventory locations or catalog assets belonging to other tenants without proper channel isolation validation.		
CVE-2026-14939	The Visualizer WordPress plugin before 4.0.6 does not restrict a user-supplied URL to safe address ranges before fetching it server-side, allowing users with Contributor-level access and above to perform Server-Side Request Forgery against link-local instance-metadata endpoints. As the fetched response is returned in the reply, the attack is non-blind, enabling retrieval of cloud instance metadata (including IAM credentials) on cloud-hosted sites.	6.8	More Details
CVE-2026-46678	Pydantic AI is a Python agent framework for building Generative AI applications. In versions 1.56.0 through 1.98.0, when an application opts a URL into force_download='allow-local' (disabling the default block on private/internal IPs), the cloud-metadata blocklist could be bypassed by encoding the metadata IP in an IPv6 transition form (IPv4-mapped IPv6, 6to4, or NAT64), exposing cloud IAM short-term credentials on dual-stack or translated networks. This is an incomplete fix of GHSA-2jrp-274c-jhv3 / CVE-2026-25580, whose remediation did not hold for IPv6-encoded forms of the metadata IPs. An application is affected only if it explicitly opts a FileUrl (ImageUrl, AudioUrl, VideoUrl, DocumentUrl) into force_download='allow-local' on a URL influenced by untrusted input; it is not affected when using bundled integrations to ingest user input (Agent.to_web / clai web, VercelAIAdapter, AGUIAdapter / Agent.to_ag_ui), since they do not propagate force_download from external data, nor when downloading only from developer-controlled URLs. This issue has been fixed in version 1.99.0.	6.8	More Details
CVE-2026-54249	Pydantic AI is a Python agent framework for building Generative AI applications. In versions 1.65.0 through 1.105.0, and 2.0.0b1 through 2.0.0b5, a client that submits message history to a Pydantic AI UI adapter (such as the Vercel AI adapter) can reference arbitrary files in the application's model-provider or cloud-storage account. While file URL parts are validated against a scheme allowlist, UploadedFile references — which point to a file by provider file ID or cloud-storage URI (e.g. s3://..., gs://...) — were forwarded without validation. Because the provider resolves an UploadedFile using the server-side identity (IAM role, service account, or provider API key) rather than the client's, an attacker can craft message history to make the server read objects from its own account or other tenants, given a referenceable identifier. Exploitation requires a valid file identifier, which is not always unguessable depending on how the application names objects. This issue has been fixed in versions 1.106.0 and 2.0.0b6.	6.8	More Details
CVE-2026-18382	A flaw was found in koku-metrics-operator. The operator's CostManagementMetricsConfig custom resource allows a user able to edit the CR to specify an arbitrary OAuth token endpoint. When authentication.type is set to service-account, the operator sends the tenant's Red Hat SSO client_id and client_secret to this user-controlled URL, allowing the attacker to obtain the credentials.	6.8	More Details
CVE-2026-18214	Keycloak allows users to log in using Google accounts and can be configured to only allow users from specific Google Workspace domains. A flaw was found where the token exchange feature, which allows swapping a Google token for a Keycloak token, does not check these domain restrictions. This means an attacker with a valid Google account from a different domain could bypass the security check and gain access to the Keycloak realm.	6.8	More Details
CVE-2026-16069	The Brizy WordPress plugin before 2.8.19 does not sanitize or escape featured-image focal-point coordinates submitted through one of its AJAX actions before storing them and later echoing them into HTML attributes in the post editor's Featured Image meta box, allowing users with the Contributor role or above to inject arbitrary web scripts that execute in the session of a higher-privileged user who opens the post for review.	6.8	More Details
CVE-2026-18215	Keycloak provides a way to let users log in using Microsoft accounts while restricting access to a specific organization (tenant). A flaw was discovered where this restriction is ignored when using the token exchange feature. This means an attacker with a valid Microsoft token from a completely different organization could gain access to the Keycloak realm, potentially accessing sensitive data or performing unauthorized actions.	6.8	More Details
CVE-2026-14872	The Database for Contact Form 7, WPforms, Elementor forms WordPress plugin before 1.5.5 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL Injection exploitable by users granted a specific capability which is limited to administrators by default but can be delegated to lower privileged roles.	6.8	More Details
CVE-2026-	The Element Pack Addons for Elementor WordPress plugin before 8.7.13 does not sanitize option values passed through certain data attributes before a bundled front-end library re-parses and renders them in the browser, allowing users with contributor-level access or higher to inject	6.8	More Details

14817	arbitrary JavaScript that executes in the session of any visitor who views the affected content.		
CVE-2026-66313	Origin validation error in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform tampering locally.	6.8	More Details
CVE-2026-67311	Budibase before 3.38.1 contains a server-side request forgery vulnerability in the REST datasource integration that fails to validate HTTP redirects against the IP blacklist. Attackers with Builder role can configure a REST datasource pointing to an external server that returns a redirect to internal IP addresses, bypassing blacklist protection to access cloud metadata endpoints and internal services.	6.8	More Details
CVE-2026-65834	Capsule is a multi-tenancy and policy-based framework for Kubernetes. Prior to 0.13.8, CapsuleConfiguration.Spec.NodeMetadata.ForbiddenLabels.Regex and CapsuleConfiguration.Spec.NodeMetadata.ForbiddenAnnotations.Regex were not validated by the configuration admission webhook, allowing a Cluster Admin to store a malformed regex that later reached regexp.MustCompile in pkg/api/forbidden_list.go through internal/webhook/node/user_metadata.go and crashed the node admission webhook on Node create, update, or patch requests. This issue is fixed in version 0.13.8.	6.8	More Details
CVE-2026-70620	Odysseus before commit 87babb5 contains a server-side request forgery vulnerability that allows admin-privileged attackers to direct the server to probe internal network resources by supplying arbitrary URLs to the embedding endpoint configuration without scheme, host, IP range, or DNS rebind validation. Attackers can submit loopback addresses, RFC 1918 ranges, or link-local addresses through the embedding endpoint API to partially read responses from cloud instance metadata services, internal APIs, and other hosts reachable from the server.	6.8	More Details
CVE-2026-15153	The WP Hotel Booking WordPress plugin before 2.3.2 does not sanitise and escape a search parameter on an administrative listing before using it in a SQL query, allowing users holding the WP Hotel Booking WordPress plugin before 2.3.2's booking-management roles to perform SQL injection attacks.	6.8	More Details
CVE-2026-14318	The GiveWP WordPress plugin before 4.16.3 does not escape a donation-form template setting before outputting it in an HTML attribute, allowing users with the GiveWP Worker role and above to inject arbitrary web scripts that execute on the public donation form viewed by any visitor.	6.8	More Details
CVE-2026-9593	A vulnerability in the iDTM FDI allows an attacker with elevated privileges and access to the host system to enable the debug interface by placing a crafted file in the application directory, potentially resulting in unauthorized access to connected devices and exposure, modification, or disruption of device data or operation.	6.7	More Details
CVE-2026-24076	Memory Corruption when processing registry values with incorrect types using a direct query method.	6.7	More Details
CVE-2026-70594	Ghost is a Node.js content management system. From 2.2.0 until 6.54.1, Ghost Admin did not invalidate existing sessions on login which could have allowed for session fixation attacks. Successful exploitation would have required another vulnerability on the same domain where Ghost Admin was hosted. This issue is fixed in version 6.54.1.	6.7	More Details
CVE-2026-48121	@langchain/langgraph-checkpoint-mongodb provides a LangGraph.js CheckpointSaver implementation that uses MongoDB for storage. Versions 1.3.0 and below are vulnerable to NoSQL injection: checkpoint identifiers (thread_id, checkpoint_ns, checkpoint_id) from config.configurable are passed into MongoDB find() queries in MongoDBSaver.getTuple() without type enforcement. If an attacker supplies an object payload (such as MongoDB operators $gt or $ne) instead of a string, it can be interpreted as a query operator, bypassing thread scoping and leaking checkpoints, including pending writes, across tenants. Applications are at risk if they forward untrusted input into config.configurable without coercing it to strings or validating it against a schema, particularly in multi-tenant or user-isolated setups. Apps that only use server-issued, string-typed identifiers with schema validation rejecting non-string fields are not affected. This issue has been fixed in version 1.3.1.	6.7	More Details
CVE-2026-18571	A flaw was found in the user creation component of Keycloak when Fine-Grained Admin Permissions V2 (FGAP V2) is enabled. This issue allows a sub-administrator with permission to create users to add those users to any group, even groups the sub-administrator is not authorized to manage. This could lead to unauthorized access to sensitive information or elevated privileges	6.6	More Details

	for the newly created users.		
CVE-2026-70593	Ghost is a Node.js content management system. From 0.10.0 until 6.54.1, a vulnerability in custom themes allowed a staff user to write files outside of the uploads directory. This could be used to alter the behavior of the installation through custom theme upload path traversal in LocalStorageBase and theme storage name handling. This issue is fixed in version 6.54.1.	6.6	More Details
CVE-2026-47619	NVIDIA Dynamo for Linux examples and recipes contain a vulnerability where an attacker could cause a system failure. A successful exploit of this vulnerability might lead to code execution, data tampering, denial of service, and information disclosure.	6.6	More Details
CVE-2026-65835	Capsule is a multi-tenancy and policy-based framework for Kubernetes. From 0.13.0 until 0.13.8, after the incomplete CVE-2026-22872 fix, TenantResource RawItems and Generators in internal/controllers/resources/collect.go, including handleRawItem and handleGeneratorItem, did not apply the ResourceReference.LoadResources and IsNamespacedGVK cluster-scoped resource rejection guard used by NamespacedItems, allowing a Tenant Owner to create cluster-scoped resources such as ClusterRole or ValidatingWebhookConfiguration through the cluster-admin controller client. This issue is fixed in version 0.13.8.	6.6	More Details
CVE-2026-44105	The credentials for the local user "user-app" may be exposed in log files, potentially enabling a low-privileged local attacker with access to the logs to authenticate via SSH as the limited user "user-app". Charging could be interrupted.	6.6	More Details
CVE-2026-67438	OliveTin gives access to predefined shell commands from a web interface. From 3000.2.0 until 3000.17.0, the service/internal/executor/arguments.go checkShellArgumentSafety function does not treat regex: custom argument types as unsafe for Shell mode actions, allowing values that pass typeSafetyCheckRegex to be interpolated by wrapCommandInShell into an sh -c command string and enabling OS command injection. This issue is fixed in version 3000.17.0.	6.6	More Details
CVE-2026-17605	The Payment forms, Buy now buttons, and Invoicing System | GetPaid plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.8.56 via the getpaid_payment_form_element function. This makes it possible for authenticated attackers, with administrator-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	6.6	More Details
CVE-2026-16062	The Event Booking Manager for WooCommerce WordPress plugin before 5.3.7 does not prevent the deserialization of user-controlled input in some of its event content fields, allowing users with Contributor-level access and above to inject PHP objects. No POP chain is present in the Event Booking Manager for WooCommerce WordPress plugin before 5.3.7 itself, but if one is present via another installed Event Booking Manager for WooCommerce WordPress plugin before 5.3.7 or , this could lead to actions such as arbitrary file deletion, sensitive data retrieval, or remote code execution. This is an incomplete fix of the Event Booking Manager for WooCommerce WordPress plugin before 5.3.7's earlier object-injection advisories.	6.6	More Details
CVE-2026-40717	Dell Monitor driver, version 1.0.0.0, contains 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.	6.6	More Details
CVE-2026-16057	The Contest Gallery WordPress plugin before 30.0.7 does not perform per-object capability or nonce checks in one of its post-deletion handlers, gating it only by a coarse role-membership test, which allows any Author-level or higher user to permanently delete arbitrary posts, pages, and other content they do not own.	6.5	More Details
CVE-2026-15254	The Simply Schedule Appointments WordPress plugin before 1.6.12.11 does not perform a capability check on an administrative appointment-listing shortcode, and its per-user result scoping fails open for non-staff users, allowing users with the Contributor role and above to disclose all customers' appointment records, including names, email addresses, phone numbers and notes, across the whole site.	6.5	More Details
CVE-2026-16563	The Academy LMS WordPress plugin before 3.8.3 does not verify course enrollment or lesson publication status when returning a single lesson through its REST API, allowing users with a self-service student (Subscriber-level) account to disclose the content of arbitrary lessons, including lessons of paid courses they are not enrolled in and unpublished (draft, pending, private) lessons.	6.5	More Details
CVE-	In wlan STA FW, there is a possible system becoming unresponsive due to logging. This could lead		More

2026-20482	to remote (proximal/adjacent) denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00486814; Issue ID: MSV-6824.	6.5	Details
CVE-2026-17348	In SERVER mode, pgAdmin 4 enforces authentication per route via the @pga_login_required decorator; the application's before_request hook only handles desktop-mode auto-login and the Kerberos/Webserver-auth redirect, so any route shipped without the decorator is reachable without authentication (CWE-306). This is the same defect class previously fixed as CVE-2026-12046 (the sqleditor close/update_connection routes). A follow-up sweep, prompted by a report describing an incomplete fix for CVE-2026-12046, found further routes missing @pga_login_required: the Constraints blueprint's nodes and proplist (object listing) routes and its delete route (a state-mutating DELETE that removes table constraints); preferences.get_all_cli (GET, discloses all CLI-settable preference values); debugger.close (DELETE); and schema_diff.close (DELETE). An unauthenticated network client could therefore enumerate constraint metadata, delete table constraints, read preference values, and force-close debugger or schema-diff sessions belonging to other users, without ever authenticating. Fix adds the missing @pga_login_required decorator (and the corresponding import to the Constraints module) to each of these routes. The change is decorator-only; no behavioral changes to the underlying handlers. This issue affects pgAdmin 4 in SERVER mode: the Constraints and Debugger routes from 1.0, the Schema Diff close route from 4.18, and preferences.get_all_cli from 8.2, all before 9.17.	6.5	More Details
CVE-2026-20464	In hevc decoder, there is a possible out of bounds write due to an integer overflow. This could lead to remote escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11104718; Issue ID: MSV-8297.	6.5	More Details
CVE-2026-47620	NVIDIA Dynamo for Linux contains a vulnerability where an attacker could cause a race condition in the LoRA manager singleton initialization. A successful exploit of this vulnerability might lead to data tampering and denial of service.	6.5	More Details
CVE-2026-54364	CentreStack before 17.4 contains a session variable injection vulnerability that allows unauthenticated attackers to inject arbitrary session variables by embedding newline and tab characters into a crafted AccountName parameter posted to the SelectProvider.aspx endpoint. Attackers can exploit the lack of input sanitization in the custom session serialization format to inject a resellerid session variable, bypassing the IsValidRSession authentication check and gaining unauthorized access to management pages.	6.5	More Details
CVE-2026-68582	Vikunja versions >= 0.24.0 and <= 2.3.0 contain a broken object level authorization (BOLA) vulnerability in the task-collection endpoint (GET /api/v1/projects/{project}/views/{view}/tasks). The endpoint loads the requested project view from the URL path without verifying the caller is authorized for it. For a link-share token holder, the task scope is pinned to the share's own project, but the view is taken from the attacker-controlled path and never re-validated. As a result, a holder of any project share link can read any other tenant's kanban bucket records — bucket titles and the full created_by user object (username, name, id) — for every view in the instance. The same missing pre-authorization view load also creates a project/view-ID existence oracle (404 vs. non-404) usable by link shares and ordinary authenticated users. Task contents remain constrained to the share's own project and are not disclosed. Fixed in 2.4.0.	6.5	More Details
CVE-2026-47621	NVIDIA Dynamo for Linux contains a vulnerability where an attacker could cause a race condition in the LoRA manager singleton initialization. A successful exploit of this vulnerability might lead to denial of service and data tampering.	6.5	More Details
CVE-2026-70489	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.0 until 0.11.0, automation recurrence parsing in backend/open_webui/utils/automations.py anchored minutely and hourly rules at a fixed date of 2000-01-01 and then walked forward one interval at a time to find the next run. A single FREQ=MINUTELY rule enumerates roughly a quarter-century of occurrences synchronously on the event loop that also serves scheduler, HTTP, and WebSocket traffic, and the scheduler recomputes the next run for every claimed row on each poll. This causes availability impact for every other user of the instance. This issue is fixed in 0.11.0.	6.5	More Details
	Zephyr's Bluetooth host declares a GATT characteristic as two consecutive attributes: a Characteristic Declaration whose permission is hard-coded to BT_GATT_PERM_READ, and a Characteristic Value attribute that carries the application-specified security permissions (e.g. BT_GATT_PERM_READ_ENCRYPT / READ_AUTHEN / READ_LESC). The public notify and indicate APIs explicitly accept either attribute, and passing the declaration is the documented, common idiom. Before sending each notification or indication, the host re-checks link security with		

CVE-2026-2411	bt_gatt_check_perm() against params->attr in gatt_notify(), gatt_indicate(), and gatt_notify_multiple_verify_params() (subsys/bluetooth/host/gatt.c). When the application passed the Characteristic Declaration attribute, the host correctly redirected the value handle but left params->attr pointing at the declaration, so the security check evaluated the declaration's permissions (no security required) instead of the value's. As a result the encryption/authentication/LESC requirement configured on the characteristic value was skipped. The Notify-Multiple path additionally used a mask that omitted the LE Secure Connections requirement. A remote peer triggers the disclosure by connecting (optionally without pairing or encryption) and writing the Client Characteristic Configuration descriptor to enable notifications or indications, causing the server to emit the protected value over a link that has not reached the required security level. The impact is information disclosure / access-control bypass for characteristic values the application intended to expose only over a secured link; exposure depends on the application declaring encrypt/authen-required notify/indicate characteristics and on the CCC being writable at a lower security tier. There is no memory-safety or availability impact. The fix adds bt_gatt_attr_resolve_value(), which maps a declaration attribute to the following value attribute before the permission check, and switches the Notify-Multiple path to the full BT_GATT_PERM_READ_ENCRYPT_MASK so the LESC requirement is also enforced.	6.5	More Details
CVE-2026-6453	The CubeWP Framework plugin for WordPress is vulnerable to SQL Injection in all versions up to and including 1.1.30. This is due to insufficient input sanitization in the cubewp_remove_relation() AJAX function, specifically the use of wp_unslash() on the relation_id parameter before interpolating it directly into a raw SQL query without using $wpdb->prepare(). The wp_unslash() call explicitly removes the backslash escaping that WordPress's wp_magic_quotes() adds to all $_POST data, neutralizing the only layer of SQL injection protection. The sanitize_text_field() function applied afterward offers no SQL protection. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries to the existing query.	6.5	More Details
CVE-2026-13389	The webtoffee-cookie-consent WordPress plugin before 3.5.3 does not perform authorization checks on several of its REST API routes, allowing unauthenticated attackers to export and delete stored visitor consent records, create posts, and modify the webtoffee-cookie-consent WordPress plugin before 3.5.3's licensing state.	6.5	More Details
CVE-2026-67337	better-auth versions before 1.4.9 contain a two-factor authentication bypass vulnerability when session.cookieCache is enabled. Attackers with valid primary credentials can access authenticated routes without completing second-factor verification by exploiting premature session caching.	6.5	More Details
CVE-2026-17580	The Advanced Views – Display Custom Fields (ACF, Pods, MetaBox), Posts, CPT and Woo Products anywhere in Gutenberg, Elementor, Divi, Beaver... plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.9.1 via the register_rest_routes. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract sensitive admin-authored editor content — including template markup, CSS code, JavaScript code, and PHP controller variables — for any Layout or Post Selection post on the site.	6.5	More Details
CVE-2026-16087	The Icegram Engage – Popups, Optins, CTAs & Lead Generation plugin for WordPress is vulnerable to second-order SQL Injection via 'messages[][id]' Parameter in all versions up to, and including, 3.1.42 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The injection is second-order: the malicious id value is first persisted to post meta via the save_campaign_preview() AJAX action (gated by a nonce check and edit_post capability, requiring Editor-level access or above), and only executed as SQL when a subsequent preview request triggers get_message_data() to interpolate the stored value directly into a SQL IN() clause without $wpdb->prepare() or integer casting.	6.5	More Details
CVE-2026-15382	The Ultimate Addons for WPBakery Page Builder WordPress plugin before 3.21.4 does not perform a capability or nonce check before deleting a site's custom-uploaded icon font packs, allowing unauthenticated attackers to permanently delete all of a site's custom icon fonts with a single request.	6.5	More Details
CVE-2026-70493	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.6 until 0.11.0, the built-in knowledge search path in backend/open_webui/tools/knowledge_fs.py and backend/open_webui/tools/builtin.py let a chat participant choose a pattern used to grep knowledge files. Patterns containing regex metacharacters were compiled with Python's backtracking re engine and run against every line of every reachable file with no time limit, so a	6.5	More Details

	crafted pattern such as (x|x)*y and one matching uploaded file line can pin one CPU core and block the event loop. This causes availability impact for every other user of the affected worker. This issue is fixed in 0.11.0.		
CVE-2026-70491	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. In 0.10.2 and earlier, the GET /api/v1/tools/, GET /api/v1/tools/list, and GET /api/v1/tools/id/{id} endpoints in backend/open_webui/routers/tools.py returned full Python tool source to authenticated non-admin read-only users. ToolResponse deliberately omitted source and specs, but ToolUserResponse permitted extra fields and handlers spread a full tool model dump into the response, re-admitting omitted fields. A non-admin with a read grant can obtain another user's server-side tool source, which commonly embeds hard-coded API keys, credentials, and internal service URLs. This issue is fixed in 0.11.0.	6.5	More Details
CVE-2026-44615	Path traversal vulnerability in Apache Zeppelin. When FileSystemNotebookRepo is configured, an authenticated attacker with permission to rename a note, or access to folder operations, could supply traversal segments in note or folder paths. Zeppelin composed these values into filesystem paths using the server's filesystem or Hadoop identity without ensuring that the result remained under the configured notebook directory. This could allow notebook files or directories to be moved, written, or deleted outside the notebook root. This issue affects Apache Zeppelin versions 0.9.0 through 0.12.0. Users are recommended to upgrade to version 0.12.1, which fixes this issue.	6.5	More Details
CVE-2026-69702	SnailJob 1.7.0 contains a denial of service vulnerability in the FuryUtil.deserialize helper that allows authenticated attackers to crash the server by supplying a crafted Zstandard-compressed payload with an inflated frame_content_size field in the frame header. Attackers can store a base64-encoded Zstandard payload declaring an arbitrarily large decompressed size in a retry task argument, causing the JVM to attempt an unbounded array allocation and triggering an unrecoverable java.lang.OutOfMemoryError when the task is dispatched through the retry-task pipeline.	6.5	More Details
CVE-2026-14561	The Authora : Easy login with mobile number WordPress plugin before 1.7.7 does not keep its one-time login code confidential, returning the code and a valid verification token in the response of an unauthenticated action, allowing unauthenticated attackers to log in as any user whose registered mobile number they know (including administrators) or to create arbitrary accounts.	6.5	More Details
CVE-2026-14315	The Pixel Tag Manager for WooCommerce WordPress plugin before 2.2.1 does not perform an authorization check on one of its AJAX actions, allowing unauthenticated users to submit forged e-commerce conversion events to the site's configured server-side advertising conversion APIs using the site's stored credentials.	6.5	More Details
CVE-2026-13329	The Buckaroo Woocommerce Payments Plugin WordPress plugin before 4.9.0 does not perform any capability check or nonce validation on an AJAX action that processes payment capture refunds, allowing any authenticated user, including Subscribers, to trigger refunds against captured orders.	6.5	More Details
CVE-2026-18573	A flaw was found in the keycloak-services component of Keycloak, which is used for managing authentication and authorization flows. The issue occurs when a realm administrator configures client policies to enforce specific authentication requirements on confidential clients. Due to improper evaluation of the client state during an update operation, an attacker with client management permissions can bypass these security policies by first creating a public client and then updating it to a confidential client with weaker authentication. This can result in the persistence of clients that do not comply with the intended security hardening of the realm.	6.5	More Details
CVE-2026-45377	Decidim is a participatory democracy framework. Prior to 0.30.9, from 0.31.0 before 0.31.5, and in 0.32.0.rc1 before 0.32.0.rc2, the normal download_your_data flow requires the requester to be logged in as the export owner, but the resulting Active Storage blob redirect URL can be replayed without authentication by anyone who obtains it. This is because Decidim::DownloadYourDataController#download_file authenticates the export owner but redirects to a signed Active Storage blob URL that is no longer bound to the owner session. This issue is fixed in versions 0.30.9, 0.31.5, and 0.32.0.rc2.	6.5	More Details
CVE-2026-52371	A Server-Side Request Forgery (SSRF) in the xxl-job-admin/jobinfo/trigger component of xxl-job v3.4.0 allows authenticated attackers to scan resources via supplying a crafted HTTP request.	6.5	More Details
CVE-	A flaw was found in the PCP (Performance Co-Pilot) `pmproxy` service. A remote attacker can exploit a vulnerability in the `pmLogLoadInDom()` function by sending a specially crafted request.		

2026-16530	This bypasses a critical bounds check, which can lead to the `pmproxy` service crashing, causing a Denial of Service (DoS). Additionally, this flaw may enable the leakage of sensitive information from the system's memory.	6.5	More Details
CVE-2026-69704	Atals-Livre contains a SQL injection vulnerability that allows attackers to manipulate database queries by passing unsanitized input through a GET parameter to the supp() deletion helper function. Attackers can inject malicious SQL syntax via the vulnerable GET parameter to perform unauthorized database operations including data deletion and extraction.	6.5	More Details
CVE-2026-67292	FreeRDP before 3.29.0 contains a buffer over-disclosure vulnerability in the gateway WebSocket transport (libfreerdp/core/gateway/websocket.c). The client's Pong reply reuses a fixed 1024-byte response stream whose length is not sealed to the actual received Ping payload, so a malicious gateway/WebSocket peer sending a non-empty Ping control frame causes the client to reply with an overlong Pong that discloses bytes beyond the received payload (the peer receives the masking key and can unmask the reply). A zero-length Ping reaches an assertion and terminates the client (denial of service).	6.5	More Details
CVE-2026-18572	Keycloak provides authorization services that allow administrators to restrict access to resources based on time policies (for example, only allowing access during business hours). A flaw was discovered where a user can include a fake time value in their authorization request that overrides the actual server time. This allows the user to bypass these time-based restrictions and access protected resources at unauthorized times.	6.5	More Details
CVE-2026-68501	Sylius Mollie Plugin provides Mollie payment integration for Sylius applications. Prior to 2.2.8, 3.2.4, and 3.3.1, Sylius Mollie Plugin's GET /{_locale}/thank-you PageRedirectController::thankYouAction and GET /{_locale}/get-code QrCodeAction::fetchQrCodeFromOrder endpoints look up sequential orderId values without ownership or session checks, exposing order tokenValue values that can be used with GET /{_locale}/register-after-checkout/{tokenValue} to view customer first name, last name, and email. This issue is fixed in 2.2.8, 3.2.4, and 3.3.1.	6.5	More Details
CVE-2026-63563	Sharp and Toshiba Tec MFPs (multifunction printers) for a certain market have been shipped with the user authentication feature disabled in the initial configuration. When used with the initial configuration, the address book editing and a range of features related to Document Filing can be accessed without user authentication. Products intended for the Japanese market are not affected.	6.5	More Details
CVE-2026-70371	Koha's reports/issues_avg_stats.pl builds dynamic SQL in sub calculate by concatenating several user-controlled request parameters directly into the query string. The Line and Column parameters are not validated against any whitelist and land verbatim in identifier positions (SELECT DISTINCTROW, GROUP BY, ORDER BY), and each Filter slot is concatenated raw into single-quoted LIKE, BETWEEN, and comparison fragments with no bound parameters. An authenticated staff user holding the reports module permission can inject arbitrary SQL and read any table reachable by the Koha database user, including borrowers (password hashes, two-factor secrets, personal data), api_keys, and sessions.	6.5	More Details
CVE-2026-70370	Koha's reports/catalogue_stats.pl builds dynamic SQL in sub calculate by interpolating the user-controlled Line and Column request parameters directly into identifier positions of the query (SELECT DISTINCTROW, GROUP BY, ORDER BY) with no whitelist validation. When Line contains itemcallnumber and the cotedigits parameter is truthy, cotedigits is additionally concatenated raw as the numeric argument of a LEFT() call. An authenticated staff user holding the reports module permission can inject arbitrary SQL and read any table reachable by the Koha database user, including borrowers (password hashes, two-factor secrets, personal data), api_keys, and sessions.	6.5	More Details
CVE-2026-70369	Koha's reports/acquisitions_stats.pl builds its per-cell statistics query in sub calculate by interpolating the user-controlled Filter request parameters directly into WHERE fragments covering aqbasket.closedate, aqorders.datereceived, aqbooksellers.name, items.homebranch, items.ccode, biblioitems.itemtype, aqbudgets.budget_code, aqorders.sort1, and aqorders.sort2. The statement is prepared and executed with no bound parameters. An authenticated staff user holding the reports module permission can inject arbitrary SQL and read any table reachable by the Koha database user, including borrowers (password hashes, two-factor secrets, personal data), borrower_password_recovery, api_keys, and sessions.	6.5	More Details
CVE-2026-	The GOOSE parser contains an off-by-one boundary-handling flaw that can be triggered by a single unauthenticated Layer-2 multicast frame on the process bus. When specific GOOSE message fields are processed, the parser advances its internal buffer position incorrectly,	6.5	More Details

66369	resulting in a heap out-of-bounds read. On affected platforms, this condition reliably terminates the subscriber process and causes a denial-of-service.		
CVE-2026-18809	Information disclosure in Firefox for Android and Firefox Focus for Android. This vulnerability was fixed in Firefox 153.0.3.	6.5	More Details
CVE-2026-66364	The GOOSE payload parser contains a boundary handling flaw that can be triggered by a single unauthenticated Layer 2 multicast frame on the process bus. When processing specific payload fields, an attacker controlled inner element length may exceed its enclosing length, causing the parser to over read by one byte. This out-of-bounds read reliably terminates the subscriber process, resulting in a denial-of-service condition.	6.5	More Details
CVE-2026-18737	Shlink contains a blind SQL injection vulnerability that allows any authenticated API key holder to inject arbitrary SQL fragments by supplying an unvalidated direction value in the orderBy query parameter of the tag statistics endpoint. Attackers can craft a malicious direction string containing SQL subqueries that flows unsanitized into a Doctrine QueryBuilder ORDER BY clause, enabling time-based, boolean-oracle, and error-based extraction of sensitive data including long URLs, visitor records, IP addresses, geolocation data, user agents, and hashed API key secrets from any tenant.	6.5	More Details
CVE-2026-14465	Insufficient session expiration vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Reusing Session IDs (aka Session Replay). This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	6.5	More Details
CVE-2026-10700	IBM Langflow OSS 1.0.0 through 1.8.4 contains multiple broken access control vulnerabilities in its file handling API that allow unauthorized access to user files.The /api/v1/files/images/{flow_id}/{file_name} endpoint does not enforce authentication or authorization checks, allowing unauthenticated remote attackers to retrieve image files associated with any flow by specifying a valid flow_id and file_name.Additionally, the /api/v1/files/download/{flow_id}/{file_name} endpoint requires authentication but fails to properly validate ownership of the requested resource. As a result, an authenticated user can access files belonging to other users by supplying arbitrary identifiers, leading to an authorization bypass (IDOR).Successful exploitation may result in unauthorized disclosure of sensitive data, including files stored in private flows. This issue breaks tenant isolation in multi-user deployments.	6.5	More Details
CVE-2026-14194	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Path Traversal. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	6.5	More Details
CVE-2026-66349	The MMS server connection handler contains a flaw in its processing of BER-encoded request data. When an MMS confirmed request PDU containing an extended BER tag is received over an established session, the decoder may advance its internal buffer incorrectly due to a missing bounds check. This results in a one byte heap out-of-bounds read and causes the MMS service process to terminate, leading to a denial-of-service condition.	6.5	More Details
CVE-2026-15974	SGLang contains an SSRF and local file read in the multimodal generation endpoint /v1/chat/completions due to unsanitized image_url, allowing access to internal metadata, secrets, and services.	6.5	More Details
CVE-2026-14816	The GDPR Framework By Data443 WordPress plugin before 2.4.0 does not properly verify authorization or the identity of the data subject when recording cookie-consent choices and privacy requests, allowing unauthenticated attackers to forge consent records for arbitrary email addresses and to flood the site's privacy-request queue with arbitrary entries.	6.5	More Details
CVE-2026-65421	The MMS BER decoder contains a flaw in decoding fixed-width BER fields (boolean/integer): an attacker-supplied length value is not validated, causing a read past the end of a heap buffer. This leads to termination of the MMS service process and a denial-of-service condition.	6.5	More Details
CVE-2026-63550	The MMS BER decoder contains a boundary-handling flaw in the processing of certain fields within confirmed-request messages. When a crafted BER-encoded element is received over an established MMS session (TCP port 102), the decoder may advance its internal read position incorrectly, leading to a heap out-of-bounds read. This condition causes the MMS handling process to terminate unexpectedly, resulting in a denial-of-service.	6.5	More Details
CVE-2026-	An improper authentication vulnerability in the "social_login.cgi" CGI program in Zyxel WAX650S firmware versions through 7.10(ABRM.4)C0 could allow an attacker on the WLAN to bypass	6.5	More Details

8508	captive portal authentication.		
CVE-2026-66326	Missing authorization in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	6.5	More Details
CVE-2026-63033	A crafted IEC 60870-5-104 I-frame with a declared object count exceeding what fits in the ASDU body causes InformationObject_ParseObjectAddress to read one byte past the end of the heap-allocated message buffer.	6.5	More Details
CVE-2026-61893	A crafted IEC 60870-5-104 I-frame with TypeID 104 (C_TS_NA_1) and an inflated object count causes TestCommand_getFromBuffer to read one byte past the end of the heap-allocated message buffer.	6.5	More Details
CVE-2026-56758	The ACSE layer contains a flaw in the processing of AARQ PDUs during MMS connection establishment. When parsing certain fields within the calling AP title, an attacker controlled length value of zero or one may cause the parser to read past the end of a heap buffer.	6.5	More Details
CVE-2026-64816	RapidRAW before 1.6.0 does not validate the lutPath field in preset files before passing it to File::open() in lut_processing.rs. On Windows, a UNC path in lutPath causes an outbound SMB connection to an attacker-controlled host, leaking the victim's NTLMv2 credentials. The vulnerable code path is reachable through two vectors: community presets fetched automatically from the remote preset repository when the victim opens the Community tab, and individual preset files imported directly by the victim via the preset import feature (handle_import_presets_from_file in file_management.rs). The second vector does not require control of the community preset repository and is triggered when a user imports a preset file shared through Discord, forums, or similar channels.	6.5	More Details
CVE-2026-66312	Buffer over-read in Microsoft Edge (Chromium-based) allows an authorized attacker to execute code over a network.	6.5	More Details
CVE-2026-66720	The GOOSE subscriber component improperly validates the UTC timestamp field in unauthenticated IEC 61850 GOOSE (EtherType 0x88B8) Layer-2 multicast messages. A specially crafted GOOSE frame containing an undersized timestamp field can trigger a heap out-of-bounds read during message processing, causing the process to crash and resulting in a denial-of-service condition.	6.5	More Details
CVE-2026-58139	The DuckDB AWS extension for DuckDB contains a security policy bypass vulnerability that allows any database user with SQL execution permissions to extract plaintext AWS credentials by calling the load_aws_credentials function with the redact_secret parameter set to false, circumventing the database-wide allow_unredacted_secrets=false policy. Attackers can invoke this single function to retrieve the underlying AWS credential chain including access_key_id, secret_access_key, session_token, and region in plaintext, which are immediately valid against AWS APIs and particularly impactful in managed environments where pg_duckdb is preloaded and an AWS credential chain such as IMDSv2, IRSA, ECS task role, or EC2 instance role is reachable.	6.5	More Details
CVE-2026-18208	A flaw was found in the OIDC token introspection endpoint of the keycloak-services component. Keycloak is an open-source identity and access management solution used to secure modern applications and services. The issue occurs when a confidential client, configured to receive signed JWT introspection responses, attempts to introspect a token issued for a different audience. Although the endpoint correctly identifies the token as inactive for that client, it still returns the full set of token claims within a signed JWT field. This allows an unauthorized client to bypass audience-based restrictions and access sensitive information contained in the token.	6.5	More Details
CVE-2026-70372	Koha's reports/bor_issues_top.pl builds dynamic SQL in sub calculate by concatenating several user-controlled request parameters directly into the query string. The Criteria parameter is only normalized by a table-name prefix and is never whitelisted, landing verbatim in identifier positions (SELECT DISTINCTROW, GROUP BY, ORDER BY); Filter values are concatenated raw into single-quoted LIKE, BETWEEN, and comparison fragments, and the Limit parameter is appended raw to a LIMIT clause. An authenticated staff user holding the reports module permission can inject arbitrary SQL and read any table reachable by the Koha database user, including borrowers (password hashes, two-factor secrets, personal data), api_keys, and sessions.	6.5	More Details
CVE-	A flaw was found in the group policy evaluation logic of Keycloak, an identity and access management solution. When a group policy is set to extend permissions to child groups, the		More

2026-18203	system incorrectly uses a simple text-based prefix check to verify group membership. This allows a user who belongs to a different group with a similar starting name to bypass security checks and gain unauthorized access to administrative functions or protected resources.	6.5	Details
CVE-2026-15209	The JS Help Desk WordPress plugin before 3.1.5 does not verify that the requesting user owns the ticket being loaded: a low-privileged authenticated user can supply another user's ticket ID and read that ticket's contents, including the reporter's PII and message body.	6.5	More Details
CVE-2026-14931	The JS Help Desk WordPress plugin before 3.1.4 grants a support-agent capability to the Contributor role on activation and does not perform a capability check on a user-listing handler, allowing Contributor-level users to enumerate the email addresses of all registered WordPress users.	6.5	More Details
CVE-2026-14834	The Mailgun for WordPress plugin before 2.2.1 does not perform any capability or nonce check on an unauthenticated AJAX action that adds subscribers to the site owner's configured email service mailing lists, allowing unauthenticated attackers to enrol arbitrary email addresses into those lists using the owner's stored API credentials.	6.5	More Details
CVE-2026-66314	Time-of-check time-of-use (toctou) race condition in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2026-69087	The Grav form plugin (getgrav/grav-plugin-form) before 9.1.13 contains an open redirect vulnerability. Since v9.1.11, the redirect process action evaluates user-supplied form data inside Twig expressions, and Grav::redirect() accepts external URLs without origin validation. When a form blueprint defines a redirect target such as redirect: "{{ form.value('next') }}" using an attacker-controllable field, an unauthenticated form submitter can supply a value like https://evil.com to cause a 302 redirect to an arbitrary external site, enabling phishing.	6.5	More Details
CVE-2026-14554	The Check & Log Email WordPress plugin before 2.0.15 does not properly sanitize and escape parameters before using them in SQL queries, allowing users with administrator privileges to perform SQL injection attacks.	6.5	More Details
CVE-2026-69092	Admidio versions before 5.0.11 contain a reflected cross-site scripting vulnerability in the SSO/SAML endpoint that echoes unencoded exception messages to the HTTP response. Unauthenticated attackers can inject arbitrary JavaScript through SAML Issuer elements or LightSaml library parameters to execute code in users' browsers and hijack sessions.	6.5	More Details
CVE-2026-24078	Information Disclosure when IPSec negotiation fails or is not established properly during NG-eCall SIP signaling.	6.5	More Details
CVE-2026-24077	Information Disclosure when processing wireless network channel switch information with improperly formatted length fields.	6.5	More Details
CVE-2026-68930	Russh is a Rust SSH client & server library. Prior to 0.62.5, russh dispatches channel-scoped Handler callbacks for recipient channel IDs that were never opened or confirmed in russh/src/server/encrypted.rs, server_read_authenticated, and the exec_request callback. Version 0.62.5 fixes the issue.	6.5	More Details
CVE-2026-67618	marimo before 0.23.15 contains a configuration injection vulnerability that allows notebook authors to exfiltrate operator API keys by embedding a malicious base_url in PEP-723 inline script metadata, which is merged into session configuration with higher precedence than the operator's own settings due to insufficient sanitization in sanitize_pyproject_dict. When an operator opens the crafted notebook and makes an AI request, marimo resolves the attacker-controlled base_url from the notebook config while falling back to the operator's OPENAI_API_KEY environment variable for authentication, transmitting the API key to the attacker-controlled endpoint without requiring any cell execution.	6.5	More Details
CVE-2026-67199	Perspective 5.0.0 contains a denial of service vulnerability that allows remote attackers to block the server event loop indefinitely by submitting a crafted expression containing unbounded for or while loop constructs in a TableMakeViewReq message. Attackers can embed an arbitrarily large iteration count in an expression column evaluated once per table row, causing the Tornado IOLoop to block without any iteration cap, deadline, or cancellation check, rendering the server unresponsive to all connected clients.	6.5	More Details

CVE-2026-15657	A vulnerability in the foreUP customer REST API allows any authenticated user to read cleartext payment-processor merchant credentials in the response body.	6.5	More Details
CVE-2026-55497	Cloudreve is a self-hosted file management and sharing system. Prior to 4.17.0, the built-in thumbnail and avatar image decoders limit compressed file size but do not limit decoded pixel dimensions, allowing an authenticated user to submit a small PNG, JPEG, or GIF that triggers an unbounded allocation and terminates the Cloudreve process through fatal out-of-memory behavior. This issue is fixed in version 4.17.0.	6.5	More Details
CVE-2026-18655	Improper restriction of intended endpoints in the RabbitMQ broker connection tools of the Amazon MQ MCP Server (awslabs.amazon-mq-mcp-server) before 2.0.24 may allow a remote unauthenticated actor (via prompt injection) to obtain Amazon MQ for RabbitMQ broker credentials or OAuth access tokens sent to a crafted endpoint controlled through a broker hostname introduced in the MCP client context. To remediate this issue, users should upgrade to version 2.0.24.	6.5	More Details
CVE-2026-70368	A stack-based out-of-bounds read vulnerability exists in the "s_vlog" function of stunnel, when handling oversized log messages via "vsnprintf". A remote attacker with network access to a stunnel service can send protocol inputs that trigger a log message longer than 1024 bytes, leading to an out-of-bounds stack read and a potential crash. In certain corner cases, the same vulnerability could be used to replace a series of trailing "\n" characters with "\0".	6.5	More Details
CVE-2026-70373	Koha's reports/issues_stats.pl (the circulation statistics report) builds its calculation query in sub calculate by concatenating several user-controlled request parameters directly into the SQL string. The PeriodTypeSel, PeriodDaySel, and PeriodMonthSel parameters are interpolated raw into single-quoted equality and function-comparison fragments, and the Filter slots plus the Line and Column identifiers are likewise interpolated with no whitelist and no placeholder binding. An authenticated staff user holding the reports module permission can inject arbitrary SQL and read any table reachable by the Koha database user, including borrowers (password hashes, two-factor secrets, personal data), api_keys, and sessions.	6.5	More Details
CVE-2026-44616	LDAP injection vulnerability in Apache Zeppelin. ActiveDirectoryGroupRealm constructed LDAP search filters without escaping user-controlled input, allowing an authenticated attacker to inject LDAP filter syntax through the user-search endpoint and potentially expose directory information. The role-lookup path was also affected after successful LDAP authentication. This issue affects Apache Zeppelin versions 0.6.0 through 0.12.0. Users are recommended to upgrade to version 0.12.1, which fixes this issue.	6.5	More Details
CVE-2026-44617	LDAP filter injection vulnerability in Apache Zeppelin. LdapRealm used RFC 4514 distinguished-name escaping when constructing LDAP search filters instead of RFC 4515 filter escaping, leaving special filter characters insufficiently escaped. This is an incomplete fix of CVE-2024-31867. This issue affects Apache Zeppelin versions 0.11.1, 0.11.2, and 0.12.0. Users are recommended to upgrade to version 0.12.1, which fixes this issue.	6.5	More Details
CVE-2026-48910	A carefully crafted editing request could trigger an XSS vulnerability on Apache JSPWiki when parsing errors on the markdown renderer, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. This issue affects Apache JSPWiki: through 2.12.3. Users are recommended to upgrade to version 2.12.4, which fixes the issue.	6.5	More Details
CVE-2026-69245	Guzzle is an extensible PHP HTTP client. Prior to 7.15.2 and 8.0.1, SetCookie::matchesDomain() gives every subdomain of a cookie Domain that cookie unless SetCookie::matchesDomain() recognizes the Domain as an IP literal or a numeric host, and the decision comes from the domain's own text, so two spellings a transport reads as an address keep subdomain scope. Hexadecimal and mixed-base forms such as 0x7f000001 and 0177.0.0.0x1 go unrecognized while libcurl 8.21.0 reads both as 127.0.0.1. A percent-escaped Domain keeps that scope on both branches because percent-decoding sits above numeric parsing, so 192.168.0.%31 and 127.0.0.1%2e are registered names in the URI grammar rather than address literals, and no numeric rule in any base classifies them, while libcurl decodes the host before resolving and reads them as 192.168.0.1 and 127.0.0.1. A cookie stored for Domain=0x7f000001 is placed in the Cookie header of a request to evil.0x7f000001, disclosing a session identifier or token to a host that is not that address, and a response from evil.0x7f000001 setting Domain=0x7f000001 is accepted into the jar and replayed to the address, so a server answering for the look-alike name can fix a session or set application state. Exploitation requires the application to enable cookie	6.5	More Details

	support, address an origin by one of these spellings, and contact a host whose name ends in that spelling. This issue is fixed in versions 7.15.2 and 8.0.1.		
CVE-2026-14928	The JS Help Desk WordPress plugin before 3.1.4 does not perform authorization or ownership checks before returning support-ticket content in a nonce-gated search handler, allowing any authenticated user (Subscriber and above) to read the subject and full message body of every other user's support tickets.	6.5	More Details
CVE-2026-17756	Insufficient policy enforcement in Presentation in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-54082	veraPDF validation model is an implementation of the veraPDF validation model. From 1.25.73 until 1.30.2 and 1.31.71, veraPDF-validation contains an XML External Entity vulnerability in PDFAValidator.validate(...) and GFPDAcroForm.getdynamicRender(), where default DocumentBuilderFactory parsing of rich-text annotation or form-field values and XFA configurations in untrusted PDFs can allow local file disclosure and outbound network requests. This issue is fixed in versions 1.30.2 and 1.31.71.	6.5	More Details
CVE-2026-17683	Inappropriate implementation in ANGLE in Google Chrome prior to 151.0.7922.72 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-2026-17690	Insufficient validation of untrusted input in PDF in Google Chrome on Android prior to 151.0.7922.72 allowed a local attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-17953	Insufficient policy enforcement in WebView in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-17946	Uninitialized Use in Dawn in Google Chrome prior to 151.0.7922.72 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: Low)	6.5	More Details
CVE-2026-17703	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-17707	Uninitialized Use in Media in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-17714	Uninitialized Use in ANGLE in Google Chrome prior to 151.0.7922.72 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-2026-17936	Inappropriate implementation in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-17931	Inappropriate implementation in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-17929	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a malicious file. (Chromium security severity: Low)	6.5	More Details
CVE-2026-17743	Insufficient policy enforcement in ControlledFrame in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17926	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-			

2026-17923	Policy bypass in Enterprise in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted domain name. (Chromium security severity: Low)	6.5	More Details
CVE-2026-17921	Insufficient validation of untrusted input in Navigation in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-17917	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-17679	Insufficient validation of untrusted input in Print Preview in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-17968	Uninitialized Use in WebXR in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-17674	Inappropriate implementation in HTML in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-17985	Insufficient policy enforcement in Speech in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass site isolation via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-17999	Race in PictureInPicture in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-67194	Courier IMAP before 6.0.1 and Courier Mail Server before 2.0.2 allow authenticated IMAP users to crash the imapd process via deeply nested parenthesized SEARCH queries. The SEARCH command parser (alloc_search_key in searchinfo.C) recursively descends on nested parenthesized groups through a mutual recursion chain with alloc_search_andlist() and alloc_search_notkey(), with no depth limit. Courier IMAP has no overall command line length limit, making exploitation trivial. A single IMAP command with ~2500 nested parentheses overflows the 8MB default stack, causing SIGSEGV.	6.5	More Details
CVE-2026-13723	A vulnerability in the `zipx.Unzip` extraction routine of Develar's app-builder allows an attacker to overwrite arbitrary files on macOS APFS by exploiting a Unicode Normalization Collision combined with symlink following behavior. APFS treats certain Unicode equivalent filenames as identical (e.g., ß ↔ ss), while app builder performs no canonical normalization before validating or writing paths. As a result, a crafted ZIP archive containing: • a symlink entry named ss pointing to a target file, and • a regular file named ß containing attacker controlled data, will cause the second write to follow the symlink and overwrite the target file.	6.5	More Details
CVE-2026-17992	Uninitialized Use in Skia in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-17988	Insufficient validation of untrusted input in Navigation in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-17986	Insufficient policy enforcement in Bluetooth in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-59920	Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.136.Final and 4.2.16.Final, Netty's STOMP encoder (StompSubframeEncoder) does not escape or validate header values in CONNECT and CONNECTED frames, so raw newline (\n) characters in a header value are written directly to the wire, allowing an attacker who controls a header value to inject additional STOMP headers. This happens because the encoder intentionally skips escaping for CONNECT/CONNECTED frames per the STOMP 1.2 specification but never rejects the raw newlines, and since a broker parses each line as a separate header, an attacker controlling a value such as a user-supplied login or passcode can overwrite connection	6.5	More Details

	parameters or add authentication/role headers to bypass authentication or escalate privileges (the actual impact is broker-dependent). The issue is fixed in versions 4.1.136.Final and 4.2.16.Final.		
CVE-2026-17668	Uninitialized Use in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-13113	GitLab has remediated an issue in GitLab EE affecting all versions from 17.0 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user to merge code into a protected branch without the required approvals due to a race condition in approval rule processing.	6.5	More Details
CVE-2026-17975	Inappropriate implementation in IME in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-17974	Insufficient policy enforcement in DevTools in Google Chrome prior to 151.0.7922.72 allowed a local attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-65975	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. In versions 1.88.0 up to but not including 1.107.1 and 2.0.0b1 up to but not including 2.5.0, the UI adapters (AG-UI via Agent.to_ag_ui()/AGUIAdapter, and Vercel AI via VercelAIAdapter) use sanitize_messages to strip unresolved ("dangling") client-submitted tool calls from untrusted message history before it reaches the agent, a defense-in-depth default that prevents the agent from executing tool calls the model never emitted. However, the strip anchored to a message index computed before sanitization ran, so when a trailing client message sanitized to empty and was dropped (for example a client system message under the default manage_system_prompt='server'), a preceding assistant response carrying an unresolved tool call became the new tail and was dispatched without inspection. As a result, a remote client could cause a registered, non-approval server tool to run with client-supplied arguments rather than arguments the model produced. The impact is bounded by what the affected tools do and is most significant for applications that gate tool execution in a model-request hook (before_model_request / after_model_request), since a forged call skips the model turn and bypasses that guardrail; approval-gated tools (requires_approval=True) are not auto-executed by this path. This issue has been fixed in versions 1.107.1 and 2.5.0.	6.5	More Details
CVE-2026-17664	Insufficient validation of untrusted input in Loader in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-17667	Uninitialized Use in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-17748	Inappropriate implementation in Extensions in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17754	Inappropriate implementation in Blink in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17759	Uninitialized Use in Codecs in Google Chrome prior to 151.0.7922.72 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-2026-17828	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17846	Inappropriate implementation in Media in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-	Insufficient policy enforcement in Extensions in Google Chrome prior to 151.0.7922.72 allowed an		

2026-17821	attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17822	Race in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17823	Insufficient policy enforcement in WebXR in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17824	Insufficient policy enforcement in ServiceWorker in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17825	Insufficient policy enforcement in Passwords in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17830	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17850	Inappropriate implementation in Permissions in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17831	Insufficient validation of untrusted input in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17835	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17838	Incorrect security UI in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17839	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17840	Incorrect security UI in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17841	Race in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17819	Inappropriate implementation in WebAppInstalls in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17852	Inappropriate implementation in Media Router in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17764	Inappropriate implementation in FedCM in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17796	Side-channel information leakage in WebXR in Google Chrome prior to 151.0.7922.72 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-	Inappropriate implementation in DevTools in Google Chrome prior to 151.0.7922.72 allowed a		

2026-17787	remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17789	Insufficient validation of untrusted input in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via malicious network traffic. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17791	Insufficient validation of untrusted input in Payments in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17792	Inappropriate implementation in Credential Management in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17793	Inappropriate implementation in Messages in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17892	Inappropriate implementation in WebXR in Google Chrome prior to 151.0.7922.72 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-2026-17883	Inappropriate implementation in Headless in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17854	Insufficient policy enforcement in WebMCP in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17882	Policy bypass in Extensions in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to bypass site isolation via a crafted Chrome Extension. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17800	Inappropriate implementation in MediaRecording in Google Chrome prior to 151.0.7922.72 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-2026-17873	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17805	Insufficient policy enforcement in Glic in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17813	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-17814	Insufficient validation of untrusted input in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-18001	Inappropriate implementation in WebGL in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-17842	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-18207	A flaw was found in the client policy enforcement mechanism of Keycloak. The issue occurs when the system checks group membership by name instead of a unique identifier. An attacker with client management privileges could bypass security policies by joining a group with a matching name in a different part of the group hierarchy, potentially allowing them to register or update	6.5	More Details

	clients without following required security hardening profiles.		
CVE-2026-11867	The Frontend Admin by DynamiApps WordPress plugin before 3.29.7 does not perform capability checks on its taxonomy term creation, modification, and deletion operations, allowing authenticated users with low privileges (such as Subscribers) to create, rename, and delete arbitrary taxonomy terms.	6.5	More Details
CVE-2026-16092	The Improved Save Button plugin for WordPress is vulnerable to second-order SQL Injection via 'meta_key' Custom Field via 'Save and Duplicate' Action in all versions up to, and including, 1.2.1 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 author-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2026-5060	The MasterStudy LMS WordPress Plugin – for Online Courses and Education plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.7.14. This is due to the `stm_lms_delete_cover()` function lacking ownership validation on the `file_id` parameter before passing it to `wp_delete_attachment()`. This makes it possible for authenticated attackers, with Instructor-level access and above, to delete arbitrary attachments belonging to any user by enumerating sequential attachment IDs.	6.5	More Details
CVE-2026-18014	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a malicious file. (Chromium security severity: Low)	6.5	More Details
CVE-2026-35226	An out-of-bounds write vulnerability in the CODESYS PROFINET Controller allows an unauthenticated attacker on the same network segment to send malformed PROFINET communication data that triggers an exception in the affected PLC application. The exception is handled by the CODESYS Control runtime system and results in a controlled stop of the PLC application.	6.5	More Details
CVE-2026-58160	Apache Traffic Server reads out of bounds while parsing DNS answers. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	6.5	More Details
CVE-2026-63238	An authentication bypass vulnerability in Koollab LMS allowed an unauthenticated attacker to take over any account, including administrator accounts, by supplying a valid user UUID without providing primary credentials via the 2FA validation endpoint.	6.5	More Details
CVE-2026-65891	Joomla Extension - joomlacontenteditor.net - Creation of hidden files and unintended file overwrite via rename function in Joomla Content Editor (JCE) < 2.20.2 - Improper input validation in the file rename functionality allowed an authenticated user with file management permissions to rename files to otherwise invalid names, resulting in the creation of hidden files. The issue also allowed existing files at the destination path to be unintentionally replaced.	6.5	More Details
CVE-2026-16751	Authorization Bypass in the emergency recovery approval component in Ente Technologies Ente Museum Server allows an authenticated attacker configured as a victim's emergency contact to bypass the configured recovery waiting period and take over the victim's account via a crafted `approve-recovery` API request.	6.5	More Details
CVE-2026-18192	VIN-DS783E-E6 developed by Vacron has an Arbitrary File Read vulnerability, allowing authenticated remote attackers to exploit Relative Path Traversal to download arbitrary system files.	6.5	More Details
CVE-2026-67247	A path traversal vulnerability was found in the IHM Log handling of ADM. The vulnerability occurs because user-controlled disk serial input is not sufficiently validated before being used to construct the path of an IHM log database file. An authenticated attacker can exploit this issue to cause the affected component to access an unintended filesystem path or log database file. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.RUN1 as well as from ADM 5.0.0 through ADM 5.1.3.RI81.	6.5	More Details
CVE-2026-67246	A path traversal vulnerability was found in the Wallpaper component of ADM. The vulnerability occurs because user-controlled wallpaper path input is not sufficiently validated before being used for file access. An authenticated attacker can exploit this issue to access or manipulate files outside the intended wallpaper directory, subject to user permissions and filesystem restrictions. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.RUN1 as well as from ADM 5.0.0 through ADM 5.1.3.RI81.	6.5	More Details

CVE-2026-14923	The Sync Post With Other Site WordPress plugin before 1.9.3 does not correctly enforce the page-editing capability on a REST route that creates and updates posts, because of an operator-precedence flaw in its authorization check. An authenticated user holding only the post-editing capability (such as a Contributor) can create, publish, and overwrite arbitrary Pages, including modifying content authored by higher-privileged users.	6.5	More Details
CVE-2026-18005	Inappropriate implementation in WebXR in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-17161	The WowStore – Store Builder & Product Blocks for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'filterMobileText' Block Attribute in all versions up to, and including, 4.4.24 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The save-time wp_kses_post sanitization is ineffective because the payload is stored inside a Gutenberg block delimiter comment as JSON, which wp_kses_post preserves, allowing an attribute-breakout string to survive to the server-side render_callback.	6.4	More Details
CVE-2026-13362	The SendPulse Email Marketing Newsletter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via _sp_form_code Post Meta in all versions up to, and including, 2.2.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the attacker to create a sendpulse_form post containing a benign SendPulse loader script tag alongside arbitrary HTML (e.g., an img onerror payload), which bypasses the allow-list check and executes in the browser of any user — including administrators — who previews or views a page rendering the [sendpulse-form] shortcode.	6.4	More Details
CVE-2026-15649	The Powerkit – Supercharge your WordPress Site plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 3.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-18435	The Kadence Blocks — Page Builder Toolkit for Gutenberg Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'toggleIcon' Block Attribute in all versions up to, and including, 3.7.8 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-2026-67530	WACRM is a self-hostable CRM template for WhatsApp. In 0.7.0 and earlier, the automation send_webhook action in src/lib/automations/engine.ts and its validation in src/lib/automations/validate.ts allowed an authenticated user with automation privileges to submit an arbitrary webhook URL that the server fetched without the existing isDeliverableUrl SSRF guard in src/lib/webhooks/ssrf.ts, allowing requests to private, loopback, link-local, or cloud metadata addresses such as the cloud metadata endpoint at 169.254.169.254. This vulnerability is fixed with commit 23838a9959550e975d732ae08a44a3a2f0cc084b.	6.4	More Details
CVE-2026-15645	The Powerkit – Supercharge your WordPress Site plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'nav' Shortcode Attribute in all versions up to, and including, 3.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-15950	The Cozy Blocks – Page Builder for Gutenberg Editor & FSE with 600+ Patterns, 58 Blocks & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'layoutCircle.alignment' Block Attribute in all versions up to, and including, 2.2.11 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-	The Newsletters Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'target' attribute of the [newsletters_post] shortcode in versions up to and including 4.15. This is due to insufficient input sanitization and output escaping in the posts_single() function which propagates the attacker-controlled 'target' attribute into the global $wpml_target, and in the		More

2026-12938	shortcode_posts() 'post_thumbnail' handler which concatenates $wpml_target into a target="..." 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	Details
CVE-2026-15644	The Powerkit – Supercharge your WordPress Site plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'style' Shortcode Attribute in all versions up to, and including, 3.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-16090	The GamiPress – Gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'heading_size' Shortcode Attribute in 'gamipress_achievement' in all versions up to, and including, 7.9.9.1 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. WordPress save-time wp_kses_post does not neutralize this payload because the injected value is stored inside a shortcode attribute rather than as a raw HTML tag, and is only emitted into HTML at render time without escaping.	6.4	More Details
CVE-2026-13458	The GenerateBlocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Dynamic Tag Injection in HTML 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. A Contributor-level attacker can store the malicious payload by placing a dynamic tag such as {{post_meta key:...}} in a non-URL HTML attribute (e.g., title, aria-label, alt, or data-* attributes) of a GenerateBlocks element block, then setting the corresponding unprotected post meta key via the Custom Fields metabox to a value containing a closing quote and an injected event-handler attribute.	6.4	More Details
CVE-2026-7623	The SureForms – Contact Form, Payment Form & Other Custom Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'headingWrapper' parameter in all versions up to, and including, 2.8.1 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-2026-15662	The Advanced Woo Labels – Product Labels & Badges for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'bg_color' parameter in all versions up to, and including, 2.48 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-2026-16684	The Easy Property Listings plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'facebook' User Contact Method in all versions up to, and including, 3.5.24 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
CVE-2026-16685	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'icon' Shortcode Attribute in all versions up to, and including, 3.3.66 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. wp_kses_post() does not neutralize the payload because it operates on post content at save time and does not process shortcode attribute values that are emitted unescaped at render time.	6.4	More Details
CVE-2026-18062	The Kadence Blocks — Page Builder Toolkit for Gutenberg Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Identity Block Inner Image Content in all versions up to, and including, 3.7.8.1 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. This vulnerability is only triggerable when the block's urlTransparent attribute is set to a non-empty value, as this is a required precondition for the vulnerable code path in build_html() to be reached.	6.4	More Details
CVE-	@better-auth/oauth-provider before 1.7.0-beta.4 fails to bind access-token audience to the		

2026-67332	authorization grant, allowing clients to request tokens for unrelated resources. Attackers can complete an OAuth flow and obtain access tokens whose audience targets resource servers the authorization never covered, bypassing intended authorization boundaries.	6.4	More Details
CVE-2026-7436	The WPC Badge Management for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'text' attribute of the `wpcbm_best_seller` shortcode in all versions up to, and including, 3.1.6 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-2026-12939	The Newsletters Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link' attribute of the post_thumbnail (and newsletters_post_thumbnail) shortcodes in versions up to and including 4.15. This is due to insufficient input sanitization and output escaping in the post_thumbnail() method in helpers/shortcode.php, which concatenates the user-controlled $link shortcode attribute directly into an href attribute without esc_url() or 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-2026-15735	The Contact Form to Any API plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'cf7anyapi_form_field' Post Meta in all versions up to, and including, 3.0.6 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-2026-8791	The Booking System Trafft plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `bookingWebsiteUrl` setting in all versions up to, and including, 1.0.17 due to a missing capability check on the `set_options` AJAX action when the plugin is operating in agency mode. The `trafftSetOptions()` handler verifies a nonce that is exposed to any authenticated user (it is printed inline on every admin page, including profile.php) but performs no capability check before calling `update_option('trafft_option', ['bookingWebsiteUrl' => ...])`. This setting is then used by `trafftAdminAssets()` to enqueue `<bookingWebsiteUrl>/embed.js` as a script on every front-end page that renders the booking shortcode. This makes it possible for authenticated attackers, with Subscriber-level access and above, to point the embed-script URL at an attacker-controlled origin and execute arbitrary JavaScript in the browser of every site visitor (including admins).	6.4	More Details
CVE-2026-17162	The WowStore – Store Builder & Product Blocks for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'currentPostId' Block Attribute in all versions up to, and including, 4.4.24 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-2026-12231	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘ exad_infobox_image’ 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-2026-16091	The GamiPress – Gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'gamipress_rank' Shortcode in all versions up to, and including, 7.9.9.1 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-2024-40683	IBM Operations Analytics - Log Analysis 1.3.5.0, 1.3.5.1, 1.3.5.2, 1.3.5.3, 1.3.6.0, 1.3.6.1, 1.3.7.0, 1.3.7.1, 1.3.7.2, and 1.3.8.0, 1.3.8.1, 1.3.8.2, 1.3.8.3, 1.3.8.4 does not invalidate session after a password chance which could allow an authenticated user to impersonate another user on the system.	6.3	More Details
CVE-2026-18766	A flaw has been found in chetans9 core-php-admin-panel up to 90d07ed5aac5e0f09b6a5828d7bb2eb83010763f. This issue affects some unknown processing of the file /Applications/MAMP/htdocs/core-php-admin-panel-master/customers.php. Executing a manipulation of the argument filter_col can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either	6.3	More Details

	affected or updated releases. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-18722	A vulnerability was found in diaowen DWSurvey up to 6.14.0. Impacted is the function in DwDeisgnSurveyController.devSurvey. of the file /api/dwsurvey/app/v6/dw-design-survey/dev-survey.do of the component Survey Handler. The manipulation results in authorization bypass. The attack can be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-67295	FreeRDP before 3.29.0 fails to properly validate server-supplied RDPDR paths in drive redirection, allowing attackers to access prefix-sibling paths outside the configured shared root. A malicious RDP server can read, write, delete, and enumerate files in sibling directories by sending non-rooted paths that bypass the shared-root boundary check.	6.3	More Details
CVE-2026-18775	A vulnerability has been found in NousResearch hermes-agent up to 0.16.0. This vulnerability affects the function browser_snapshot of the file tools/browser_tool.py of the component Browser Tooling. Such manipulation leads to server-side request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-17780	Inappropriate implementation in Isolated Web Apps in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.3	More Details
CVE-2026-67307	Wazuh 5.0.0-beta1 (fixed in 5.0.0-beta3) does not validate or override the cluster_name and cluster_node fields in inventory-sync Start FlatBuffer messages, while validating only the agentid against the authenticated agent identity. This allows a low-privileged enrolled agent to spoof cluster attribution in indexed inventory and vulnerability documents by forging wazuh.cluster.name values and influencing the document _id prefix, potentially tampering with inventory records or, in shared-indexer multi-cluster deployments, poisoning another cluster's records when numeric agent IDs collide.	6.3	More Details
CVE-2026-18774	A flaw has been found in NousResearch hermes-agent up to 0.16.0. This affects the function save_url_image of the file agent/image_gen_provider.py of the component xAI Image Generation Provider. This manipulation causes server-side request forgery. The attack may be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-18719	A vulnerability was detected in cemtan sar2html 4.0.0. This affects an unknown part of the file sar2html.py of the component Search. Performing a manipulation of the argument Search results in sql injection. It is possible to initiate the attack 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.	6.3	More Details
CVE-2026-18773	A vulnerability was detected in NousResearch hermes-agent up to 2026.6.5. Affected by this issue is the function _check_slash_access of the file gateway/run.py of the component Quick Command Handler. The manipulation results in incorrect authorization. The attack can be launched 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.	6.3	More Details
CVE-2026-62323	Cloudreve is a self-hosted file management and sharing system. Prior to 4.17.0, ViewerSessionValidation uses only the session-id prefix of a WOPI access token and does not enforce the requested viewer action, allowing a malicious or compromised WOPI viewer with a view session to forge the token suffix and invoke WOPI write routes for the underlying file. This issue is fixed in version 4.17.0.	6.3	More Details
CVE-2026-18590	A vulnerability was determined in Wavlink WL-NU516U1 708c073-mt7628. Affected is the function set_sys_adm of the file adm.cgi of the component Admin Password Handler. This manipulation causes os command injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. It is suggested to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	6.3	More Details
CVE-2026-	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.8.8 until 0.11.0, the terminal WebSocket route in backend/open_webui/routers/terminals.py authenticated its own first-message JWT and never applied the verified-user role gate that get_verified_user enforces on HTTP terminal routes. An account whose role is pending, including a registered but unapproved account or an account deactivated back to pending, can open an	6.3	More Details

70490	interactive terminal session when at least one terminal server is configured and its access grants cover the account. This loses the account-approval boundary for terminal access while the HTTP terminal routes correctly reject the same account. This issue is fixed in 0.11.0.		
CVE-2026-54020	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.11.0, Open WebUI resolved a hostname during URL validation and rejected private, loopback, and link-local addresses, but the HTTP clients resolved the hostname again at connection time. An authenticated attacker who controlled authoritative DNS for a submitted hostname could answer with a public address during validation and an internal one during connection, reaching cloud metadata, loopback admin APIs, or internal services through URL ingest, chat image_url fetches, image editing, or OAuth profile-picture fetches, with most paths returning the response to the attacker and the OAuth path forwarding the OAuth access token. This issue is fixed in 0.11.0.	6.3	More Details
CVE-2026-18631	A vulnerability was identified in jeequan jeepay up to 3.2.9. This vulnerability affects the function WebSecurityConfig of the file jeepay-manager/src/main/java/com/jeequan/jeepay/mgr/ctrl/sysuser/SysLogController.java of the component PreAuthorize Handler. The manipulation leads to authorization bypass. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-54705	MathLive provides web components for math display and input. Prior to 0.110.0, MathLive fails to escape text-mode content in \text{} and \mbox{} commands in Box.toMarkup at src/core/box.ts, in xmlEscape, scanText, and text-mode output in src/formats/atom-to-math-ml.ts, and through convertLatexToMarkup, convertLatexToMathMl, <math-span>, <math-div>, and the default identity MathfieldElement.createHTML, allowing malicious input to run arbitrary JavaScript when rendered. This issue is fixed in version 0.110.0.	6.3	More Details
CVE-2026-18632	A security flaw has been discovered in langgenius dify up to 1.14.2. This issue affects the function jinja2.Template of the file api/core/helper/code_executor/jinja2/jinja2_transformer.py of the component Jinja2 Handler. The manipulation results in improper neutralization of special elements used in a template engine. The attack may be launched 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-2026-18723	A vulnerability was determined in diaowen DWSurvey up to 6.14.0. The affected element is an unknown function of the file /api/dwsurvey/app/survey/up-survey-status.do of the component Survey Status Handler. This manipulation causes improper authorization. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-18818	A weakness has been identified in Ehco1996 django-sspanel up to 2023.12.26. This affects the function TicketDetailView of the file apps/sspanel/views.py of the component Support Ticket Handler. Executing a manipulation can lead to authorization bypass. The attack can be executed remotely. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-66311	Missing authorization in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform tampering locally.	6.2	More Details
CVE-2026-68499	re2 provides Node.js bindings for Google's RE2 regular expression engine. Prior to 1.25.2, re2's String.prototype.match implementation with a global RE2 pattern that can match the empty string fails to advance its native matching cursor in lib/match.cc, causing an infinite loop and unbounded native memory growth that blocks the event loop and can exhaust host memory. This issue is fixed in 1.25.2.	6.2	More Details
CVE-2026-10695	IBM Db2 12.1.0 through 12.1.4 federated server is vulnerable to a denial of service when running non fenced federated queries.	6.2	More Details
CVE-2026-54785	gemini-bridge is a lightweight MCP server bridging AI agents to Google's Gemini AI via the official CLI. From 1.0.0 until 1.3.1, consult_gemini_with_files in inline mode read any file path supplied in the files argument without confining it to the working directory, then forwarded the contents to the Gemini CLI. Because the caller also controls query, the file contents are echoed back through the Gemini round-trip (and sent to Google), making this an arbitrary local file read. This issue is fixed in version 1.3.1.	6.2	More Details

CVE-2026-20470	In Telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS11086431; Issue ID: MSV-8189.	6.2	More Details
CVE-2026-63119	MCP Ruby SDK is the official Ruby SDK for Model Context Protocol servers and clients. Prior to 0.23.0, MCP::Server::Transports::StdioTransport and MCP::Client::Stdio in the mcp gem use IO#gets without a byte limit, allowing a peer that sends data without a newline to exhaust process memory. This issue is fixed in version 0.23.0.	6.2	More Details
CVE-2026-68562	A flaw was found in ansible-collection-redhat-leapp. An attacker with privileged write access to a managed node's Leapp report content can manipulate it. When an operator runs a specific remediation task, this manipulated report can cause the Ansible controller to read its own local files and copy them to the managed node. This vulnerability leads to information disclosure, potentially exposing sensitive controller-side data such as private keys or credentials.	6.2	More Details
CVE-2026-67596	CSL 1010 M2M 3G WiFi Module firmware through 2.2.1.4 contains a weak encryption vulnerability that allows unauthenticated attackers to recover all stored secrets in plaintext by reversing a single-byte XOR cipher that uses a static key to obfuscate the configuration backup file. Attackers can trivially decrypt the Router.cfg backup file to expose web administration and telnet passwords, WPA/WPA2 pre-shared keys, PPPoE and 3G/APN credentials, and SIM identifiers including IMSI and IMEI.	6.2	More Details
CVE-2026-17996	Inappropriate implementation in Browser in Google Chrome on Mac prior to 151.0.7922.72 allowed a local attacker to bypass navigation restrictions via a malicious file. (Chromium security severity: Low)	6.2	More Details
CVE-2026-17966	Inappropriate implementation in Views in Google Chrome on Mac prior to 151.0.7922.72 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	6.2	More Details
CVE-2026-15430	Improper access control in the IRP_MJ_WRITE command interface in Wellbia XIGNCODE3 xhunter2.sys, version 2026.6.1.192, allows a local, unprivileged attacker to achieve local privilege escalation to NT AUTHORITY\SYSTEM, extract credentials from PPL-protected lsass.exe, and terminate PPL-protected security processes.	6.2	More Details
CVE-2026-17827	Inappropriate implementation in CSS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	6.1	More Details
CVE-2026-17571	The Fluent Forms – Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via 'param' in all versions up to, and including, 6.2.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-17845	Inappropriate implementation in CSS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	6.1	More Details
CVE-2026-52232	A reflected cross-site scripting (XSS) vulnerability in the /logo.asp component of FS Inc S3150-8T2F Switch 2.2.0D Build 118101 allows attackers to execute arbitrary Javascript in the context of the victim's browser via a crafted URL.	6.1	More Details
CVE-2026-14592	The WP Real IP-based Access Control WordPress plugin through 1.3.1 does not perform any capability or nonce checks before storing one of its option values, and does not escape that value on output on its settings page, allowing unauthenticated users to store arbitrary JavaScript that executes in the context of any administrator who views the page.	6.1	More Details
CVE-2026-61526	AdonisJS HTTP Server is a package for handling HTTP requests in the AdonisJS framework. In versions 8.0.0-next.0 through 8.2.0 and 9.0.0 through 9.0.2, the error.message is interpolated into the default HTML exception response without escaping, allowing a crafted missing-route URL to execute attacker-controlled JavaScript when a victim opens it and no custom status page or JSON response handles the error. When debug mode is disabled and no custom status page handles the error, the default HTML renderer interpolates error.message directly into an HTML response. This issue is fixed in versions 8.2.1 and 9.1.0.	6.1	More Details
	The Fluent Forms WordPress plugin before 6.2.6 does not sanitise and escape one of its form field		

CVE-2026-11881	configuration settings before outputting it inside an inline script when a form is rendered, which could allow users with a role as low as Contributor (with delegated form-management permission, and therefore lacking the unfiltered_html capability, e.g. in a multisite setup) to perform Stored Cross-Site Scripting attacks that execute in the browser of any visitor who loads the form, including administrators previewing it.	6.1	More Details
CVE-2026-17818	Inappropriate implementation in Network in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	6.1	More Details
CVE-2026-14841	The King Addons for Elementor WordPress plugin before 51.1.76 does not escape a user-supplied grid setting before reflecting it into an HTML attribute in an unauthenticated AJAX response, allowing attackers to execute arbitrary JavaScript in the browser of a visitor who is tricked into loading a crafted page.	6.1	More Details
CVE-2026-15920	An issue was discovered in Django 5.2 before 5.2.17 and 6.0 before 6.0.8. `django.contrib.admin.utils.display_for_field()` renders `URLField` values as clickable links in the admin without validating the URL. A value stored with an unsafe scheme is displayed as a link on changelist and read-only admin pages, which allows cross-site scripting against staff users who click the link. Exploitation requires the unsafe value to already be stored in the database. `URLField` validation through a `ModelForm` or the admin rejects unsafe schemes, so this affects applications that persist `URLField` data without running model validation, for example through direct queryset writes, deserialization, or bulk import of untrusted input. Django would like to thank Egor Saltykov for reporting this issue.	6.1	More Details
CVE-2026-67338	JupyterLab before 4.5.9 contains a stored cross-site scripting vulnerability in the Extension Manager that fails to validate URI protocols in package metadata URLs. Attackers can publish malicious PyPI packages with javascript: URLs in project metadata that execute arbitrary JavaScript in the JupyterLab origin when users click the extension name.	6.1	More Details
CVE-2026-14845	The NewStatPress WordPress plugin before 1.4.5 does not sanitise and escape data derived from unauthenticated visitor requests before storing it and later outputting it in one of its widgets, which could allow unauthenticated attackers to perform Stored Cross-Site Scripting attacks against users viewing the affected widget.	6.1	More Details
CVE-2026-17853	Inappropriate implementation in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to inject scripts or HTML into a privileged page via a crafted HTML page. (Chromium security severity: Medium)	6.1	More Details
CVE-2026-16792	An improper certificate validation vulnerability was reported in multiple Lenovo XClarity Orchestrator (LXCO) 2.2.0 microservices that could allow an adjacent network attacker to intercept sensitive communications by performing a machine-in-the-middle attack against HTTPS connections during TLS certificate validation under certain circumstances.	6.1	More Details
CVE-2026-13330	The Animation Addons for Elementor WordPress plugin before 2.7.0 does not sanitise uploaded SVG/SVGZ files, which it adds to the list of allowed upload types, allowing users with the upload_files capability (Author and above) to upload files containing malicious JavaScript, leading to Stored Cross-Site Scripting.	6.1	More Details
CVE-2026-17872	Cryptographic Flaw in WebAppInstalls in Google Chrome on Android prior to 151.0.7922.72 allowed a local attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	6.1	More Details
CVE-2026-17878	Inappropriate implementation in CSS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	6.1	More Details
CVE-2026-18344	The Wp Responsive Thumbnail Slider plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'id' parameter in versions up to, and excluding, 1.1.53. This is due to insufficient input sanitization and output escaping in the responsive_thumbnail_image_management() function, which echoes $_GET['id'] directly into a double-quoted HTML attribute with no esc_attr() call. The only guard is a loose PHP numeric comparison ($_GET['id']>0) that a string beginning with a numeric prefix trivially satisfies, and the addslashes() applied by wp_magic_quotes() is inert in HTML-attribute context because backslash is not an HTML escape character. 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-2026-14922	WP Photo Album Plus is vulnerable to stored Cross-Site Scripting in all versions up to, and including, 9.2.03.001 through a decode-after-sanitize (double-encoding) flaw in the photo-comment pipeline. On write, `wppa_do_comment()` sanitizes the comment with `wppa_filter_html()` (wp_kses) followed by `wp_strip_all_tags()` (`wppa-functions.php:2623-2624`). Because `wp_strip_all_tags()` only removes *real* tags, an attacker who submits a **double HTML-entity-encoded** payload (e.g. `&lt;img src=... onload=...&gt;`) passes the write filters as harmless entity text and is stored one decode-level down (`<img ... onload=...>`).	6.1	More Details
CVE-2026-14921	The Ultimate Addons for WPBakery Page Builder WordPress plugin before 3.21.5's shared link-rendering function, Ultimate_VC_Addons::uavc_link_init(),	6.1	More Details
CVE-2026-17797	Inappropriate implementation in CSS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	6.1	More Details
CVE-2026-14207	The LifterLMS WordPress plugin before 10.0.10 does not strip event-handler attributes from a course pricing field before storing and rendering it, allowing users with a course-editing role to inject JavaScript that executes in the session of an administrator who views the course.	6.1	More Details
CVE-2025-65342	code-projects Blood System 1.0 is vulnerable to Cross Site Scripting (XSS) in /don.php via the city field.	6.1	More Details
CVE-2026-65946	Joomla Extension - rolandd.com - XSS vectors in AJAX endpoint handlers RO CSVI < 9.11.0	6.1	More Details
CVE-2025-51684	CleverTap Web SDK v1.15.1 is vulnerable to Cross Site Scripting (XSS). The application does not sanitize untrusted data received via window.postMessage before injecting it into the page DOM. An attacker can craft a malicious message that, when processed by renderCustomHtml, results in execution of arbitrary JavaScript in the context of the hosting site.	6.1	More Details
CVE-2025-65341	Ecommerce Fruits Bazar 1.0 is vulnerable to Cross Site Scripting (XSS) in admin/edit_product.php.	6.1	More Details
CVE-2026-44613	Cross-Site Request Forgery (CSRF) vulnerability in Apache Zeppelin. The default CORS configuration allowed cross-origin state-changing requests and accepted text/plain request bodies, allowing an attacker who lures an authenticated user to a malicious site to perform actions on the user's behalf through REST and WebSocket endpoints. This issue affects Apache Zeppelin versions 0.6.0 through 0.12.0. Users are recommended to upgrade to version 0.12.1, which fixes this issue.	6.1	More Details
CVE-2026-13340	The SVG Support WordPress plugin before 2.5.17 does not apply its SVG sanitisation to uploaded files using the .svgz extension, even though it registers and serves them as SVG, allowing a user permitted to upload SVGs (such as an Author once granted upload access) to store a script-bearing file that executes in the browser of anyone who later views it, including an administrator.	6.1	More Details
CVE-2026-17962	Inappropriate implementation in Blink in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Low)	6.1	More Details
CVE-2026-15383	The Blog Floating Button WordPress plugin through 1.4.20 does not sanitize or escape the visitor User-Agent header, which it stores through an unauthenticated tracking REST endpoint and later renders unescaped in an administrator report page. This allows an unauthenticated attacker to store a malicious script that executes in the session of any administrator who views the access report, leading to site takeover.	6.1	More Details
CVE-2026-15931	The Simple Membership WordPress plugin before 4.7.8 does not sanitise a subscriber name value received from an unauthenticated payment approval request, nor escape it when displaying it in the administration dashboard, allowing unauthenticated attackers to store arbitrary JavaScript that executes in an administrator's session.	6.1	More Details
CVE-2025-	IBM Engineering Requirements Management DOORS and DOORS Web Access 9.7.2.1 through 9.7.2.11, and 9.6.1.1 through 9.6.1.13 is vulnerable to cross-site scripting. This vulnerability	6.1	More

0152	allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.		Details
CVE-2026-66490	Joomla Extension - balbooa.com - Stored cross-site scripting via a comment avatar in Gridbox < 2.20.2	6.1	More Details
CVE-2026-66414	Leantime 3.6.2 contains an open redirect vulnerability in the Login controller that allows unauthenticated attackers to redirect authenticated users to arbitrary external sites by manipulating the redirectUrl POST parameter. Attackers can craft a malicious login URL with a tampered redirectUrl value that bypasses FILTER_SANITIZE_URL validation to redirect victims to attacker-controlled sites for phishing or credential theft.	6.1	More Details
CVE-2026-54663	swagger-typescript-api generates API clients for Fetch or Axios from OpenAPI specifications. Prior to 13.12.2, src/resolved-swagger-schema.ts warmUpRemoteSchemasCache resolves external $ref URLs and fetchRemoteSchemaDocument uses isHttpUrl to fetch any http or https target without private IP, redirect, DNS rebinding, or same-origin validation, allowing an attacker-controlled OpenAPI spec to make the generator issue requests to internal or link-local services. This issue is fixed in version 13.12.2.	6.1	More Details
CVE-2025-65337	Sourcecodester Fantastic Blog CMS 1.0 is vulnerable to Cross Site Scripting (XSS) in pageEditMember.php via the address field.	6.1	More Details
CVE-2026-38446	A stored cross-site scripting (XSS) vulnerability exists in osTicket 1.18.3 due to improper sanitization of the thread entry title field. User-controlled input in the title is stored without adequate HTML escaping and later rendered in multiple staff-facing templates without proper output encoding. An attacker can inject arbitrary JavaScript by submitting a crafted ticket reply or email with a malicious subject line.	6.1	More Details
CVE-2026-38444	osTicket v1.18.3 is vulnerable to Stored Cross-Site Scripting (XSS) via the email From-header display name. The value is extracted without sanitization in include/class.mailparse.php and stored raw in the poster field of ost_thread_entry. When an unauthenticated attacker sends a reply email to an existing ticket from an unregistered address with an XSS payload in the From display name.	6.1	More Details
CVE-2026-20466	In sec boot, there is a possible escalation of privilege due to a heap buffer overflow. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: AUTO00845351 (Note: For MT2737) / ALPS11072643 (Note: For MT6880, MT6890, MT6990); Issue ID: MSV-6929.	6.1	More Details
CVE-2026-16465	A maliciously crafted DWG or DXF file, when parsed through Autodesk AutoCAD, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage this vulnerability to cause a crash or disclose sensitive information.	6.1	More Details
CVE-2026-66325	Server-side request forgery (ssrf) in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	6.1	More Details
CVE-2026-65804	Improper control of generation of code ('code injection') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	6.1	More Details
CVE-2026-20485	In HFRP, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11049569; Issue ID: MSV-7931.	6.0	More Details
CVE-2026-20474	In display, there is a possible escalation of privilege due to a race condition. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11019183; Issue ID: MSV-7758.	6.0	More Details
CVE-2026-20469	In trusted_mem, there is a possible escalation of privilege due to improper input validation. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: AUTO00834868; Issue ID: MSV-6533.	6.0	More Details

CVE-2026-20475	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11004276; Issue ID: MSV-7748.	6.0	More Details
CVE-2026-20497	In geniezone, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10965550 / ALPS11393405; Issue ID: MSV-6941.	6.0	More Details
CVE-2026-20477	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11009963; Issue ID: MSV-7658.	6.0	More Details
CVE-2026-20481	In geniezone, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10965373; Issue ID: MSV-6935.	6.0	More Details
CVE-2026-20473	In display, there is a possible memory corruption due to use after free. 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: ALPS11019722; Issue ID: MSV-7759.	6.0	More Details
CVE-2026-20467	In apusys, there is a possible escalation of privilege due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: AUTO00837766; Issue ID: MSV-6767.	6.0	More Details
CVE-2026-20468	In apusys, there is a possible escalation of privilege due to a confused deputy. 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: AUTO00833804; Issue ID: MSV-6741.	6.0	More Details
CVE-2026-20498	In geniezone, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10900493; Issue ID: MSV-6765.	6.0	More Details
CVE-2026-67294	FreeRDP before 3.29.0 improperly validates the Extended Key Usage (EKU) purpose of the peer certificate during client-side server TLS authentication. In x509_utils_verify(), when server-purpose (X509_PURPOSE_SSL_SERVER) verification fails, the code falls back to client-purpose and any-purpose verification, so a trusted, hostname-matching certificate valid only for clientAuth can be accepted as the RDP server certificate. In environments relying on EKU separation between client and server certificates, this allows a clientAuth-only certificate issued by a trusted CA to bypass server certificate purpose validation.	5.9	More Details
CVE-2026-58185	The Apache Traffic Server intercept plugin has a use-after-free. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	5.9	More Details
CVE-2026-58183	The Apache Traffic Server prefetch plugin can crash when processing attacker-influenced input. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	5.9	More Details
CVE-2026-48154	GoRest is a Golang starter kit built with the Gin framework for prototyping and developing RESTful APIs. In versions prior to 1.12.2 nMemorySecret2FA contains a race condition due to an unsynchronized package-level map used to store 2FA secrets. Multiple HTTP handlers in handler/login.go and handler/twoFA.go read from and write to this map concurrently, and because Go's runtime treats unsynchronized concurrent map access as an unrecoverable fatal error, an attacker can repeatedly trigger this condition to crash the process on demand. This results in high, repeatable availability impact with no confidentiality or integrity consequences. This issue has been fixed in version 1.12.2.	5.9	More Details
CVE-2026-67607	LightFTP 2.3.1 contains a residual race condition vulnerability (an incomplete fix for CVE-2024-11144) in the worker_thread_cleanup() function of ftpserv.c that allows remote unauthenticated attackers to destabilize or crash the daemon by triggering unsynchronized access to shared per-connection state without holding the required mutex lock. Attackers can send a data-transfer command such as LIST followed immediately by ABOR to exploit the missing synchronization on shared context and detached thread id reuse, resulting in daemon destabilization or crash which	5.9	More Details

	can lead to a denial of service. The 2.3.1 patch only narrowed the timing window (an extra re-check and reordered cleanup), it never added the missing lock, so the underlying race remains.		
CVE-2026-50558	Penelope Shell Handler is a post-exploitation shell handler for authorized security testing. Prior to 0.20.0, the Unix download() implementation in penelope.py used tar.extractall(local_download_folder) on tar archives returned by remote sessions without validating member paths, allowing a malicious or compromised session to write files outside the intended download directory and potentially overwrite ~/.penelope/peneloperc. This issue is fixed in version 0.20.0.	5.9	More Details
CVE-2026-67213	nanoid (Nano ID) before 5.1.6 contains an infinite loop in the customAlphabet and customRandom functions. When these functions are configured with a size of 0, the internal generation loop never satisfies its exit condition and spins indefinitely, hanging the calling thread. An application that passes an unvalidated, attacker-controlled size of 0 to these functions is exposed to a denial-of-service condition.	5.9	More Details
CVE-2026-67216	cJSON through 1.7.19 contains an inefficient algorithmic complexity flaw in cJSON_Compare(). When comparing objects, the function recurses into each shared subtree twice, once in each direction, with no depth guard, making the running time exponential in nesting depth. A small, deeply nested document of a few hundred bytes (depth around 40) compared for equality consumes hours of CPU, and the cost roughly doubles with each additional level of nesting. An application that calls cJSON_Compare() on attacker-influenced JSON that is structurally equal to a reference document is exposed to a denial-of-service condition.	5.9	More Details
CVE-2026-16547	The REST API Log WordPress plugin before 1.7.1 does not bind the token protecting its log download feature to the log entry being requested, nor does it check the capability of the requester, allowing unauthenticated users in possession of any such token to download the logged REST API requests and responses of any entry, which may contain sensitive data such as credentials, authentication tokens or private content.	5.9	More Details
CVE-2026-14643	undici's cache interceptor mishandles optional whitespace placed around the equals sign of a qualified no-cache or private Cache-Control directive. In undici from 7.0.0 up to before 7.29.0 and from 8.0.0 up to before 8.9.0, the parser either drops the directive or stores a field name with literal quote characters, so the cache decision fails to recognize the qualification and the response is stored. In shared-cache mode, this lets a response containing one user's authenticated data be served from cache to a later caller, including an unauthenticated one, when both requests resolve to the same cache key. It affects applications that enable the cache interceptor in shared mode, forward Authorization headers upstream, and receive cacheable responses with qualified directives padded with whitespace around the equals sign. This is the whitespace-around-equals variant that the fix for CVE-2026-9678 did not normalize, and it is fixed in undici 7.29.0 and 8.9.0.	5.9	More Details
CVE-2026-48061	Litestar is an Asynchronous Server Gateway Interface (ASGI) framework. In versions prior to 2.22.0, an attacker can bypass the allowed hosts validation by omitting the Host header and supplying an X-Forwarded-Host header set to a whitelisted domain. The AllowedHostsMiddleware trusts the X-Forwarded-Host header as a fallback when the Host header is absent. Since X-Forwarded-Host is a client-controllable header, this enables host header injection attacks such as password reset poisoning, cache poisoning, and server-side request routing manipulation. Any application using AllowedHostsConfig is affected when deployed without a reverse proxy that strips X-Forwarded-Host, or when accepting HTTP/1.0 connections. This issue has been fixed in version 2.22.0.	5.9	More Details
CVE-2026-58152	Apache Traffic Server mishandles integers while decoding HPACK/XPACK headers, corrupting memory. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	5.9	More Details
CVE-2026-33930	Apache Traffic Server copies the client Host header into a fixed-size stack buffer without a bound during redirect handling, so an over-long Host header overflows the stack when redirect following is enabled. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	5.9	More Details
CVE-2026-	nanoid (Nano ID) before 5.1.16 contains an infinite loop in the customAlphabet and nanoid functions of its non-secure module (nanoid/non-secure). When these functions are given a negative size, the loop counter is decremented from a negative value and never reaches its termination condition, spinning indefinitely and hanging the calling thread. An application that	5.9	More Details

67214	passes an unvalidated, attacker-controlled negative size to these functions is exposed to a denial-of-service condition.		
CVE-2026-58158	Apache Traffic Server mishandles PROXY protocol input, truncating ports and overflowing the stack. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	5.9	More Details
CVE-2026-18362	The IRIS web application in version 2.4.26 and possibly others does not protect its user authentication against brute-force attacks.	5.9	More Details
CVE-2026-67354	guzzlehttp/guzzle versions before 7.15.1 contain an information disclosure vulnerability in RedirectMiddleware. When the optional allow_redirects.referer setting is enabled, the middleware copies the URI fragment (the portion after '#') from the referring request into the generated Referer header when following a same-scheme redirect (e.g., HTTPS to HTTPS). An attacker who controls the redirect destination can read this fragment from the incoming Referer header, potentially disclosing one-time login secrets, access tokens, state values, or other sensitive client data to a server never meant to receive it. The referer setting is disabled by default. Fixed in 7.15.1, which strips the fragment before generating the Referer value.	5.9	More Details
CVE-2026-16971	The IRIS web application in version 2.4.26 and possibly others does not protect its MFA validation against brute-force attacks.	5.9	More Details
CVE-2026-67355	guzzlehttp/guzzle versions before 7.15.1 fail to preserve host-only cookie scope, storing the request host in the Domain field instead of marking cookies as host-only. Attackers controlling child hosts can receive host-only cookies intended only for parent hosts, potentially disclosing session identifiers and authorization tokens when the same cookie jar is reused across trust boundaries.	5.9	More Details
CVE-2026-63362	An unsigned integer underflow in the PubSub signature verification path in open62541 may allow a remote attacker to cause a denial of service via a crafted UDP packet.	5.9	More Details
CVE-2026-11782	The Points and Rewards for WooCommerce WordPress plugin before 2.10.1 does not have authorisation checks in place on a wallet and points update action that is available to unauthenticated users, and does not verify that the requester owns the account being changed, allowing unauthenticated attackers to arbitrarily modify or corrupt (including driving it negative) the stored wallet balance and loyalty points of any user. Modifying the wallet balance additionally requires the companion Wallet System for WooCommerce Points and Rewards for WooCommerce WordPress plugin before 2.10.1 to be active.	5.9	More Details
CVE-2025-71401	better-auth (npm) before 1.4.2 allows an external request to configure baseURL when it is not otherwise defined (e.g., BETTER_AUTH_URL is unset). An attacker able to make the very first request to the server after startup can poison the router's base path, causing all routes to return 404 for all users (denial of service). The issue is not reachable when baseURL is explicitly configured or on typical managed hosting platforms.	5.9	More Details
CVE-2026-17736	Insufficient validation of untrusted input in WebView in Google Chrome on Android prior to 151.0.7922.72 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)	5.8	More Details
CVE-2026-18369	A flaw was found in Dogtag PKI's ACME responder where the HTTP-01 challenge validator accepts IP address literals as dns identifiers and follows HTTP redirects without validating that the target is a public address. An unauthenticated ACME account holder can exploit this to perform server-side request forgery (SSRF), making the Dogtag server send HTTP GET requests to internal network services. With the InMemory database backend, the response body of internal targets is disclosed to the attacker through the ACME challenge error.	5.8	More Details
CVE-2026-17809	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 151.0.7922.72 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)	5.8	More Details
CVE-	Type Confusion in Tab in Google Chrome on Android prior to 151.0.7922.72 allowed a remote		

2026-17866	attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	5.8	More Details
CVE-2026-17806	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 151.0.7922.72 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)	5.8	More Details
CVE-2026-17891	Use after free in ANGLE in Google Chrome on Android prior to 151.0.7922.72 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)	5.8	More Details
CVE-2026-17776	Policy bypass in Receiver in Google Chrome prior to 151.0.7922.72 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)	5.8	More Details
CVE-2026-68585	SiYuan versions before v3.7.3 contain a metadata disclosure vulnerability in the /api/block/getBlockInfo endpoint that returns document root metadata including title for publish-forbidden documents without publish-access checks. Anonymous readers or publish RoleReader tokens can supply a block ID to retrieve the title, notebook, path, root ID, and icon of documents administrators marked as excluded from publishing.	5.8	More Details
CVE-2026-10526	The EmbedPress WordPress plugin before 4.6.1 does not validate user-supplied URLs before making server-side requests through unauthenticated endpoints, allowing unauthenticated attackers to induce the site to send HTTP requests to internal hosts and services that WordPress core URL validation does not cover (a blind Server-Side Request Forgery).	5.8	More Details
CVE-2026-10686	Zephyr's IPv6 forwarding path re-sent routed unicast packets without ever decrementing the IPv6 hop limit. Both routing branches of ipv6_route_packet() (subsys/net/ip) were affected: the explicit-route path (net_route_packet()) and the on-link cross-interface path (net_route_packet_if()). Each set the packet forwarding flag and called net_send_data() with the hop limit untouched and no expiry check. Per RFC 8200 the hop-limit decrement is the mechanism that bounds packet lifetime and terminates routing loops; without it, a device acting as an IPv6 router relays looping packets indefinitely. An on-path attacker who can induce or exploit a transient L3 loop turns it into a permanent forwarding storm, causing CPU/bandwidth resource exhaustion (availability DoS) on the forwarder and adjacent links; path-discovery and loop diagnostics that rely on hop-limit expiry are also defeated. Affected configurations. In every affected release the forwarding path is reached via CONFIG_NET_ROUTE (enabled by default when CONFIG_NET_IPV6_NBR_CACHE is set), together with CONFIG_NET_ROUTING for cross-interface routing. Note that CONFIG_NET_IPV6_FORWARDING and CONFIG_NET_IPV4_FORWARDING — which appear in the fix and in this advisory's evidence notes — were introduced after v4.4.0, when the routing options were split and renamed; they do not exist in any affected release. When auditing a v4.4.1-or-earlier configuration, look for CONFIG_NET_ROUTE and CONFIG_NET_ROUTING. IPv4 is not affected in any release. The IPv4 forwarding path (net_route_ipv4_packet() in route_ipv4.c) was added after v4.4.0 and has never shipped in a release. Its TTL decrement and IPv4 header-checksum recomputation landed on main as part of the same fix, so the evidence notes below discuss it, but no released version is reachable by way of IPv4. Affected releases are v1.8.0 through v4.4.1: v1.8.0 introduced net_route_packet() and v2.2.0 added net_route_packet_if(), and neither decremented the hop limit. v4.3.1 carries the explicit-route fix but not the on-link one, so it is affected as well. Fixed on main by 7d8f1afa7345 (explicit-route path) and 589eadc74efa (on-link path).	5.8	More Details
CVE-2026-17745	Out of bounds read in Skia in Google Chrome prior to 151.0.7922.72 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)	5.8	More Details
CVE-2026-17746	Use after free in GPU in Google Chrome on Mac prior to 151.0.7922.72 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)	5.8	More Details
CVE-2026-17890	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 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)	5.8	More Details
CVE-2026-17770	Out of bounds read in Media in Google Chrome on Mac prior to 151.0.7922.72 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)	5.8	More Details

CVE-2026-17906	Insufficient validation of untrusted input in Bluetooth in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	5.8	More Details
CVE-2026-17908	Insufficient validation of untrusted input in Printing in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	5.8	More Details
CVE-2026-17893	Insufficient validation of untrusted input in Updater in Google Chrome on Mac prior to 151.0.7922.72 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)	5.8	More Details
CVE-2026-5846	The affected Watchfire Controller Software contains self-signed hard-coded RSA private keys and corresponding X.509 certificates used for authenticating and encrypting HTTPS/TLS connections to the controller's built-in web management interface. These keys are embedded in plaintext within the application patch binaries in the firmware directly from Watchfire's Remote Support filestore.	5.7	More Details
CVE-2026-67550	re2 provides Node.js bindings for Google's RE2 regular expression engine. Prior to 1.25.2, re2 validates lastIndex against the UTF-8 byte length of a subject but uses it as a UTF-16 code-unit offset in exec, test, match, replace, and split, allowing an attacker-influenced lastIndex on a non-ASCII subject to trigger an out-of-bounds heap read and an uncatchable process crash, with limited heap information disclosure in some cases. This issue is fixed in 1.25.2.	5.7	More Details
CVE-2026-18257	Improper validity period check for root issuer certificate in CycloneCrypto cryptographic wrapper of S2OPC allows a certificate issued by this root issuer to be considered trusted	5.6	More Details
CVE-2026-18593	A weakness has been identified in vxcontrol PentAGI up to 2.1.0. This affects an unknown part of the file backend/pkg/templates/prompts/pentester.tmpl of the component Tool Management Protocol Handler. Executing a manipulation can lead to sandbox issue. It is possible to launch the attack remotely. The attack requires a high level of complexity. It is indicated that the exploitability is difficult. 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.	5.6	More Details
CVE-2026-20494	In wifi, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10960006 / BORA00155314, BORA00155001, BORA00154907; Issue ID: MSV-7570.	5.5	More Details
CVE-2026-68743	A flaw was found in SSSD. The extract_authtok_v1() function in the PAM responder does not validate the auth_token_length field against the remaining buffer size before processing. A local attacker can exploit this via a crafted protocol v1 request to the PAM responder socket, causing an out-of-bounds read and process crash, resulting in a denial of service.	5.5	More Details
CVE-2026-17973	Inappropriate implementation in Views in Google Chrome on Mac prior to 151.0.7922.72 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	5.5	More Details
CVE-2026-59919	Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.136.Final and 4.2.16.Final, Netty's HAProxy encoder (HAProxyMessageEncoder) writes AF_UNIX source and destination socket addresses into the HAProxy V1 text protocol without validating them for CRLF characters, so an attacker who controls an AF_UNIX address can inject \r\n sequences and split the single PROXY header into multiple lines. This is possible because the V1 protocol uses CRLF as its line terminator and, unlike IPv4/IPv6 addresses whose format checks implicitly reject CRLF, AF_UNIX addresses are only validated for length (up to 108 bytes), allowing a forged second PROXY header line that spoofs the client source/destination IP to a downstream server or load balancer. The issue is fixed in versions 4.1.136.Final and 4.2.16.Final.	5.5	More Details
CVE-2026-70592	Ghost is a Node.js content management system. From 1.20.1 until 6.54.1, an Administrator-level user could remotely overwrite certain files on the filesystem through the database backup filename, leading to integrity and availability issues. The database export endpoint failed to reject path separators in the caller-supplied filename. This issue is fixed in version 6.54.1.	5.5	More Details
CVE-	In med, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for		More

2026-20491	exploitation. Patch ID: ALPS10981478 (Note: For MT6890, MT6990, MT6988) / AUTO00851173 (Note: For MT2735, MT2737); Issue ID: MSV-7652.	5.5	Details
CVE-2026-6694	A flaw was found in GIMP's file-png plugin. A remote attacker can exploit this by crafting a malicious Animated Portable Network Graphics (APNG) image containing an oversized tRNS chunk. This can lead to a stack-based buffer overflow (CWE-121), causing the file-png plugin to crash and resulting in a Denial of Service (DoS) for the user.	5.5	More Details
CVE-2026-6695	A flaw was found in GIMP. A remote attacker could exploit this by tricking a user into opening a specially crafted PAA (Paint Shop Pro Array) image file. This vulnerability, a heap-based out-of-bounds write in the decode_lzss() function of the PAA file format plugin, allows data to be written beyond the intended memory buffer. This could lead to heap metadata corruption and potentially enable the attacker to execute arbitrary code on the affected system.	5.5	More Details
CVE-2026-20492	In Audio HAL, there is a possible system becoming unresponsive due to a race condition. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS10960026 (Note: For MT6880, MT6890, MT6990, MT6988) / AUTO00851250 (Note: For MT2735, MT2737); Issue ID: MSV-7583.	5.5	More Details
CVE-2026-17550	A maliciously crafted DWG or DXF file, when parsed through Autodesk AutoCAD, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage this vulnerability to cause a crash or disclose sensitive information.	5.5	More Details
CVE-2026-20476	In ccci, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS10981532; Issue ID: MSV-7660.	5.5	More Details
CVE-2026-68563	A flaw was found in ansible-collection-redhat-leapp. When a remediation task is executed with elevated privileges and the `leapp_old_postgresql_data` option is selected, a PostgreSQL data backup archive is created with insecure permissions. This allows a local non-root user on the managed node to read sensitive archived PostgreSQL data, leading to information disclosure.	5.5	More Details
CVE-2026-18772	Improper input validation vulnerability in Samsung Open Source rlottie allows Oversized Serialized Data Payloads.	5.5	More Details
CVE-2026-18201	Keycloak provides a way to manage identity providers and organizations through its administrative API. A flaw was discovered where an administrator with permission to manage identity providers could link a new provider to an organization without having the required permissions to manage that organization. This could allow an unauthorized administrator to influence how users log into specific organizations.	5.5	More Details
CVE-2026-68742	A flaw was found in SSSD. The sss_nss_protocol_parse_addr() function in the NSS responder does not validate the addrlen field against the remaining packet body size. A local attacker can exploit this via a crafted GETHOSTBYADDR request to the NSS responder socket, causing an out-of-bounds read and process crash, resulting in a denial of service.	5.5	More Details
CVE-2026-17932	Use after free in DataTransfer in Google Chrome on Windows prior to 151.0.7922.72 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	5.5	More Details
CVE-2026-52857	Wings is the server control plane for Pterodactyl, a free, open-source game server management panel. Prior to 1.13.0, unbounded json, yaml, and xml configuration-file parsers in parser.go can process an oversized non-file parser configuration file and exhaust Wings process memory. This issue is fixed in version 1.13.0.	5.5	More Details
CVE-2026-45376	Decidim is a participatory democracy framework. Prior to 0.30.9, from 0.31.0 before 0.31.5, and in 0.32.0.rc1 before 0.32.0.rc2, the GET /admin/organization/users search interpolates params[:term] into raw Arel.sql ORDER BY similarity expressions before sanitization, allowing an authenticated organization administrator to execute blind PostgreSQL expressions and infer data through timing differences. This issue is fixed in versions 0.30.9, 0.31.5, and 0.32.0.rc2.	5.5	More Details
CVE-2026-20480	In Audio HAL, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS10960023 (Note: For MT6880, MT6890, MT6980D, MT6988, MT6990) / AUTO00851189 (Note: For MT2735, MT3737); Issue ID: MSV-7586.	5.5	More Details

CVE-2026-20478	In Audio HAL, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS10981454 (Note: For MT6880, MT6890, MT6988, MT6990) / AUTO00851293 (Note: For MT2735, MT2737); Issue ID: MSV-7638.	5.5	More Details
CVE-2025-36374	IBM DataPower Gateway is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A privileged user could exploit this vulnerability to expose sensitive information or consume memory resources.	5.5	More Details
CVE-2026-62324	Jodit Editor is a WYSIWYG editor with a built-in file browser & image editor. Prior to 4.12.31, Jodit's sanitizeHTMLElement method fails to use isDangerousUrl to normalize javascript: href values before checking the scheme, allowing case variants, control-byte prefixes, and embedded tabs or newlines to bypass filtering and execute attacker-controlled script when a victim clicks a stored link rendered by an application. This issue is fixed in version 4.12.31.	5.4	More Details
CVE-2026-45086	Decidim is a participatory democracy framework. From 0.31.1 before 0.31.5 and in 0.32.0.rc1 before 0.32.0.rc2, a participant can directly load /admin/demographics/questions/edit_questions and reach the demographics questionnaire editor without the required administrator authorization. The demographics questionnaire editor should require admin access, but the route under /admin/demographics/questions renders the editor interface without checking whether the caller is an admin. A normal participant can load the page and see the live update form action, which proves the protected interface is reachable. This issue is fixed in versions 0.31.5 and 0.32.0.rc2.	5.4	More Details
CVE-2026-63239	A hard-coded AWS IAM credentials vulnerability in Koollab LMS allowed an attacker to access shared multi-tenant S3 buckets and SQS queues, exposing sensitive data and enabling malicious content injection, job manipulation, or email interception.	5.4	More Details
CVE-2026-16548	The Chat Widget: Floating Customer Support Button for 30+ Channels, Supporting SMS, Calls, and Chat WordPress plugin before 1.8.2 does not validate the type, extension, content, or size of files submitted to its public response endpoint and stores them under the uploads directory, so an unauthenticated user can upload arbitrary files. The original extension is discarded (files are stored under a bare UUID), so this does not yield code execution or stored XSS; impact is bounded to disk consumption and content hosting. The storing path requires the channel's response storage or mail-forwarding to be configured.	5.4	More Details
CVE-2026-49131	OPNsense before 26.1.9 contains a stored cross-site scripting vulnerability that allows authenticated attackers with firewall rule management privileges to inject arbitrary HTML or JavaScript by embedding payloads in the firewall rule description field via the filter API endpoint. The unsanitized description value is persisted and later rendered through the default cell formatter in opnsense_bootgrid.js, which assigns raw cell content to innerHTML, causing injected scripts to execute in the browser of any authenticated user who views the Firewall Rules page, enabling session hijacking or credential theft.	5.4	More Details
CVE-2026-67196	Perspective 5.0.0 contains a cross-site scripting vulnerability in the built-in Debug plugin that allows attackers to inject arbitrary HTML and JavaScript by writing table cell values containing unescaped HTML markup, which are interpolated directly into innerHTML during CSV serialization rendering. Attackers can craft table rows with payloads such as unquoted attribute injections containing event handler attributes that bypass RFC 4180 quoting, since angle brackets and event handler attributes are never escaped before assignment, causing malicious scripts to execute in the embedding page's origin.	5.4	More Details
CVE-2026-67310	OpenRemote (org.openremote:openremote) versions <= 1.26.2 contain an insecure direct object reference vulnerability in the setAssetLinks endpoint of AlarmResourceImpl. The realm access check validates only a single realm obtained via realms.stream().findFirst() on a HashSet of realms from the request, rather than all realms. Because HashSet iteration order is non-deterministic, an authenticated attacker who includes alarm-asset links from both their own realm and a victim realm can, with roughly 50% probability per request (retryable), persist cross-tenant links and disclose victim asset names (returned via @Formula fields) through GET requests on the attacker's own alarm. Fixed in 1.27.0.	5.4	More Details
CVE-	The Easy Appointments WordPress plugin through 3.12.26 does not verify that the appointment targeted by its customer-data update action belongs to the current user; the action only checks a shared nonce that any authenticated user can obtain from their own appointment's edit form. A subscriber-level user with an appointment of their own can therefore reuse that nonce to		More

2026-14224	overwrite the customer metadata (email, name, phone, description) of another user's appointment. Because the Easy Appointments WordPress plugin through 3.12.26 then treats that metadata as the appointment's contact data, a subsequent administrator status change with customer notifications enabled delivers the victim's appointment notification to the attacker-controlled email address.	5.4	Details
CVE-2026-67306	FreeRDP versions 3.28.0 and earlier contain an out-of-bounds read vulnerability in the RDP6 planar RLE bitmap decoder functions planar_decompress_plane_rle and planar_decompress_plane_rle_only in libfreerdp/codec/planar.c. Only the 1-byte control byte is bounds-checked; the subsequent 0–15 attacker-declared raw bytes are read without validating that the source buffer contains them. A malicious or compromised RDP server can send a truncated planar-encoded bitmap or surface update (reachable via both the Bitmap Update PDU and RDPGFX Surface Command paths) that causes the client to read past the end of the source buffer. The issue is fixed in FreeRDP 3.29.0.	5.4	More Details
CVE-2026-49132	OPNsense before 26.1.9 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject arbitrary HTML or JavaScript by embedding payloads in the certificate description field via the trust certificate API. The unsanitized description value is persisted and later rendered in the Dashboard Certificates widget through Certificates.js, which interpolates the raw value into HTML attribute and text content sinks without encoding, causing injected scripts to execute in the browser of any authenticated user who views the Dashboard, enabling session hijacking or credential theft.	5.4	More Details
CVE-2026-14848	The Paid Membership Subscriptions WordPress plugin before 3.0.8 does not verify that the subscription being modified through its change-subscription checkout belongs to the current user, allowing any authenticated user with Subscriber-level access and above to take over another member's subscription and overwrite its plan, status and expiration.	5.4	More Details
CVE-2026-54707	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. Prior to 2.6.4, OnionShare CLI/Desktop does not enforce the Receive mode disable_files setting in cli/onionshare_cli/web/receive_mode.py, where ReceiveModeRequest._get_file_stream() writes multipart file[] data to disk despite the text-only setting. This issue is fixed in version 2.6.4.	5.4	More Details
CVE-2026-66316	Origin validation error in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	5.4	More Details
CVE-2026-17728	Inappropriate implementation in Extensions in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	5.4	More Details
CVE-2026-66317	Origin validation error in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform tampering over a network.	5.4	More Details
CVE-2026-	The per-tool permission system (custom roles / role-based tool permissions, introduced in pgAdmin 4 9.3) did not enforce its permission check consistently. In SERVER mode, pgAdmin 4 gates each tool behind a per-tool Flask-Security permission, but the permission decorator (permissions_required) was applied only to a single "front door" route per tool. Every other backend route and Socket.IO handler in that tool's workflow relied solely on pga_login_required/socket_login_required, which check authentication but not the tool permission. The reporter verified three cases against a test build: (1) a user without tools_query_tool permission received 403 on the protected sqleditor initialization route, but the same session went on to connect the server, initialize the viewdata backend chain, and retrieve real table row content; (2) a user without tools_grant_wizard received 403 on the protected acl route, but the same session still enumerated grantable objects, generated GRANT SQL, and successfully applied it -- confirmed database-side via has_table_privilege(); (3) a user without tools_schema_diff received 403 on the protected panel route, but the same session initialized schema diff, enumerated and connected databases, and obtained real DDL differences via the compare_database Socket.IO handler. The reporter also confirmed a related but distinct issue: a non-owner triggering /misc/workspace/adhoc_connect_server against an administrator-owned shared server caused pgAdmin to persist a new server row still owned by the administrator (user_id/shared unchanged from the source), even though the connection attempt itself reported failure. During remediation, the same front-door-only permission gap was found to also affect the ERD, PSQL, and Debugger tools, and the Backup, Restore, Maintenance, and Import/Export	5.4	More

17350	blueprints, none of which were part of the original report; these were fixed using the same pattern as an extension of the reported defect class. An authenticated user who had valid pgAdmin login and a stored, working database connection, but had been explicitly denied a specific tool's permission by an administrator, could therefore still drive that tool end-to-end through its other routes and sockets, including obtaining an interactive psql session over the /pty Socket.IO namespace and invoking backup/restore/maintenance/import-export jobs. Because the bypass only restores access to tools operating over the user's own already-authenticated database connection, it does not grant the user any database privilege they did not already hold; it circumvents pgAdmin's own tool-level access-control policy (an organisational segregation-of-duties control, separate from database-level authorization), letting a user reach a pgAdmin feature an administrator intended to withhold from them, using capabilities their existing database role already permits through other means. Socket.IO event handlers had no permission-aware equivalent of permissions_required; only socket_login_required existed, checking authentication but not the tool permission. Fix adds a socket_permissions_required decorator (mirroring permissions_required, honouring the Administrator bypass, reading permissions via has_permission()) and applies it, alongside permissions_required, as the outermost decorator on every backend route and Socket.IO handler for the affected tools. Regression tests assert 403 on every gated route and socket handler for a permission-less user. This issue affects pgAdmin 4 in SERVER mode: from 9.3 before 9.17.		Details
CVE-2026-68583	luci-app-adblock-fast before 1.2.4-4 contains a stored cross-site scripting vulnerability in the blocklist name field that allows lower-privileged users to inject active HTML. When an administrator views the AdBlock Fast status page, the injected payload executes in the administrator's browser under the LuCI origin.	5.4	More Details
CVE-2026-17734	Inappropriate implementation in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	5.4	More Details
CVE-2026-16292	The Frontend File Manager Plugin WordPress plugin through 23.6 does not perform nonce validation on one of its file-metadata update actions, allowing an attacker to modify the metadata of a logged-in user's uploaded file via a CSRF attack, which can be leveraged to download that file. When guest uploads are enabled, the same action is reachable unauthenticated against any user's file.	5.4	More Details
CVE-2026-70481	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.5.0 until 0.11.0, the standard channel message update and delete handlers accepted any caller holding write access on the channel without checking that the caller wrote the message. Because write access is the same grant a member needs to post, any ordinary participant in a shared standard channel could rewrite or permanently delete another participant message, while group and direct message handlers enforced authorship. This issue is fixed in 0.11.0.	5.4	More Details
CVE-2026-18645	A security flaw has been discovered in danpros HTMLy up to 3.1.1. This affects the function add_content of the file /system/admin/admin.php of the component Admin Content Endpoint. Performing a manipulation of the argument oldfile results in path traversal. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-14864	The JetEngine WordPress plugin before 3.8.12 does not escape a post meta value before outputting it through one of its shortcodes, allowing users with the Contributor role and above to perform Stored Cross-Site Scripting attacks that execute in the context of higher-privileged users such as administrators.	5.4	More Details
CVE-2026-15385	The RT Mega Menu WordPress plugin before 1.5.2 does not perform a capability check on the AJAX action that saves mega-menu configuration and per-menu-item settings; its only gate is a nonce that any logged-in user can read from a standard admin page. A subscriber-level user can therefore enable the mega menu on a site menu and store a menu-item style value that is rendered, without output escaping, into a style attribute on the public navigation. By breaking out of that attribute the user persists a JavaScript event handler that executes for every visitor who hovers the navigation, including administrators, leading to session/site takeover.	5.4	More Details
CVE-2026-16063	The Event Booking Manager for WooCommerce WordPress plugin before 5.3.7 does not sanitise or escape event timeline content submitted by users with post-editing access before storing it and rendering it on the public event page, allowing users with the Author role and above to inject arbitrary JavaScript that executes in the browser of any visitor viewing the event, including administrators.	5.4	More Details

CVE-2026-17761	Insufficient validation of untrusted input in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via malicious network traffic. (Chromium security severity: Medium)	5.4	More Details
CVE-2026-17799	Insufficient validation of untrusted input in Safe Browsing in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass discretionary access control via a malicious file. (Chromium security severity: Medium)	5.4	More Details
CVE-2026-10773	The DHCPv4 client helper net_dhcpv4_msg_type_name() in subsys/net/lib/dhcpv4/dhcpv4.c indexes a static 8-element const char * name table after a faulty bounds check. The guard used msg_type <= sizeof(name) instead of msg_type <= ARRAY_SIZE(name); sizeof returns the byte size of the pointer array (32 on 32-bit, 64 on 64-bit targets) rather than the element count of 8, so message-type values from 9 up to that byte size pass the check and cause name[msg_type - 1] to read past the end of the array. The msg_type value originates from the DHCP MESSAGE TYPE option, which is read as an unchecked raw byte from a received packet (net_pkt_read_u8) and passed unmodified into the lookup. A DHCP server, or any host able to inject a spoofed DHCP reply onto the client's link, can therefore drive the index out of bounds. The out-of-range slot yields a garbage const char * that is then dereferenced by a %s log conversion. The lookup is reached only from a debug log statement (NET_DBG / LOG_DBG), so the out-of-bounds read is triggerable only when the DHCPv4 log module is built at DEBUG level (CONFIG_NET_DHCPV4_LOG_LEVEL_DBG), which is not the default configuration. When that condition holds, the result is an out-of-bounds read and a wild-pointer dereference: most likely a crash of the DHCP client (denial of service) and potentially disclosure of an adjacent pointer's contents through the log output. The fix replaces sizeof with ARRAY_SIZE, restoring the correct 1..8 acceptance window.	5.4	More Details
CVE-2026-28147	Missing Authorization vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 2.0.15.	5.4	More Details
CVE-2026-16064	The Event Booking Manager for WooCommerce WordPress plugin before 5.3.7 does not properly verify authorization on the object being modified when quick-editing events, only checking a global capability, allowing users with the Contributor role and above to modify the title and publication status of arbitrary posts and pages on the site, including content they do not own.	5.4	More Details
CVE-2026-18651	A flaw was found in 389 Directory Server. During SASL PLAIN authentication, the server installs connection-level bind credentials before performing the account-lock check. If the account is subsequently found to be locked, the bind is reported as failed to the client, but the already-installed authenticated state on the connection is not reverted. A client that supplies valid credentials for an account that has been administratively locked can continue to use the same connection with that account's privileges, defeating account lock as an access-revocation control.	5.4	More Details
CVE-2026-16553	GitLab has remediated an issue in GitLab EE affecting all versions from 18.8 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed some sensitive information to be disclosed to an unintended host due to improper handling of upstream requests in virtual registries.	5.4	More Details
CVE-2026-18584	A security vulnerability has been detected in GL.iNet E5800, E750, X2000, X3000, XE3000 and XE300 up to 20260707. Impacted is an unknown function of the file /sdk/v1 of the component eSIM LPA API. Such manipulation leads to improper authorization. The attack can only be initiated within the local network. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	5.4	More Details
CVE-2026-15262	The Admin Columns for ACF Fields WordPress plugin through 0.3.2 does not escape Advanced Custom Fields values before outputting them in the WordPress admin list-table columns, allowing users with contributor-level access or above to store a payload that executes as JavaScript in the session of higher-privileged users who view the affected post-list screen.	5.4	More Details
CVE-2026-15234	The Codeless Page Builder WordPress plugin through 1.1.4 does not sanitize or validate a shortcode attribute before using it as an HTML tag name when rendering content, allowing users with contributor-level access and above to inject arbitrary HTML and JavaScript that executes in the session of any higher-privileged user (such as an administrator) who views the content.	5.4	More Details
CVE-2026-	Inappropriate implementation in Site Isolation in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass site isolation via a crafted HTML page. (Chromium security severity:	5.4	More

17779	Medium)		Details
CVE-2026-14292	The Download Manager WordPress plugin before 3.3.66 does not properly escape a package's title before outputting it in the front-end package templates, allowing users with the Author role or above to store a title that results in arbitrary JavaScript execution in the browser of any user, including unauthenticated visitors, who views a page displaying the package.	5.4	More Details
CVE-2026-17812	Inappropriate implementation in DigitalCredentials in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	5.4	More Details
CVE-2026-12696	The wpForo Forum WordPress plugin before 3.1.2 does not sanitize and escape a user profile field before outputting it inside an HTML attribute on the public participant profile page, allowing users with a subscriber-level account to inject JavaScript that executes in the browser of any visitor who views the profile, including a logged-in administrator.	5.4	More Details
CVE-2026-70367	A Server-Side Request Forgery (SSRF) bypass vulnerability exists in “stunnel” 5.79 and lower when configured in SOCKS proxy mode. This flaw allows a client to bypass intended localhost restrictions by using IPv4-mapped IPv6 addresses (e.g., “::ffff:127.0.0.1”) or unspecified addresses ("0.0.0.0", "::"), enabling access to loopback-only services on the "stunnel" host that should not be network-reachable.	5.4	More Details
CVE-2026-14192	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Stored XSS. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	5.4	More Details
CVE-2026-18570	A flaw was found in the full-scope-disabled client-policy executor within the keycloak-services component. This component is responsible for enforcing security policies during client registration and configuration in Red Hat Build of Keycloak. The issue occurs because the executor only validates the fullScopeAllowed field when it is explicitly provided in a request. By omitting this field, a delegated user can bypass the policy, resulting in a client created with full scope access. This allows the client to obtain tokens with unauthorized role mappings.	5.4	More Details
CVE-2026-18644	A vulnerability was identified in danpros HTMLy up to 3.1.1. Affected by this issue is the function unlink of the file /system/htmly.php of the component Delete Username Endpoint. Such manipulation of the argument File leads to path traversal. The attack can be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-14219	URL redirection to untrusted site ('open redirect') vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Phishing. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	5.4	More Details
CVE-2026-15252	The Search Atlas SEO WordPress plugin before 2.6.12 does not perform a capability or nonce check in one of its AJAX handlers, allowing any authenticated user such as a Subscriber to invoke the site's Google Indexing API integration, submitting or removing the site's URLs from Google's index and consuming its indexing quota.	5.4	More Details
CVE-2025-36431	IBM Sterling B2B Integrator 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.2.0 through 6.2.2.0_1 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details
CVE-2026-17915	Inappropriate implementation in WebView in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	5.4	More Details
CVE-2026-12697	The wpForo Forum WordPress plugin before 3.1.2 does not verify that an AI chat conversation belongs to the requesting user before deleting its messages, allowing users with a subscriber-level account to permanently delete the stored AI chat message history of any other user.	5.4	More Details
CVE-2026-17874	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	5.4	More Details
CVE-	The Tutor LMS WordPress plugin before 4.0.0 does not properly verify that a user has access to the course a Q&A thread belongs to before returning or writing to that thread, allowing		More

2026-14310	authenticated users with subscriber-level access and above who can access any single course to read the Q&A threads of other courses and to inject replies into them.	5.4	Details
CVE-2026-8155	The BuddyPress WordPress plugin before 14.5.0 does not properly enforce authorization on its private messaging endpoints, allowing any authenticated user (Subscriber+) to read, modify, or delete other users' private messages.	5.4	More Details
CVE-2026-17903	Insufficient policy enforcement in Chromecast in Google Chrome prior to 151.0.7922.72 allowed an attacker on the local network segment to inject scripts or HTML into a privileged page via malicious network traffic. (Chromium security severity: Low)	5.4	More Details
CVE-2025-36298	IBM Sterling B2B Integrator 6.1.2.0 through 6.1.2.7_2, 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.1.2.0 through 6.1.2.7_2, 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 Ebics server component is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details
CVE-2026-11383	IBM Tivoli System Automation Application Manager 4.1 and IBM WebSphere Application Server is affected by cross-site scripting in the Administrative Console.	5.4	More Details
CVE-2026-11870	The WP Ghost (Hide My WP Ghost) WordPress plugin before 7.0.05 does not verify that client IP information comes from a trusted proxy before trusting attacker-controllable HTTP headers, allowing unauthenticated attackers to spoof their IP address to bypass the WP Ghost (Hide My WP Ghost) WordPress plugin before 7.0.05's own brute-force protection and to downgrade its firewall by matching a hardcoded whitelisted IP range.	5.4	More Details
CVE-2026-64685	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions prior to 7.1.2-27, the BGR decoder does not check for an end-of-file in every location so a crafted image could result in an heap buffer over-read. This issue has been fixed in version 7.1.2-27.	5.3	More Details
CVE-2026-64607	HttpClient based on the classic i/o model fails to correctly release the underlying connection back to the connection manager if it encounters an invalid or unsupported `Content-Encoding` header value in the response message. Please note this defect does not affect HttpClient based on the async i/o model. This issue affects Apache HttpComponents Client: from 5.0-alpha1 through 5.6.2.	5.3	More Details
CVE-2026-14202	Observable response discrepancy vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Account Footprinting. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	5.3	More Details
CVE-2026-18059	The PixelYourSite – Your smart PIXEL (TAG) & API Manager plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 11.2.1 via the getWooPurchaseEventParams. This makes it possible for unauthenticated attackers to extract WooCommerce purchase metadata — including product names, product IDs, quantities, per-item prices, order totals, currency, and order/transaction IDs — for any existing order by supplying an invalid or arbitrary order key. This is exploitable against any known or enumerated order ID, as the plugin resolves the order from the URL path variable alone and emits the full woo_purchase tracking payload into the page HTML via the pysOptions JavaScript object across its Facebook, Google Analytics, and Google Tag Manager integrations regardless of key validity.	5.3	More Details
CVE-2026-62416	Network Scanner Tool and Network Scanner Tool Lite provided by Sharp Corporation, with the initial configuration, require no authentication and accept files unlimitedly. When the affected products are used with the initial configuration, anyone can connect to them without authentication and upload files unlimitedly. This may cause a denial-of-service (DoS) condition on the PC. Furthermore, if a malicious file is uploaded, a PC user may be tricked to execute the file to attack other entities from that PC.	5.3	More Details
CVE-2026-64635	Improper handling of the returnUrl parameter in the Forgot Password function of Veeam Service Provider Console allows an unauthenticated attacker to control the domain of the generated password reset link. When the targeted user clicks the link delivered by email, the reset code is transmitted to an attacker-controlled host, allowing the attacker to take over the account.	5.3	More Details
CVE-2026-	better-auth versions before 1.6.2 fail to validate the OAuth state parameter against the stored nonce when using cookie-backed state storage without PKCE. Attackers can forge the state	5.3	More

67335	parameter and supply an attacker-controlled authorization code to create authenticated sessions bound to the attacker's external identity or persistently link attacker accounts to victim profiles.		Details
CVE-2026-44103	An unauthenticated remote attacker can inject malicious firmware into the internal charging module because the JupiCore service transmits firmware updates without performing integrity or verification check. Successful exploitation may compromise the integrity of the affected device. This vulnerability could be used in chain with CVE-2026-44104.	5.3	More Details
CVE-2026-17914	Side-channel information leakage in Skia in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	5.3	More Details
CVE-2026-18437	The MailerPress – Newsletter, email marketing & AI automation plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the `mailerpress/v1/contact` endpoint in all versions up to, and including, 1.5.0. This makes it possible for unauthenticated attackers to update contact details.	5.3	More Details
CVE-2026-16536	The Simple Google Calendar Outlook Events Widget WordPress plugin before 3.1.0 does not validate a user-supplied URL before performing a server-side request, allowing unauthenticated attackers to perform Server-Side Request Forgery attacks and, in some cases, read the response of the internal request.	5.3	More Details
CVE-2026-6336	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.6 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an unauthorized user to view project import source information due to a missing authorization check.	5.3	More Details
CVE-2026-58218	A flaw was found in Samba's internal DNS server where unauthenticated TKEY registration requests were added to the TKEY name cache before being rejected. A remote, unauthenticated attacker can exploit this behavior by sending a large number of TKEY requests with arbitrary names, exhausting the cache and evicting legitimate TKEY entries. This can prevent legitimate TSIG authentication for signed DNS queries, resulting in a denial of service.	5.3	More Details
CVE-2026-15337	An issue was discovered in Django 5.2 before 5.2.17 and 6.0 before 6.0.8. `django.utils.translation.check_for_language()` is subject to a potential denial-of-service attack when given many distinct, very long language codes, which are retained as keys in an in-memory cache and consume process memory. Such codes reach the function through the `django.views.i18n.set_language()` view, which is not routed by default. The consumed memory is bounded, since request data is limited by the `DATA_UPLOAD_MAX_MEMORY_SIZE` setting (default 2.5 MB) and the cache holds a fixed maximum number of entries. Earlier, unsupported Django series (such as 5.1.x, 5.0.x, and 4.2.x) were not evaluated and may also be affected. Django would like to thank Jaeyoung Jang for reporting this issue.	5.3	More Details
CVE-2026-67430	MCP Ruby SDK is the official Ruby SDK for Model Context Protocol servers and clients. Prior to 0.23.0, MCP::Server::Transports::StreamableHTTPTransport in the mcp gem does not expire sessions by default, so repeated initialize requests retain unbounded ServerSession objects and can exhaust process memory. This issue is fixed in version 0.23.0.	5.3	More Details
CVE-2026-15830	An issue was discovered in Django 5.2 before 5.2.17 and 6.0 before 6.0.8. GeoDjango's `django.contrib.gis.geos.GEOSGeometry` is subject to a potential denial-of-service when parsing deeply nested `GEOMETRYCOLLECTION` objects supplied as well-known text (WKT), well-known binary (WKB), or hex-encoded WKB, which triggers unbounded recursion and a segmentation fault in the underlying GEOS library. Spatial field lookups and the `django.contrib.gis.forms.GeometryField` form field are also affected. Earlier, unsupported Django series (such as 5.1.x, 5.0.x, and 4.2.x) were not evaluated and may also be affected. Django would like to thank Andrew MacPherson and kimchunbok_ for reporting this issue.	5.3	More Details
CVE-2026-13143	The WP Travel WordPress plugin before 11.8.1 does not verify PayPal Instant Payment Notifications through the PayPal post-back handshake before marking a booking paid, allowing unauthenticated attackers to forge a notification that flips an arbitrary pending booking to a paid and booked state at an attacker-chosen amount.	5.3	More Details
CVE-2026-17567	The Fluent Forms – Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 6.2.8 via the 'transaction' parameter due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to brute-force valid transaction hashes and view sensitive payment receipt data including customer name, email address, billing address, order items, payment method, and payment status belonging to other users. Because submission	5.3	More Details

	ID, form ID, and transaction creation time are either observable or guessable by an attacker, the effective brute-force space is bounded to approximately 900 candidates per second per (submission, form) pair, making exploitation practical without any prior authentication or account.		
CVE-2026-65311	The HTTP server component of ANDRITZ HIPASE-250 (formerly 250 SCALA) in affected versions exposes an undocumented endpoint that changes the server's logging level and target without requiring authentication. A remote, unauthenticated attacker with network access to the service may suppress audit logging, potentially concealing other activity on the system.	5.3	More Details
CVE-2026-18436	The MailPress plugin for WordPress is vulnerable to unauthorized access in versions up to, and including, 1.5.0 via the campaign revision-restore REST endpoint (POST /wp-json/mailpress/v1/campaign/<id>/restore-revision/<revision_id>). The route in the vulnerable range was registered without a permissionCallback, allowing the restoreRevision() handler to run for unauthenticated requests and overwrite a campaign's content_html with any prior revision. This makes it possible for unauthenticated attackers to modify campaign content by restoring an arbitrary revision.	5.3	More Details
CVE-2026-18174	@fastify/forwarded resolves client addresses from the X-Forwarded-For header. In versions before 3.0.2, when the header contains two or more comma separated entries, the parser trims only space characters and does not strip horizontal tabs, even though RFC 7230 defines optional whitespace as both space and tab. As a result, an entry padded with a tab keeps the literal tab in the resolved address string. Applications that make exact string match security decisions on the resolved client IP, such as an allowlist, a blocklist, a per IP rate limit key, or audit log correlation, can be evaded because the tab corrupted string no longer matches the expected value. This does not cross the trust boundary, since a tab corrupted string is not a valid IP and cannot be mistaken for a trusted proxy. The issue is fixed in @fastify/forwarded 3.0.2.	5.3	More Details
CVE-2026-14843	The Events Made Easy WordPress plugin before 3.1.4 does not verify that the requester is authorized to modify the targeted record when handling an unauthenticated data-change request, relying only on a public nonce with no per-record token or ownership check, allowing unauthenticated attackers to overwrite the personal data of any person record.	5.3	More Details
CVE-2026-18582	A security flaw has been discovered in mz-automation libiec61850 up to 1.6.1. This vulnerability affects the function Reporting_RCBWriteAccessHandler of the file src/iec61850/server/mms_mapping/reporting.c of the component Report Sending Path Handler. The manipulation results in free of memory not on the heap. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 1.6.2 is able to resolve this issue. The patch is identified as 5b2a69f44256b8548927d8afdd7ac5f5381abe1e. It is suggested to upgrade the affected component. The vendor was contacted early about this disclosure.	5.3	More Details
CVE-2026-15018	The Database Collation Fix plugin for WordPress is vulnerable to time-based SQL Injection via the 'force-collation-algorithm' parameter in all versions up to, and including, 1.2.10 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires a trigger.txt file to be present in the plugin's directory (/wp-content/plugins/database-collation-fix/trigger.txt), a condition created by DesktopServer integration events such as site creation, copy, import, move, export, or deploy.	5.3	More Details
CVE-2026-11995	The Gutena Forms – Contact Form, Survey Form, Feedback Form, Booking Form, and Custom Form Builder plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.9.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to modify the read/unread status of or permanently trash arbitrary form submission entries belonging to any form. The nonce issued by check_ajax_referer() does not function as an authorization barrier because the nonce action 'gutena_Forms' is emitted to unauthenticated visitors via wp_localize_script() on any public page that contains a Gutena Forms block, making it freely obtainable by anonymous attackers.	5.3	More Details
CVE-2025-14073	The WooCommerce PayPal Payments plugin for WordPress is vulnerable to Sensitive Information Disclosure due to an Insecure Direct Object Reference in all versions up to, and including, 3.3.2 via the `enqueue_paypal_insights_script_on_order_received()` function due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to obtain sensitive order information including order keys, which can then be leveraged to access full customer billing details (name, email, phone, address) via the WooCommerce Store API within a 10-minute grace period after order creation.	5.3	More Details

CVE-2026-66488	Joomla Extension - balbooa.com - Payment bypass in Gridbox < 2.20.2	5.3	More Details
CVE-2026-4604	The Klubraum Membership Request plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `kr_mr_store_settings()` function in all versions up to, and including, 1.1.0. This makes it possible for unauthenticated attackers to update the plugin's settings, including the Klubraum API token and introduction text, effectively hijacking the plugin's integration with the Klubraum service.	5.3	More Details
CVE-2026-66489	Joomla Extension - balbooa.com - Various unauthenticated file system disclosure in Gridbox < 2.20.2	5.3	More Details
CVE-2026-1982	The Persian Elementor (المنتور فارسی) plugin for WordPress is vulnerable to Price Manipulation in all versions up to, and including, 2.8.1. This is due to the plugin trusting a user-supplied payment amount without server-side validation against the configured ZarinPal widget price. This makes it possible for unauthenticated attackers to submit arbitrary payment amounts to the ZarinPal gateway via the 'amount' parameter.	5.3	More Details
CVE-2026-54909	pion/stun is a Go implementation of STUN. Prior to 3.1.3, XORMappedAddress.GetFromAs can panic while parsing a malformed short XOR-MAPPED-ADDRESS attribute in STUN or ICE Binding-response parsing paths, allowing remote denial of service. This issue is fixed in version 3.1.3.	5.3	More Details
CVE-2026-44102	An unauthenticated remote attacker can trigger a firmware update download via the OCPP backend by supplying an invalid firmware file. This will cause the file to remain accessible for a short period before it is deleted due to improper locking during the cleanup process.	5.3	More Details
CVE-2026-13345	The Essential Addons for Elementor WordPress plugin before 6.6.10 does not perform authorization, status, or visibility checks when resolving WooCommerce products in its product-comparison feature, allowing unauthenticated users to disclose the title, price, and SKU of draft, pending, and private products that are otherwise withheld from public view.	5.3	More Details
CVE-2026-67217	cJSON through 1.7.19 applies RFC 6902 JSON Patch operations non-atomically in apply_patch() in cJSON_Utils.c. For a replace operation that is missing its value member, or a move operation whose destination path cannot be resolved, the existing target member is detached and deleted before the operation is fully validated, so the target document is mutated while cJSONUtils_ApplyPatches() or cJSONUtils_ApplyPatchesCaseSensitive() returns a failure status. An attacker who can supply the patch document can destroy addressable members of the target document even though the API reports that the patch failed, defeating the all-or-nothing behavior callers rely on to reject bad patches.	5.3	More Details
CVE-2026-18583	A weakness has been identified in mz-automation libiec61850 up to 1.6.1. This issue affects the function checkDataSetAccess of the file src/iec61850/server/mms_mapping/mms_mapping.c of the component MMS Request Handler. This manipulation causes out-of-bounds read. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 1.6.2 is capable of addressing this issue. Patch name: 062062daf4cb50c7aa76e01d6fb4d58fc9278a7d. Upgrading the affected component is recommended. The vendor was contacted early about this disclosure.	5.3	More Details
CVE-2026-47622	NVIDIA Dynamo for Linux contains a vulnerability where an attacker could cause the generation of error messages that contain sensitive information. A successful exploit of this vulnerability might lead to information disclosure.	5.3	More Details
CVE-2026-12966	The Direct Payments for WooCommerce WordPress plugin before 2.5.3 does not verify that the requester owns the targeted WooCommerce order in several unauthenticated AJAX handlers before changing its status and overwriting its payment metadata, allowing unauthenticated attackers to tamper with other customers' orders, including forging a "payment sent" state, overwriting the payment-method label, and attaching forged payment-proof files.	5.3	More Details
CVE-2026-11904	IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 and IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.	5.3	More Details

CVE-2026-18604	A vulnerability was identified in textPlus Text Message and Call App up to 8.3.5 on Android. This impacts the function DialerActivity of the component com.gogii.textplus. Such manipulation leads to improper export of android application components. The attack needs to be performed locally. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure.	5.3	More Details
CVE-2026-28145	Insufficient Verification of Data Authenticity vulnerability in StylemixThemes MasterStudy LMS allows Manipulating User State. This issue affects MasterStudy LMS: from n/a through 3.7.39.	5.3	More Details
CVE-2026-60011	Sharp and Toshiba Tec MFPs (multifunction printers) fail to properly authorize requests to directly access certain image data stored to the affected product.	5.3	More Details
CVE-2026-14317	The GiveWP WordPress plugin before 4.16.3 does not restrict the set of available payment gateways to those enabled by the administrator, deriving it in part from request input, which allows unauthenticated users to complete donations through a payment gateway the administrator has disabled.	5.3	More Details
CVE-2026-16531	An unauthenticated remote attacker can exploit a path traversal vulnerability in the PCP pmproxy logger servlet using a crafted hostname. This allows arbitrary file and directory creation, potentially leading to a denial of service.	5.3	More Details
CVE-2026-67353	guzzlehttp/guzzle versions before 7.15.1 contain a denial of service vulnerability in the CookieJar that accepts unlimited Set-Cookie header fields with no size restrictions. Attackers can return many large cookies from a malicious server, causing Guzzle to store excessive data in memory and generate oversized Cookie headers that fail in handlers or destination servers.	5.3	More Details
CVE-2026-17978	Side-channel information leakage in WebCodecs in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	5.3	More Details
CVE-2026-43833	Full details and mitigation steps are currently restricted and will be published at a later date.	5.3	More Details
CVE-2026-70487	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.8.8 until 0.11.0, inline direct model metadata accepted client-supplied knowledge attachments without filtering them against the caller's read access. Any authenticated user who knew another user's file id could have the builtin knowledge tools return indexed chunks from that file, causing a read-only cross-user confidentiality loss while leaving knowledge-base permissions and saved workspace model validation unaffected. This issue is fixed in 0.11.0.	5.3	More Details
CVE-2026-18720	A flaw has been found in kalcaddle kodbox 1.67 Build 02. This vulnerability affects unknown code of the file /index.php?plugin/msgWarning/action of the component msgWarning Plugin. Executing a manipulation can lead to improper authorization. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-13692	The PayU CommercePro Plugin WordPress plugin through 3.8.9 does not verify the payment-gateway signature before applying order modifications, allowing unauthenticated attackers to tamper with the totals, shipping and metadata of arbitrary WooCommerce orders.	5.3	More Details
CVE-2026-15250	The Appointment Booking Plugin WordPress plugin before 5.6.8 does not restrict which booking fields an unauthenticated visitor can set through its public booking funnel, allowing an unauthenticated user to assign a privileged booking field such as the approval status and thereby bypass the site's booking approval workflow.	5.3	More Details
CVE-2026-18610	A vulnerability was detected in NewType WebEIP up to 3.0. This affects an unknown part of the file /EIP_Com_FileList.aspx. The manipulation results in improper authentication. It is possible to launch the attack 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-	A vulnerability was determined in o6 open62541 ca356b088ada7dee824d1b4acd07c1ff07ce242b. Impacted is the function UA_Client_getRemoteDataTypes of the file examples/custom_datatype/client_types_custom.c. Executing a manipulation can lead to use after free. It is possible to launch the attack on the local host. The exploit has been publicly disclosed	5.3	More Details

18785	and may be utilized. The project closed the issue report, stating that this is not the official way to report a security vulnerability.		
CVE-2026-67339	guzzlehttp/guzzle versions before 7.14.2 fail to properly isolate Proxy-Authorization headers from origin servers in cURL handlers. Attackers can capture proxy credentials through origin server access logs when requests are redirected, bypassed, or sent through SOCKS proxies that Guzzle misclassifies as direct connections.	5.3	More Details
CVE-2026-11351	The ShinyStat Analytics WordPress plugin before 1.0.17 does not perform any authorization check on one of its REST API endpoints, allowing unauthenticated users to retrieve information about non-published (e.g. draft, pending or private) WooCommerce products.	5.3	More Details
CVE-2026-15257	The RegistrationMagic WordPress plugin before 6.0.9.4 does not perform authorization, ownership or nonce checks on a front-end submission-editing action, allowing unauthenticated attackers to overwrite other users' form submissions and the profile fields of the associated non-administrator WordPress accounts.	5.3	More Details
CVE-2026-18784	A vulnerability was found in o6 open62541 up to 1.5.5. This issue affects the function UA_Client_readNodeClassAttribute of the file src/client/ua_client_highlevel.c. Performing a manipulation results in heap-based buffer overflow. Attacking locally is a requirement. The exploit has been made public and could be used. The project closed the issue report, stating that this is not the official way to report a security vulnerability.	5.3	More Details
CVE-2026-58216	An out-of-bounds read flaw was found in Samba's Kerberos Key Distribution Center's (KDC) password change (kpasswd) service. When processing malformed ASN.1-encoded Kerberos password change request, Samba server miscalculates the structure size and attempts to read up to six bytes beyond the end of the allocated buffer. While this out-of-bounds read typically results in a harmless decryption failure, if the read hits unmapped memory, it causes the KDC process to crash. An authenticated attacker can send a specially crafted kpasswd request containing malformed ASN.1 data to trigger the out-of-bounds read, which may cause the KDC process to terminate, resulting in a denial of service.	5.3	More Details
CVE-2026-17909	Insufficient validation of untrusted input in Isolated Web Apps in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via malicious network traffic. (Chromium security severity: Low)	5.3	More Details
CVE-2026-14305	The WP Delicious WordPress plugin before 1.10.2 does not perform an authorization check on one of its AJAX actions, allowing unauthenticated users to modify limited post metadata (a like counter and an associated identifier list) on arbitrary posts, including inflating the counter and growing the stored metadata without bound.	5.3	More Details
CVE-2026-18648	A vulnerability was detected in Blix Email Blue Mail Calendar App 2.2.305. Impacted is the function FileDirectory.getDataColumn/FileDirectory.getFileFromUri of the component react-native-receive-sharing-intent. The manipulation of the argument _display_name results in path traversal. The attack is only possible with local access. 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-2026-18646	A weakness has been identified in danpros HTMLy up to 3.1.1. This vulnerability affects unknown code of the file /system/htmly.php of the component Author Name Handler. Executing a manipulation of the argument Name can lead to path traversal. The attack may be launched 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.	5.3	More Details
CVE-2026-20316	A vulnerability in the web interface of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to log in to an affected device using a low-privileged account to access sensitive data within the impacted systems. This vulnerability is due to the presence of static user credentials for a low-privileged account. An attacker could exploit this vulnerability by using the account to log in to an affected system. A successful exploit could allow the attacker to log in to the affected system and access sensitive data as the low-privileged user. Note: If the FMC management interface does not have public internet access, the attack surface that is associated with this vulnerability is reduced. Cisco has assigned this security advisory a Security Impact Rating (SIR) of High rather than Medium as the score indicates. The reason is that this vulnerability can be used with other Cisco Secure FMC Software vulnerabilities to elevate privileges.	5.3	More Details
	The RegistrationMagic WordPress plugin before 6.0.9.4 does not properly validate that a one-time		

CVE-2026-15255	password presented in a cookie belongs to the identity being requested before returning front-end form submissions, allowing unauthenticated attackers to read other users' form submission data, including personal information.	5.3	More Details
CVE-2026-67193	Xlight FTP Server before 3.9.5 contains an information disclosure vulnerability that allows unauthenticated attackers to obtain the server's current GetTickCount() value by sending a USER command with a username ending in the :adm suffix. Attackers can trigger the admin protocol path within the standard FTP listener pre-authentication to leak timing information from the FTP 331 response without requiring a separate port or configuration change.	5.3	More Details
CVE-2026-62946	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions prior to both 6.9.13-52 and 7.1.2-27, processing an extremely large JNX file on 32-bit platforms can cause an integer overflow, leading to a heap buffer over-write. This issue has been fixed in versions 6.9.13-52 and 7.1.2-27.	5.1	More Details
CVE-2026-56567	HCL iControl v4.3.0 was affected by Security Misconfiguration vulnerabilities. It involves the public exposure of internal configuration files due to improper web server or application hardening.	5.1	More Details
CVE-2026-18816	A vulnerability was identified in Baserow up to 2.3.2. Affected by this vulnerability is the function verify of the file backend/src/baserow/api/two_factor_auth/views.py of the component 2FA Verify Endpoint. Such manipulation leads to improper authentication. The attack may be launched remotely. This attack is characterized by high complexity. The exploitation appears to be difficult. Upgrading to version 2.3.3 addresses this issue. You should upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	5.0	More Details
CVE-2026-66300	SNOMED International Snowstorm contains a reflected XSS vulnerability within the "Web Route" redirection functionality. An attacker can inject arbitrary JavaScript which will execute upon a target user navigating to a crafted, malicious link. Fixed in 10.12.2 and 10.9.3.	5.0	More Details
CVE-2026-18736	Shlink contains a server-side request forgery vulnerability that allows authenticated API key holders to cause the server to issue arbitrary HTTP GET requests by supplying a crafted long URL during short URL creation with title auto-resolution enabled. Attackers can submit URLs pointing to public hosts that redirect to internal targets, including loopback addresses, link-local ranges, and cloud metadata endpoints such as 169.254.169.254, to exfiltrate internal service information via the HTML title element returned in the short URL creation response.	5.0	More Details
CVE-2026-70588	Ghost is a Node.js content management system. From 5.26.0 until 6.54.1, the Universal Import feature in Ghost Admin failed to properly sanitize imported content resulting in XSS in post content. This issue is fixed in version 6.54.1.	5.0	More Details
CVE-2026-17737	Use after free in Bluetooth in Google Chrome on Android prior to 151.0.7922.72 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)	5.0	More Details
CVE-2026-62363	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions prior to 7.1.2-27, a heap buffer over-write can occur in the fx operation by passing a crafted argument. This issue has been fixed in version 7.1.2-27.	5.0	More Details
CVE-2026-58156	Apache Traffic Server mis-parses ports in URLs and userinfo, allowing port-based access-control bypass. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	4.9	More Details
CVE-2026-16105	A flaw was found in the RoleContainerResource component of Keycloak. The issue occurs because certain name-based endpoints in the admin REST API do not properly enforce authorization checks when managing composite roles. This allows a delegated administrator with manage-realm permissions to remove essential child roles from built-in admin roles, potentially disrupting administrative functions within a realm.	4.9	More Details
CVE-2026-15344	The WP Photo Album Plus plugin for WordPress is vulnerable to generic SQL Injection via the 'table' parameter in all versions up to, and including, 9.2.04.002 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. The export-table endpoint lacks a nonce check, meaning this	4.9	More Details

	vulnerability can also be triggered via CSRF by tricking an authenticated administrator into visiting a malicious page.		
CVE-2026-15403	The Pinpoint Booking System – Version 2 plugin for WordPress is vulnerable to blind SQL Injection via the 'field' parameter in all versions up to, and including, 2.9.9.6.9 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. The nonce required to reach the vulnerable endpoint is emitted on all plugin admin pages loaded under manage_options, making it trivially obtainable by any authenticated administrator.	4.9	More Details
CVE-2026-15951	The Icegram Mailer plugin for WordPress is vulnerable to SQL Injection via the 'fields' parameter in versions up to, and including, 1.0.12. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query in the Icegram_Mailer_Logs_Table::get_logs() function, where each element of the `fields` array received from $_REQUEST['data'] is joined verbatim into the SELECT clause via implode() with no whitelist, escaping, or prepared-statement placeholder. 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-2025-15673	The Import and export users and customers WordPress plugin before 2.4.3 does not restrict the path of a file it reads and displays during a CSV import, allowing high-privileged users to read arbitrary files on the server.	4.9	More Details
CVE-2026-14227	An API session-management flaw in products with the MikroTik RouterOS API enabled are vulnerable to a Insufficient Session Expiration vulnerability. This could allow active sessions to retain their previous permission set after inactivity timeouts or user-group changes. As a result, an authenticated user whose permissions have been reduced may continue accessing information.	4.9	More Details
CVE-2026-15601	The Kirki – Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to Path Traversal (Zip Slip) in all versions up to, and including, 6.0.13 via the extract_zip_file function. This makes it possible for authenticated attackers, with custom-level access and above, to write arbitrary files on the server, which can allow for remote code execution. The install_app, update_app, and get_kirki_template_from_zip code paths accept a user-supplied app src value to construct the download URL, and no sanitization is applied to prevent a crafted ZIP from being fetched and extracted with path-traversing entry names that escape the intended destination directory.	4.9	More Details
CVE-2026-45330	Decidim is a participatory democracy framework. Prior to 0.30.9, from 0.31.0 before 0.31.5, and in 0.32.0.rc1 before 0.32.0.rc2, the identity-document verification admin controllers load pending Authorization records by raw identifier without confirming current_organization ownership, allowing an administrator from one tenant to view, approve, or reject another tenant’s ID-document request. This issue is fixed in versions 0.30.9, 0.31.5, and 0.32.0.rc2.	4.9	More Details
CVE-2026-11973	The WP-Lister Lite for eBay plugin for WordPress is vulnerable to generic SQL Injection via the 'orderby' parameter in all versions up to, and including, 3.8.8 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 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-2026-69090	Admidio before 5.0.11 fails to validate target organization membership in role handlers, allowing authenticated role administrators to delete, activate, deactivate, or edit roles belonging to other organizations. Attackers can supply a role UUID from another organization to groups_roles.php handlers to modify that organization's roles without authorization.	4.9	More Details
CVE-2026-16614	The GSheetConnector – CF7 Google Sheets Connector with Real-Time Sync plugin for WordPress is vulnerable to generic SQL Injection via the 's' parameter in all versions up to, and including, 5.2.1 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. wp_unslash() strips magic-quote protection and sanitize_text_field() does not escape SQL metacharacters, leaving single quotes and other SQL metacharacters intact before the value is interpolated into the query.	4.9	More Details

CVE-2026-6089	The WP CTA plugin for WordPress is vulnerable to Server-Side Request Forgery via the 'sticky_s_media' parameter in imported JSON files in all versions up to, and including, 2.1.2. This is due to the import_sidebars() function passing user-supplied URLs from imported JSON data to file_get_contents() with only FILTER_VALIDATE_URL validation (which allows internal IPs). 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, which can be used to query and modify information from internal services. The response content is saved as a WordPress media attachment, making this a full-read SSRF.	4.9	More Details
CVE-2026-17555	The WPvivid Backup & Migration plugin for WordPress is vulnerable to SQL Injection via the export_data parameter in versions up to, and including, 0.9.131. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. The values are received in prepare_export_post(), passed through sanitize_text_field() and stripslashes(), JSON-decoded, and the attacker-controlled JSON object keys are collected as $posts_ids without integer casting. They are stored in the export task options and later joined with commas and interpolated directly into a `WHERE ID IN (...)` clause inside a $wpdb->get_results() call in export_post_to_xml() (unquoted, numeric context), with no $wpdb->prepare() or esc_sql(). 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-2026-14341	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.8 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user with Maintainer role to modify protected branch configuration due to improper authorization in a projects API endpoint.	4.9	More Details
CVE-2026-16729	undici's setCookie function does not fully sanitize cookie attributes. In undici before 6.28.0, from 7.0.0 up to before 7.29.0, and from 8.0.0 up to before 8.9.0, a domain value is not checked for semicolons and entries in the unparsed array are not sanitized, so attacker-influenced input can inject additional cookie attributes. For example, a domain value containing a semicolon can append attributes such as SameSite, and an unparsed entry can inject attributes such as HttpOnly, without the caller setting them. Applications that pass user-controlled input to these fields, such as multi-tenant or reverse-proxy servers that scope session cookies to a tenant-supplied domain, can have SameSite CSRF protections bypassed, or the Secure, HttpOnly, and SameSite attributes forced, stripped, or overridden. The issue is fixed in undici 6.28.0, 7.29.0, and 8.9.0.	4.8	More Details
CVE-2026-67617	Microweber CMS through 2.0.20 contains a stored cross-site scripting vulnerability in the content tagging system that allows admin-authenticated attackers to inject arbitrary JavaScript by submitting malicious payloads via the tag_names parameter of the GET /api/save_content_admin endpoint, bypassing three independent sanitization controls including XSS middleware that ignores GET requests, a strip_unsafe() function that only matches double-quoted onerror attributes, and a titlecase normalizer that passes HTML decimal entity-encoded payloads through unchanged. Attackers can store malicious scripts that execute without user interaction for every visitor to the public blog page and within the admin post editor, enabling session riding through same-origin fetch requests using the CSRF token embedded in the page.	4.8	More Details
CVE-2025-15675	The Charitable WordPress plugin before 1.8.5.3 does not sanitise and escape one of its campaign image text fields before outputting it in an HTML attribute, allowing users with a high-privilege campaign-management role to perform Stored Cross-Site Scripting attacks that execute on the front-end campaign page.	4.8	More Details
CVE-2025-15669	The Bit Form WordPress plugin before 3.1.4 does not sanitise one of its conversational-form display settings before rendering it on the public-facing form, allowing high-privilege users (such as administrators, who do not hold the unfiltered_html capability on multisite) to store JavaScript that executes in the browser of any visitor who views the form.	4.8	More Details
CVE-2026-16728	undici's retry interceptor can deliver a response whose body length does not match the Content-Length header exposed to the application after a retry or resume of a partial response. In undici before 6.28.0, from 7.0.0 up to before 7.29.0, and from 8.0.0 up to before 8.9.0, a malicious or faulty upstream can return a partial response with a mismatched framing header, close the socket early, and have the retry interceptor assemble a body of a different length while the original Content-Length stays attached. Applications that use the retry interceptor and forward upstream headers and bodies downstream, such as proxies or gateways, may then emit an invalid HTTP response with a stale Content-Length, leading to downstream response desynchronization,	4.8	More Details

	connection hangs, or response corruption. Exploitation requires the retry interceptor enabled, an upstream returning a mismatched partial response, and a downstream forwarder that does not remove or recalculate Content-Length. The issue is fixed in undici 6.28.0, 7.29.0, and 8.9.0.		
CVE-2026-56609	HCL iControl is affected by Weak SSL/TLS Version Supported vulnerability. It was observed that the application was using weak TLS versions such as TLS 1.0 and 1.1. These outdated protocols lack modern security features, making them vulnerable to known attacks and exposing sensitive information during data transmission.	4.8	More Details
CVE-2026-70589	Ghost is a Node.js content management system. From 4.22.0 until 6.54.1, a missing validation check allowed users to redeem subscription offers that were no longer active. This issue is fixed in version 6.54.1.	4.8	More Details
CVE-2026-15233	The Nested Pages WordPress plugin before 3.2.15 does not properly escape post titles before outputting them into HTML attributes on an administrative listing screen, allowing users with the Editor role (or Contributor/Author when the Nested Pages WordPress plugin before 3.2.15 is enabled for the post type) to inject arbitrary JavaScript that executes in the session of any higher-privileged user who views that screen.	4.8	More Details
CVE-2026-13344	The Essential Addons for Elementor WordPress plugin before 6.6.10 does not validate the HTML tag name of the Pricing Table widget title before outputting it, allowing users with Contributor-level access and above to inject JavaScript that will be executed (Stored Cross-Site Scripting) when the page is viewed, including in the session of an administrator previewing or visiting the post.	4.8	More Details
CVE-2026-66400	Grav Login Plugin versions before 3.8.13 contain an insufficient session expiration vulnerability in TokenStorage.php where the findTriplet() method fails to properly validate Remember Me token timestamps. Attackers with a captured Remember Me cookie can authenticate indefinitely instead of the configured timeout period, as the expiry check compares an array to a scalar value which always evaluates incorrectly in PHP.	4.8	More Details
CVE-2026-65325	Apache Traffic Server reuses multiplexed HTTP/2 origin connections without verifying the server certificate covers the new request hostname. This issue affects Apache Traffic Server: from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	4.8	More Details
CVE-2026-54706	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. Prior to 2.6.4, OnionShare CLI/Desktop follows symbolic links in cli/onionshare_cli/web/send_base_mode.py through SendBaseModeWeb.set_file_info() and stream_individual_file(), allowing remote recipients of Share or Website mode to read local files outside the selected directory. This issue is fixed in version 2.6.4.	4.8	More Details
CVE-2026-63237	A TOTP two-factor authentication bypass vulnerability in Koollab LMS allowed an attacker to supply a client-controlled seed to generate a matching one-time password and bypass the second authentication factor, potentially enabling unauthorised access to administrator accounts.	4.8	More Details
CVE-2026-65100	Apache Traffic Server updates the HTTP/2 HPACK dynamic table before confirming the header block encoded successfully, so an encode failure leaves the encoder out of sync with the peer decoder and corrupts subsequent header blocks on the connection. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	4.8	More Details
CVE-2026-14824	The Quiz and Survey Master (QSM) WordPress plugin before 11.2.2 does not properly escape a question setting before outputting it into an unquoted HTML attribute, allowing users with contributor-level access and above to inject arbitrary JavaScript that executes in the browser of any user viewing the affected quiz.	4.8	More Details
CVE-2026-63220	CodeIgniter is a PHP full-stack web framework. In versions prior to 4.7.4, IncomingRequest::isSecure() trusted the X-Forwarded-Proto and Front-End-Https headers from any incoming request, allowing an attacker could spoof these headers and cause the application to incorrectly treat an HTTP request as secure. This may have impacted applications that rely on isSecure(), force_https(), forceGlobalSecureRequests, or similar logic to enforce HTTPS-only access or make security-sensitive decisions. Exploitability depends on deployment configuration. Applications are most exposed if the backend is reachable directly over HTTP, or if a reverse proxy/load balancer forwards client-supplied forwarding headers without stripping or overwriting them. This issue has been fixed in version 4.7.4.	4.8	More Details

CVE-2026-70590	Ghost is a Node.js content management system. Prior to 6.54.1, any staff-level user was able to leak the hashed passwords of other staff users through the Ghost Admin API. An offline password-guessing attack against the hashes could lead to account takeover if successful, but Device Verification should have prevented an attacker from logging in with a recovered password. Depending on the database used, leaked hashes may not have had the correct casing for all characters, increasing the difficulty of a password-guessing attack. This issue is fixed in version 6.54.1.	4.8	More Details
CVE-2026-67612	OpenEMR through 8.2.0 contains a stored cross-site scripting vulnerability in the patient portal template system that allows authenticated administrators to inject arbitrary HTML and JavaScript by storing malicious payloads through the template save mode, which only filters literal PHP open tags. Attackers can exploit the lack of output encoding at the template retrieval endpoint combined with missing HttpOnly cookie attributes to exfiltrate session tokens via document.cookie access, enabling full session hijacking of any admin, clinician, or portal patient who views a poisoned template.	4.8	More Details
CVE-2026-18321	Buffer overflow in NTPsec's Zyfer refclock allows local attacker to crash ntpd	4.7	More Details
CVE-2026-3093	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 14.0 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an attacker to execute arbitrary JavaScript in another user's browser via a crafted URL, due to improper sanitization of user-controlled input.	4.7	More Details
CVE-2026-18738	Shlink versions 5.0.0 through 5.1.5 contain a CSV formula injection vulnerability that allows unauthenticated remote attackers to plant spreadsheet formulas into exported visit data by supplying malicious values in User-Agent, Referer, or request path headers beginning with formula-triggering characters such as =, +, -, or @. Attackers can craft a single unauthenticated request against any short URL to embed DDE or WEBSERVICE formula payloads into CSV cells, which are then executed on an administrator's client machine when the exported CSV file is opened in a spreadsheet application that evaluates formulas.	4.7	More Details
CVE-2026-62343	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions prior to 6.9.13-51 and 7.0.1-0 and above prior to 7.1.2-26, an invalid kernel can cause a heap buffer over-write when performing a morphology operation with a user supplied kernel. This issue has been fixed in versions 6.9.13-51 and 7.1.2-26.	4.7	More Details
CVE-2026-18592	A security flaw has been discovered in osCommerce 4.14.63493. Affected by this issue is the function EmailController of the file app/lib/backend/controllers/EmailController.php of the component Email Template Configuration. Performing a manipulation of the argument email_templates_key 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. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-16296	The Clearfy Cache WordPress plugin before 2.4.3 does not validate the redirect target in its Cyrlitera old-URL redirect handler, passing a decoded request URI to an unsafe redirect function, which allows unauthenticated attackers to redirect visitors to an arbitrary external URL when a non-default option is enabled.	4.7	More Details
CVE-2026-62845	Kamaji is the Hosted Control Plane Manager for Kubernetes. Prior to 26.7.4-edge, the PostgreSQL and MySQL datastore drivers build DDL statements by interpolating the user-supplied DataStoreUsername/DataStoreSchema directly into SQL via fmt.Sprintf, without escaping identifiers. These fields have no format validation, so a value containing a quote character breaks out of the quoted identifier — SQL injection executed over Kamaji's root connection to the shared datastore. etcd driver is not affected.This issue is fixed in version 26.7.4-edge.	4.7	More Details
CVE-2026-20471	In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS10991588 (Note: For MT6880, MT6890, MT6990, MT6988, MT6986, MT6813) / AUTO00851171 (Note: For MT2735, MT2737); Issue ID: MSV-7790.	4.6	More Details
CVE-2026-	Admidio before 5.0.11 does not validate the adm_csrf_token in modules/category-report/preferences.php, which performs persistent Category Report configuration changes based on GET parameters (delete and copy). An attacker can trick an authenticated administrator into	4.6	More

69093	visiting a crafted URL to delete or duplicate Category Report configurations, affecting the integrity and availability of that module's configuration.		Details
CVE-2026-16273	The Narrative Publisher WordPress plugin through 1.0.7 does not restrict write access to a REST-exposed post meta field or escape it when rendering, allowing users with contributor-level access and above to store JavaScript that executes in the browser of any higher-privileged user who views the affected post.	4.6	More Details
CVE-2026-20490	In ccci, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10981501; Issue ID: MSV-7669.	4.4	More Details
CVE-2026-20493	In wifi, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: BORA00154903; Issue ID: MSV-7575.	4.4	More Details
CVE-2026-47487	NVIDIA Triton Inference Server for Linux contains a vulnerability where a user could cause files outside the model repository to be read, written to, or modified by providing a path in the model name to the Triton MLflow plugin. A successful exploit of this vulnerability might lead to denial of service and information disclosure.	4.4	More Details
CVE-2026-18477	A TOCTOU (Time-of-Check Time-of-Use) vulnerability in GNU tar's incremental dumpdir 'X' rename handling allows a local attacker with write access to a directory being backed up to influence the restore process if the attacker has access to the system where the restore is being performed. During restoration, files or directories may be created, renamed or overwritten outside the intended extraction directory. This could lead to unauthorized file modification or, in some cases, privilege escalation. Exploitation does not require the attacker to modify or craft the archive, and standard backup and restore workflows—including extracting into a newly created directory without using the -P option do not mitigate the issue.	4.4	More Details
CVE-2026-20495	In Bluetooth driver, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00488300; Issue ID: MSV-7296.	4.4	More Details
CVE-2026-20496	In geniezone, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11036877; Issue ID: MSV-7132.	4.4	More Details
CVE-2026-20489	In display, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11004274; Issue ID: MSV-7749.	4.4	More Details
CVE-2026-20486	In imgsensor, there is a possible application crash due to incorrect error handling. 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: ALPS11012302; Issue ID: MSV-7833.	4.4	More Details
CVE-2026-18508	A flaw was found in GNU tar. When extracting an archive with the --one-top-level option, hardlink targets are not confined to the designated top-level directory and may resolve relative to the extraction working directory. A crafted archive can create hardlinks that escape the intended boundary and, when combined with a preexisting symbolic link under the working directory, may allow writing outside that boundary during a single extraction.	4.4	More Details
CVE-2026-20488	In display, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11004276; Issue ID: MSV-7757.	4.4	More Details
CVE-2026-17614	A path traversal flaw was found in WildFly's domain mode implementation. The LocalFileRepository.getFile() and getConfigurationFile() methods in wildfly-core/deployment-repository do not validate that the resolved file path remains within the configured repository or configuration root directories. A remote attacker who has obtained the slave host controller secret or compromised a slave host controller can supply a crafted relative path containing directory traversal sequences (e.g., ../../etc/passwd) via the slave-DC wire protocol, causing the Domain Controller to resolve and serve arbitrary files readable by the DC process. This leads to unauthorized disclosure of sensitive information such as configuration files, keystores, and system credentials.	4.4	More Details
CVE-	In TFA, there is a possible out of bounds write due to a missing bounds check. This could lead to		

2026-20472	local denial of service if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10991467; Issue ID: MSV-7764.	4.4	More Details
CVE-2026-59327	Spring Tools for Eclipse stores the Spring Boot DevTools remote secret (spring.devtools.remote.secret) as a plain string attribute on the "Spring Boot DevTools Client" launch configuration. Eclipse persists launch configuration attributes as cleartext XML, either to workspace metadata or, if the user marks the configuration as a shared file, directly into the project tree where it can be committed to version control. This secret is the sole credential protecting the DevTools remote restart/reload endpoint, which accepts and executes arbitrary class bytes on the target application. Anyone able to read the .launch file (via filesystem access, a workspace backup, or a shared VCS repository) can extract the secret and use it to achieve remote code execution against the associated Spring Boot application. Affected Spring Products and Versions: Spring Tools for Eclipse: 5.2.0 and earlier	4.4	More Details
CVE-2026-20484	In TFA, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11053160; Issue ID: MSV-8004.	4.4	More Details
CVE-2026-17706	Insufficient validation of untrusted input in Media in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-17941	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-67529	OpenProject is open-source, web-based project management software. Prior to 17.6.0, GET /api/v3/time_entries and GET /api/v3/cost_entries rendered _links.workPackage.title and _links.workPackage.href through associated_resource in modules/costs/lib/api/v3/time_entries/time_entry_representer.rb and modules/costs/lib/api/v3/cost_entries/cost_entry_representer.rb without checking WorkPackage.visible or view_work_packages, allowing users with view_time_entries or view_cost_entries to read private work package subjects and ids. This issue is fixed in 17.6.0.	4.3	More Details
CVE-2026-67528	OpenProject is open-source, web-based project management software. Prior to 17.6.0, GET /api/v3/custom_options/:id resolved CustomOption records by global numeric id and allowed UserCustomField and GroupCustomField options without checking visible(current_user), so authenticated non-admin users could enumerate sequential custom option ids and read labels belonging to admin_only user or group custom fields. This issue is fixed in 17.6.0.	4.3	More Details
CVE-2026-17942	Side-channel information leakage in SVG in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17755	Incorrect security UI in Extensions in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17763	Inappropriate implementation in GPU in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17939	Insufficient validation of untrusted input in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via malicious network traffic. (Chromium security severity: Low)	4.3	More Details
CVE-2026-13145	The WP Travel WordPress plugin before 11.8.1 does not verify that the booking requested on its customer account dashboard belongs to the current user, allowing any logged-in user to read another customer's booking details, including billing address information, by supplying an arbitrary booking identifier.	4.3	More Details
CVE-2026-17757	Uninitialized Use in Skia in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-	Inappropriate implementation in Autofill in Google Chrome prior to 151.0.7922.72 allowed a		More

2026-17753	remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	Details
CVE-2026-17912	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-16042	The LWS Optimize WordPress plugin before 3.4 does not perform a capability check on its cache-clearing actions, allowing any authenticated user, including Subscribers, to flush the site's caches and force repeated cache rebuilds.	4.3	More Details
CVE-2026-17925	Inappropriate implementation in Cast in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17927	Insufficient policy enforcement in DevTools in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17760	Side-channel information leakage in NoStatePrefetch in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17911	Insufficient policy enforcement in SVG in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17742	Insufficient policy enforcement in Payments in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-16291	The ProfileGrid WordPress plugin before 5.9.9.8 does not verify that a notification belongs to the requesting user before deleting it, allowing any authenticated user such as a Subscriber to delete other users' notifications by enumerating notification identifiers.	4.3	More Details
CVE-2026-17928	Inappropriate implementation in DataTransfer in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17740	Uninitialized Use in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17762	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-67344	ArcadeDB before 26.7.2 fails to enforce the UPDATE_SCHEMA database permission on the ALTER TYPE ... CUSTOM and ALTER TYPE ... BUCKETSELECTIONSTRATEGY SQL operations, which map to setCustomValue and setBucketSelectionStrategy in LocalDocumentType. An authenticated user with only read access (e.g., a read-only API token) can submit these ALTER TYPE statements via the HTTP command endpoint to mutate a type's custom schema metadata and bucket-selection strategy, bypassing the documented updateSchema permission boundary and potentially corrupting schema metadata and record routing.	4.3	More Details
CVE-2026-17934	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17937	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17733	Inappropriate implementation in QUIC in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-	Inappropriate implementation in Autofill in Google Chrome on Android prior to 151.0.7922.72		More

2026-17731	allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	Details
CVE-2026-17730	Side-channel information leakage in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17938	Inappropriate implementation in FullScreen in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17933	Inappropriate implementation in DOMStorage in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-18819	A security vulnerability has been detected in RackTables up to 0.22.0/e5fff9f8aab339798ed47e8c6d7d977ed97a82bd. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The project maintainer confirms: "[I]t seems plausible, in that RackTables does not at this time have any CSRF prevention. You may assign a CVE ID to this, but there is no guarantee it will be handled in urgent, or even timely, manner, or at all."	4.3	More Details
CVE-2026-17943	Inappropriate implementation in Parser in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-67439	OliveTin gives safe and simple access to predefined shell commands from a web interface. Prior to 3000.17.0, the service/internal/api/api.go StartActionAndWait and StartActionByGetAndWait endpoints return full LogEntry output after execution without enforcing the logs permission, allowing a user with exec permission but logs:false to read action output. This issue is fixed in version 3000.17.0.	4.3	More Details
CVE-2026-18009	Insufficient validation of untrusted input in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via malicious network traffic. (Chromium security severity: Low)	4.3	More Details
CVE-2026-16546	The Wired Impact Volunteer Management WordPress plugin before 2.8.2 does not have authorisation checks in one of its AJAX actions, and does not verify that the RSVP being removed belongs to the requesting user, allowing users with a role as low as Subscriber to remove arbitrary users' RSVPs from any volunteer opportunity.	4.3	More Details
CVE-2026-16295	The Clearfy Cache WordPress plugin before 2.4.3 does not perform a capability check in one of its admin-page dispatch paths, allowing any authenticated user such as a Subscriber to render admin-only settings pages and disclose their contents, including administrative nonces, while the canonical page URL correctly restricts access.	4.3	More Details
CVE-2026-16056	The Contest Gallery WordPress plugin before 30.0.7 does not perform any capability or nonce check in one of its handlers, allowing any authenticated user down to Subscriber to read the site's entire stored OpenAI prompt history.	4.3	More Details
CVE-2026-69094	Admidio before 5.0.11 contains an insecure direct object reference vulnerability in the save_temporary mode of mylist_function.php that allows authenticated users to hijack list configurations. Attackers can enumerate global list UUIDs and overwrite admin-curated global lists or other users' private lists by supplying a list_uuid parameter, transferring ownership and demoting global lists to personal configurations.	4.3	More Details
CVE-2026-17972	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-16035	The miniOrange 2FA WordPress plugin before 6.2.7 does not restrict who can trigger its second-factor configuration OTP send, nor bind the OTP recipient to the enrolling user's own address, allowing a low-privileged user to send one-time-passcode emails to arbitrary recipients and to exhaust the site's metered OTP allowance, preventing legitimate users from receiving their second-factor codes.	4.3	More Details

CVE-2026-18008	Inappropriate implementation in Settings in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via malicious network traffic. (Chromium security severity: Low)	4.3	More Details
CVE-2026-18007	Inappropriate implementation in Input in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-12698	The wpForo Forum WordPress plugin before 3.1.3 does not restrict which profile fields a member may set when editing their own account, allowing users with a subscriber-level account to write administrator-controlled account-state and reputation fields on their own profile, including self-activating a pending or banned account and forging their forum reputation score.	4.3	More Details
CVE-2026-18006	Inappropriate implementation in Google Lens in Google Chrome prior to 151.0.7922.72 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-2026-4672	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.4 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user with guest-role permissions to access test report contents they were not authorized to view due to improper access control enforcement.	4.3	More Details
CVE-2026-15831	GitLab has remediated an issue in GitLab EE affecting all versions from 19.1 before 19.1.3 and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user to bypass administrator-configured tool governance policies due to improper authorization enforcement during token generation.	4.3	More Details
CVE-2026-15077	GitLab has remediated an issue in GitLab EE affecting all versions from 19.1 before 19.1.3 and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user to access information from unauthorized projects due to improper neutralization of untrusted content processed by the AI-assisted code review functionality.	4.3	More Details
CVE-2026-18721	A vulnerability has been found in kalcaddle kodbox 1.67 Build 02. This issue affects some unknown processing of the file /user/sso/apiLogin of the component SSO API Login. The manipulation of the argument callbackUrl leads to open redirect. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-14351	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 8.8 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an unauthenticated user to view the title of a confidential issue through a publicly accessible merge request due to improper authorization checks.	4.3	More Details
CVE-2026-18004	Insufficient policy enforcement in Speech in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17976	Insufficient policy enforcement in Extensions in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to bypass discretionary access control via a crafted domain name. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17977	Policy bypass in CSS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17981	Inappropriate implementation in Blink in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17982	Insufficient validation of untrusted input in Cast in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-18003	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details

CVE-2026-17998	Incorrect security UI in Extensions in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17983	Inappropriate implementation in Global Media Controls in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17994	Inappropriate implementation in Media in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-18010	Inappropriate implementation in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via malicious network traffic. (Chromium security severity: Low)	4.3	More Details
CVE-2026-18013	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17944	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-18016	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17945	Insufficient validation of untrusted input in Navigation in Google Chrome prior to 151.0.7922.72 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-2026-10569	IBM UCD - IBM UrbanCode Deploy 7.2 through 7.2.3.23, and 7.3 through 7.3.2.18 and IBM UCD - IBM DevOps Deploy 8.0 through 8.0.1.13, 8.1 through 8.1.2.6, and 8.2 through 8.2.1.0 is susceptible to an Exposure of Sensitive Information Vulnerability in plugin output logs. This exposure could allow an attacker with access to the logs to potentially obtain senstive values related to that step.	4.3	More Details
CVE-2026-17949	Uninitialized Use in GPU in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17700	Insufficient validation of untrusted input in Actor in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-17696	Side-channel information leakage in Media in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-17954	Policy bypass in MHTML in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted MHTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17955	Insufficient validation of untrusted input in Payments in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-5582	The FuseWP plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.24.2. This is due to missing nonce verification on the toggle_sync_status() function. This makes it possible for unauthenticated attackers to toggle the status of sync rules (enable/disable) 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-2026-18019	Side-channel information leakage in Media in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details

CVE-2026-17958	Inappropriate implementation in Views in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-18585	A vulnerability was detected in GL.iNet MT3000, MT6000, BE9300, BE3600, MT3600BE, E5800, BE6500, MT5000, X3000, XE3000 and MT2500 up to 20260707. The affected element is the function nas-web.get_file_list of the component APPS-NAS Module. Performing a manipulation results in heap-based buffer overflow. The attack may be initiated remotely. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	4.3	More Details
CVE-2026-17959	Inappropriate implementation in Network in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17693	Insufficient policy enforcement in FileSystem in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-17960	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass no-referrer policy via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17961	Inappropriate implementation in Session in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-15260	The GEO my WP WordPress plugin before 4.5.5.3 does not perform any ownership or capability check on two of its logged-in AJAX actions, allowing users with subscriber-level access or above to modify or permanently delete other users' and posts' geolocation records by supplying arbitrary record IDs.	4.3	More Details
CVE-2026-17910	Insufficient policy enforcement in NFC in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17689	Uninitialized Use in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-16289	The ProfileGrid WordPress plugin before 6.0.0.0 does not perform authorization checks when listing a group's pending membership requests, allowing any authenticated user such as a Subscriber to disclose the names and request dates of the users awaiting approval to join any group, including private ones.	4.3	More Details
CVE-2026-17964	Incorrect security UI in UI in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17965	Incorrect security UI in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-16564	The Dokan: AI Powered WooCommerce Multivendor Marketplace Solution WordPress plugin before 5.0.9 does not verify order ownership on a REST endpoint that performs bulk order-status changes, allowing users with a Dokan vendor account to modify the status of any WooCommerce order on the marketplace, including orders belonging to other vendors and the store's own customers.	4.3	More Details
CVE-2026-16565	The Dokan: AI Powered WooCommerce Multivendor Marketplace Solution WordPress plugin before 5.0.9 does not verify product ownership on its product-attribute REST write endpoints, allowing users with a Dokan vendor account to modify the product attributes and default attributes of any other vendor's products on the marketplace.	4.3	More Details
CVE-2026-17970	Insufficient validation of untrusted input in Passwords in Google Chrome prior to 151.0.7922.72 allowed an attacker in a privileged network position to perform UI spoofing via malicious network traffic. (Chromium security severity: Low)	4.3	More Details
CVE-	Insufficient policy enforcement in Prefetch in Google Chrome prior to 151.0.7922.72 allowed a		

2026-17662	remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-17963	Inappropriate implementation in SVG in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-67616	Camaleon CMS through 2.9.2, fixed in commit 88ab703, contains a missing authorization vulnerability on the drafts endpoint that allows any authenticated low-privileged user to create draft posts by bypassing role and permission checks. Attackers can send requests to the drafts endpoint using only session authentication to create unauthorized drafts that appear in the administrative drafts queue.	4.3	More Details
CVE-2026-17765	Inappropriate implementation in WebProtect in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17857	Inappropriate implementation in Network in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-9720	The Facturación Electrónica Costa Rica plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.2. This is due to missing or incorrect nonce validation on the (global scope, included by fvcr_admin_page_html) function. This makes it possible for unauthenticated attackers to modify the plugin's configuration, including API tokens, access tokens, economic activity, Hacienda environment mode, invoice and ticket emission flags, exchange rate, and branch settings 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-2026-17859	Inappropriate implementation in Favicons in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17900	Inappropriate implementation in Enterprise in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a malicious file. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17790	Uninitialized Use in ANGLE in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17901	Insufficient validation of untrusted input in Sharing in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via malicious network traffic. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17858	Uninitialized Use in WebNN in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17788	Inappropriate implementation in Blink in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17851	Side-channel information leakage in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-14223	The Easy Appointments WordPress plugin through 3.12.26 does not verify ownership or capability when returning stored customer details, allowing users with subscriber-level access to read any customer's personal information by iterating an identifier.	4.3	More Details
CVE-2026-17904	Insufficient policy enforcement in NFC in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-	Uninitialized Use in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details

17785			
CVE-2026-17783	Inappropriate implementation in Loader in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17782	Incorrect security UI in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17781	Inappropriate implementation in Extensions in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17794	Insufficient validation of untrusted input in Mobile in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-67302	FreeRDP before 3.29.0 (affected versions <= 3.28.0) contains a divide-by-zero vulnerability in the rdpecam camera redirection client. ecam_dev_process_start_streams_request() parses a server-controlled CAM_MEDIA_TYPE_DESCRIPTION from a StartStreamsRequest PDU but validates only Format and Flags, not FrameRateDenominator. When a malicious or compromised RDP server sends a StartStreamsRequest with FrameRateDenominator set to zero, ecam_encoder_context_init() (channels/rdpecam/client/encoding.c) computes FrameRateNumerator / FrameRateDenominator, causing an integer division by zero (SIGFPE) and termination of the FreeRDP client process. Camera redirection must be enabled on the client for the channel to be reachable. Fixed in FreeRDP 3.29.0.	4.3	More Details
CVE-2026-17810	Uninitialized Use in Dawn in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17808	Uninitialized Use in WebGL in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2025-14469	The Theme Editor plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.1. This is due to missing nonce validation on the ms_update AJAX action. This makes it possible for unauthenticated attackers to modify child theme CSS styles via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-17870	Insufficient validation of untrusted input in Cast in Google Chrome prior to 151.0.7922.72 allowed an attacker on the local network segment to leak cross-origin data via malicious network traffic. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17895	Inappropriate implementation in DataTransfer in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17897	Inappropriate implementation in ORB in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17889	Uninitialized Use in WebXR in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17885	Inappropriate implementation in Paint in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17880	Inappropriate implementation in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details

CVE-2026-14847	The Paid Membership Subscriptions WordPress plugin before 3.0.7 does not perform capability or nonce checks on one of its payment-related AJAX actions, allowing any authenticated user with Subscriber-level access and above to disclose the payment details of any member by enumerating the payment identifier.	4.3	More Details
CVE-2026-17798	Inappropriate implementation in Cast in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17879	Inappropriate implementation in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-12376	The Academy LMS WordPress plugin through 3.8.2 does not restrict access to quiz attempt records to their owner, allowing any authenticated user with subscriber-level access and above (enrolled in any single course) to read every user's quiz attempts across the whole site, including personal data such as IP addresses, names, registration dates and quiz results.	4.3	More Details
CVE-2026-14929	The JS Help Desk WordPress plugin before 3.1.4 does not verify ownership of the targeted reply before updating it, allowing any authenticated user (Subscriber and above) to overwrite the content of any support-ticket reply on the site.	4.3	More Details
CVE-2026-17876	Inappropriate implementation in Payments in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17871	Inappropriate implementation in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17802	Side-channel information leakage in GPU in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-10782	The RealHomes Memberships plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.0.9. 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 grant themselves any premium membership tier without completing a PayPal transaction, generating a falsified active payment receipt and gaining unauthorized access to restricted property listing allowances.	4.3	More Details
CVE-2026-2916	The Jeg Kit for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.1.1 via the `enqueue_scripts()` method in `class/dashboard/class-dashboard.php`. The plugin injects a `JkitDashboardOption` JavaScript object containing full plugin inventory (names, versions, paths, active status), system environment details (WordPress version, PHP version, site URLs, server capabilities), and potentially third-party API credentials (Mailchimp API key via `jkit_user_data`) as an inline script on the `post.php` admin page. Because this data is output without any capability check beyond post editing access, any authenticated user with Contributor-level access or above can view this sensitive configuration data by inspecting the page source. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive site configuration data, installed plugin details, and potentially third-party API keys.	4.3	More Details
CVE-2026-67303	FreeRDP before 3.29.0 contains a reachable assertion (WINPR_ASSERT(OutputBufferLength == BytesReturned)) in serial_process_irp_device_control() in channels/serial/client/serial_main.c. When serial device redirection is enabled and a server-controlled IRP_MJ_DEVICE_CONTROL request specifies an unsupported IOCTL with a non-zero OutputBufferLength, CommDeviceIoControl() can fail with BytesReturned = 0, causing the mismatch to trigger the assertion and abort the client process (denial of service).	4.3	More Details
CVE-2026-17905	Inappropriate implementation in SurfaceCapture in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-	Insufficient policy enforcement in GuestView in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity:	4.3	More Details

17815	Medium)		
CVE-2026-70488	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.6 until 0.11.0, the sync cleanup endpoint authorized write access to the knowledge base in the URL but then acted on directory and file ids supplied in the request body without checking that those objects belonged to that knowledge base. A user with write access to one knowledge base could delete directories and remove file embeddings from another knowledge base, causing documents to drop out of retrieval results and breaking chat-with-file for targeted documents without disclosing contents. This issue is fixed in 0.11.0.	4.3	More Details
CVE-2026-63240	An information disclosure vulnerability in Koollab LMS allowed an authenticated learner to obtain correct quiz answers from the course status endpoint without completing the assessment legitimately, compromising the integrity of assessments.	4.3	More Details
CVE-2026-17844	Insufficient validation of untrusted input in Cast in Google Chrome prior to 151.0.7922.72 allowed an attacker on the local network segment to leak cross-origin data via malicious network traffic. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17843	Inappropriate implementation in CSS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-55495	Cloudreve is a self-hosted file management and sharing system. Prior to 4.17.0, the WOPI PUT_RELATIVE handler passes X-WOPI-SuggestedTarget to URI.JoinRaw as a path rather than a filename, allowing slash and dot-dot segments to escape the source file directory and create or conditionally overwrite files elsewhere in the same owner account. This issue is fixed in version 4.17.0.	4.3	More Details
CVE-2026-17775	Inappropriate implementation in PresentationAPI in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17773	Insufficient validation of untrusted input in Cast in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2025-62347	HCL iControl was affected by Improper Input Validation vulnerability. It is vulnerable to unexpected system behavior and potential security bypasses. This was caused by an implementation flaw in an architectural security tactic that fails to properly validate whether the received input matches the expected type.	4.3	More Details
CVE-2026-67350	Serendipity before 2.6.1 contains an open redirect vulnerability in exit.php that allows unauthenticated attackers to redirect users to arbitrary external sites by supplying a malicious Base64-encoded url parameter when the Track Exits plugin is configured with commentredirection set to s9y. Attackers can craft trusted-looking URLs leveraging the legitimate blog domain to conduct phishing, deliver malware, or bypass URL reputation filters.	4.3	More Details
CVE-2026-14226	The Easy Appointments WordPress plugin through 3.12.26 does not require a sufficient capability on one of its appointment-listing REST endpoints, restricting it only to a capability that every authenticated user holds, allowing users with subscriber-level access to read all bookings on the site, including customer names, schedules, and statuses.	4.3	More Details
CVE-2026-55499	Cloudreve is a self-hosted file management and sharing system. Prior to 4.17.0, a single-file share event-stream subscription resolves the share root to the owner’s parent folder and subscribes to that folder topic, allowing an authenticated share recipient to receive names, paths, rename targets, event types, and hashed identifiers for unshared sibling files and folders. This issue is fixed in version 4.17.0.	4.3	More Details
CVE-2026-14231	The LifterLMS WordPress plugin before 10.0.10 does not perform a capability check in one of its select2 query AJAX handlers, only verifying that the user is logged in, allowing any authenticated user with subscriber-level access to read the titles of internal post types such as coupon codes by supplying the post type.	4.3	More Details
CVE-2026-5626	The Survey Form Block plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the get_all_data() function in all versions up to, and including, 1.0.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to export all survey submission data and column metadata.	4.3	More Details

CVE-2026-17772	Out of bounds read in WebGL in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17166	The Event Booking Manager for WooCommerce – Sell Tickets, Event Registration, RSVP & Event Calendar plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.3.7. 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 modify site-wide payment settings — including WooCommerce payment enablement, cart redirect behavior, login requirements for checkout, confirmation page ID, and confirmed ticket statuses — that govern how all event bookings are processed.	4.3	More Details
CVE-2026-17771	Uninitialized Use in Skia in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17769	Insufficient validation of untrusted input in Cast in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17767	Insufficient validation of untrusted input in WebView in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-15235	The MotoPress Hotel Booking WordPress plugin before 6.0.4 does not perform a capability check before returning a booking's full customer details in one of its AJAX actions, allowing any authenticated user with a low-privileged account (Subscriber and above) to read the personal data, including name, email, phone, and address, of any customer.	4.3	More Details
CVE-2026-28144	Insertion of Sensitive Information Into Sent Data vulnerability in Flipper Code WP Maps allows Retrieve Embedded Sensitive Data. This issue affects WP Maps: from n/a through 4.9.6.	4.3	More Details
CVE-2026-17795	Inappropriate implementation in GetUserMedia in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-63242	A business logic vulnerability in Koollab LMS allowed an authenticated learner to set their lesson completion status to completed via the SCORM commit endpoint without viewing the lesson material, compromising training and completion records.	4.3	More Details
CVE-2026-17820	Insufficient policy enforcement in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17907	Side-channel information leakage in Network in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-17817	Inappropriate implementation in ReportingAndNEL in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-70484	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.7.0 until 0.11.0, the legacy chat-completions features block trusted a client-supplied image_generation flag and did not re-check the features.image_generation permission that the direct image routes and native function-calling path enforce. An authenticated user whose image-generation permission had been revoked could still consume the operator's configured image provider through chat completions, spending API credits and provider quota and writing generated files to operator storage, without exposing provider credentials or other users' data. This issue is fixed in 0.11.0.	4.3	More Details
CVE-2026-	Cloudreve is a self-hosted file management and sharing system. Prior to 4.17.0, GET /api/v4/user/search calls SearchActive without adding a StatusActive predicate and serializes matches at RedactLevelUser, allowing any logged-in user to enumerate email addresses and profile metadata for inactive or banned accounts. The service calls userClient.SearchActive, but	4.3	More

55496	despite its name that method filters only by email/nickname keyword and never adds a StatusActive predicate — while the sibling lookups GetActiveByID and GetActiveByDavAccount, defined a few lines above it, do. Search hits are serialized at RedactLevelUser, which includes the email address. This issue is fixed in version 4.17.0.		Details
CVE-2026-17833	Inappropriate implementation in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17829	Insufficient policy enforcement in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17849	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via malicious network traffic. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17777	Inappropriate implementation in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-17659	Inappropriate implementation in SiteIsolation in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	4.2	More Details
CVE-2026-10031	SFTPGo prior to 2.7.4 contains a permission bypass vulnerability that allows authenticated users to circumvent per-directory access controls by creating symbolic links in a permitted directory that point to files in directories where download, upload, or overwrite permissions are denied. Attackers can exploit the create_symlinks permission combined with read and write access in one directory to read or modify files in restricted directories, as operations are authorized against the link's directory permissions rather than the dereferenced target's directory permissions.	4.2	More Details
CVE-2026-17739	Insufficient policy enforcement in Extensions in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to inject arbitrary scripts or HTML (UXSS) via a crafted Chrome Extension. (Chromium security severity: Medium)	4.2	More Details
CVE-2026-17747	Insufficient validation of untrusted input in Payments in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.2	More Details
CVE-2026-18218	A flaw was found in the TokenManager component of the Keycloak identity management service. When an administrator attempts to revoke tokens for a specific application (client) using a "not-before" policy, the revocation may be silently ignored if the overall security realm already has an older, non-zero revocation policy in place. This issue can allow previously issued tokens to remain valid for refreshing sessions and accessing user information even after an administrator has attempted to invalidate them.	4.2	More Details
CVE-2026-15157	undici does not validate the type property of a duck-typed blob-like request body before using it as the Content-Type header on the HTTP/1.1 dispatcher. In undici before 6.28.0, from 7.0.0 up to before 7.29.0, and from 8.0.0 up to before 8.9.0, an application that passes a hand-rolled blob-like body (via request, stream, pipeline, or dispatch) whose type is derived from untrusted input allows an attacker to inject CRLF sequences and append arbitrary HTTP headers, potentially smuggling a second request past the upstream. Native Blob objects are safe because their constructor strips CRLF from the type, and fetch is unaffected because it validates headers, but ecosystem libraries that build duck-typed blob shapes from user input can reach the vulnerable path. This is the same defect class as CVE-2022-35948 and CVE-2026-1527, on a header sink that the earlier fixes did not cover. The issue is fixed in undici 6.28.0, 7.29.0, and 8.9.0.	4.2	More Details
CVE-2026-67293	FreeRDP before 3.29.0 (affected versions <= 3.28.0) contains an improper certificate hostname validation vulnerability. The TLS hostname matcher (tls_match_hostname() in libfreerdp/crypto/tls.c) treats a wildcard pattern such as *.example.com as matching any hostname ending in .example.com, so it incorrectly accepts a wildcard certificate for multi-label subdomains like a.b.example.com (which OpenSSL's X509_check_host() rejects). This weakens TLS server authentication under wildcard-certificate conditions.	4.2	More Details
	Spring Tools for Eclipse renders Spring Boot starter wizard dependency tooltips in a native		

CVE-2026-59328	embedded browser (SWT Browser) with JavaScript enabled. Using untrusted and compromised Initializr endpoints for the Spring Boot starter wizard can result in arbitrary script execution inside the embedded browser when a developer hovers a dependency checkbox in the New Spring Starter Project wizard. Impact is limited to in-IDE UI spoofing and outbound network beaconing rather than full code execution. Affected Spring Products and Versions: Spring Tools for Eclipse: 5.2.0 and earlier	4.2	More Details
CVE-2026-18211	A flaw was found in the secure-client-uris client policy executor within Keycloak core services. This component is responsible for enforcing security requirements on client configurations, such as requiring encrypted connections for redirect URIs. Due to an improper check that only looks at the start of a web address rather than properly verifying the host, an attacker can bypass these security restrictions by using a specially crafted domain name. This could allow an attacker to intercept sensitive authentication codes over unencrypted connections.	4.2	More Details
CVE-2026-17724	Race in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: High)	4.2	More Details
CVE-2026-16970	The IRIS web application in version 2.4.26 and possibly others contains a logout functionality which is ineffective. Stolen session cookies can therefore be misused for a long time.	4.2	More Details
CVE-2026-70480	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.6.34 until 0.11.0, Open WebUI renders vega and vega-lite fenced code blocks in chat content by building a Vega view in the viewer browser without a restricted resource loader. Any user who can place such a block where another user will see it can make that user browser issue attacker-chosen outbound GET requests and read responses from same-origin or CORS-permissive targets into the rendered page. This issue is fixed in 0.11.0.	4.1	More Details
CVE-2026-70591	Ghost is a Node.js content management system. From 0.10.0 until 6.54.1, a Server-Side Request Forgery in Ghost Admin image fetching allowed any staff-level user to perform a blind HTTP GET request against internal hosts. No output was returned, but this could have been used to probe open ports on internal hosts. This issue is fixed in version 6.54.1.	4.1	More Details
CVE-2026-16297	The Clearfy Cache WordPress plugin before 2.4.3 does not restrict the classes allowed when unserializing settings-import data, allowing users with administrator access to perform PHP Object Injection attacks, which may lead to remote code execution when a suitable gadget chain is present in the environment.	4.1	More Details
CVE-2026-18018	Inappropriate implementation in Updater in Google Chrome on Windows prior to 151.0.7922.72 allowed a local attacker to perform UI spoofing via a malicious file. (Chromium security severity: Low)	4.0	More Details
CVE-2026-56569	HCL iControl was affected by Sensitive Data Exposure vulnerabilities. It involves the public exposure of internal configuration files due to improper web server or application hardening.	4.0	More Details
CVE-2026-16791	A temporary file creation vulnerability in the Linux version of Lenovo XClarity Essentials OneCLI 5.5.0 and below could allow a local low-privileged attacker to overwrite or truncate arbitrary local files with program-generated data when OneCLI is executed with elevated privileges.	3.9	More Details
CVE-2026-14222	The Easy Appointments WordPress plugin through 3.12.26 does not perform any capability or nonce check in one of its connection-deletion actions, allowing users with contributor-level access to delete the booking configuration and disable the booking system.	3.8	More Details
CVE-2026-67334	better-auth versions before 1.6.11 fail to delete cached sessions when removing users via admin, anonymous, or SCIM endpoints when secondaryStorage is configured and storeSessionInDatabase is false. Attackers can reuse deleted user session tokens to maintain authentication for up to seven days after account deletion.	3.8	More Details
CVE-2026-14221	The Easy Appointments WordPress plugin through 3.12.26 does not perform capability checks in several of its appointment-management actions, relying only on a nonce that any authenticated user can obtain, allowing users with contributor-level access to read all customers' appointment details and to create, modify, and delete bookings.	3.8	More Details
	A flaw was found in the keycloak-services component of Keycloak, which provides identity and access management services. The issue occurs when a realm administrator uses a wildcard		

CVE-2026-18206	domain (like *.example.com) to restrict which hosts can register or update clients. Due to improper validation, the system accepts any hostname that ends with the specified domain suffix, even if it is not a legitimate subdomain. An attacker who can control the reverse DNS of their connection can bypass these host-based restrictions, potentially allowing unauthorized client modifications.	3.7	More Details
CVE-2026-18569	A flaw was found in the backchannel logout endpoint of the keycloak-services component, which is part of the Red Hat Build of Keycloak. This component handles authentication and session management for applications. The issue occurs when an OIDC identity provider is configured to skip signature validation. In this specific setup, the system incorrectly accepts logout requests that have no cryptographic signature. An attacker who knows certain technical details about a user's session can use this flaw to force that user to be logged out, potentially disrupting their work.	3.7	More Details
CVE-2026-15054	The Bit Form WordPress plugin before 3.1.2 does not enforce a form's active/published status on its public form-submission handlers, allowing unauthenticated users to submit entries to, and fire the configured workflows (such as email notifications) of forms the site owner has deactivated or unpublished.	3.7	More Details
CVE-2026-56608	HCL iControl is affected by Missing Access Control vulnerability. The application failed to enforce proper granular access controls, allowing users to access or view administrator-level functionalities without appropriate authorization.	3.7	More Details
CVE-2026-15381	The WP Go Maps WordPress plugin before 10.1.04 does not properly sanitise and escape a parameter before using it in a SQL query, allowing unauthenticated users to perform SQL injection attacks.	3.7	More Details
CVE-2026-14927	The FluentCart A New Era of eCommerce WordPress plugin before 1.5.3 does not perform any authorization or ownership check before rendering customer order documents keyed on a sequential numeric identifier, allowing unauthenticated visitors to enumerate and disclose customer personal data (names, email addresses, billing and shipping postal addresses, and order details) across the store.	3.7	More Details
CVE-2026-25552	Ghost CLI before 1.30.1 contains an IP spoofing vulnerability that allows unauthenticated remote attackers to bypass rate-limiting controls by manipulating the X-Forwarded-For header through a misconfigured Nginx configuration. Attackers can append attacker-controlled values to the header chain using the $proxy_add_x_forwarded_for directive to present an arbitrary IP address, circumventing Ghost's rate-limiting mechanisms on self-hosted instances.	3.7	More Details
CVE-2026-58187	The Apache Traffic Server multiplexer plugin overruns its chunk-decode buffer on upstream input, enabling denial of service. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	3.7	More Details
CVE-2026-14862	The Support Genix WordPress plugin before 1.4.48 does not properly authorize access to support-ticket attachment downloads, allowing unauthenticated users who obtain the stored attachment file name to download other users' private ticket attachments.	3.7	More Details
CVE-2026-14849	The Paid Membership Subscriptions WordPress plugin before 3.0.7 does not protect the member and payment export files it writes to a predictable location in the uploads directory, allowing unauthenticated users to download the exported member and payment data (including PII) while an export artifact is present.	3.7	More Details
CVE-2026-56568	HCL iControl was affected by Information Exposure Through Verbose Client-Side API Error Messages vulnerabilities. It involves application displays raw server/API error messages to users instead of generic error messages and exposes internal endpoint names, request parameters, error codes, and authentication status	3.7	More Details
CVE-2026-11366	The MonsterInsights WordPress plugin before 11.1.0 does not correctly validate the signature on one of its unauthenticated AJAX actions: when the MonsterInsights WordPress plugin before 11.1.0 is not connected to Google Analytics the HMAC signing key is empty, which lets unauthenticated attackers forge a valid signature and overwrite a MonsterInsights WordPress plugin before 11.1.0 configuration value, disrupting the MonsterInsights WordPress plugin before 11.1.0's server-side analytics in Manual GA4 mode.	3.7	More Details
CVE-2026-	HCL iControl was affected by Auto complete Enabled vulnerabilities. It involves expose sensitive information such as: Valid usernames, Email addresses used for login, Account identifiers If the	3.7	More

56570	system is accessed from shared environments, attackers may enumerate valid usernames through browser suggestions.		Details
CVE-2026-56571	HCL iControl was affected by Improper Error Handling vulnerabilities. It involves Out of memory, null pointer exceptions, system call failure, database unavailable, network timeout, and hundreds of other common conditions can cause errors to be generated.	3.7	More Details
CVE-2026-63236	An improper access control vulnerability in Koollab LMS allowed an unauthenticated attacker to read another user's name, internal identifier, scores, lesson status, lesson position, and cached lesson state via the SCORM API endpoint.	3.7	More Details
CVE-2026-63235	An improper access control vulnerability in Koollab LMS allowed an unauthenticated attacker to forcibly terminate the session of any user given their email address via the login kickout endpoint, resulting in a denial of service.	3.7	More Details
CVE-2026-16068	The Brizy WordPress plugin before 2.8.19 does not properly restrict who can modify its site-global design data and does not sanitise part of that data before outputting it, allowing authenticated users with Author-level access and above to store arbitrary JavaScript that is then served unsanitised on the site's front-end pages and executes in the browser of every visitor, including administrators.	3.5	More Details
CVE-2026-13393	The ElementsKit Elementor Addons WordPress plugin before 3.10.01 does not sanitize or escape certain megamenu menu-item settings before storing them and outputting them on the front end, and does not require the unfiltered_html capability to save them, allowing users with administrative capabilities to store malicious JavaScript; on a multisite network this lets a non-super subsite Administrator, who is denied unfiltered_html, plant a stored Cross-Site Scripting payload that executes in the sessions of the network Super Admin and site visitors.	3.5	More Details
CVE-2026-17902	Inappropriate implementation in Editing in Google Chrome on Linux prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	3.5	More Details
CVE-2026-18217	A flaw was found in the SAML protocol implementation of Keycloak, an open-source identity and access management solution. The issue occurs when Keycloak handles SAML authentication requests using the HTTP-Redirect binding. If a client is configured with a wildcard redirect URL, an attacker can craft a request that includes malicious parameters. When a user authenticates, Keycloak appends its legitimate response to the attacker's parameters. This can cause some service providers to process the attacker's data instead of the real login information, potentially leading to a user being logged into the wrong account.	3.4	More Details
CVE-2026-18209	A flaw was found in the keycloak-services component of Keycloak, which handles OpenID Connect (OIDC) authentication flows. The issue occurs because the security check designed to prevent HTTP parameter pollution only inspects the query portion of a redirect URL and ignores the fragment portion. When a client is configured with a wildcard redirect URI, an attacker can use this to inject duplicate security parameters into the login response. If a client application is not configured correctly, it might trust the attacker's injected data instead of the real security information from Keycloak, leading to session fixation or account confusion.	3.4	More Details
CVE-2026-17766	Insufficient validation of untrusted input in Clipboard in Google Chrome on Android prior to 151.0.7922.72 allowed a local attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	3.3	More Details
CVE-2026-18790	A weakness has been identified in Systerel S2OPC up to 1.7.3. This affects the function LockedStaMac_ProcessMsg_DeleteMonitoredItemsResponse of the file src/ClientServer/frontend/client_wrapper/internal/state_machine.c of the component DeleteMonitoredItemsRequest Handler. This manipulation causes out-of-bounds read. The attack can only be executed locally. 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.	3.3	More Details
CVE-2026-17984	Inappropriate implementation in Browser in Google Chrome on Android prior to 151.0.7922.72 allowed a local attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	3.3	More Details
	The Spring Boot language server logs the raw value of the https_proxy/HTTPS_PROXY/http_proxy/HTTP_PROXY environment variable at INFO level whenever it creates an outbound HTTP client and no explicit http.proxy workspace setting is configured.		

CVE-2026-59326	Corporate proxy URLs frequently embed Basic-auth credentials in the form http://user:pass@proxy:8080, and the language server writes this value to its log file without any redaction. Since language server log files are often attached to bug reports or are readable by other local users/processes, this can result in disclosure of proxy credentials. Affected Spring Products and Versions: Spring Tools for Eclipse: 5.2.0 and earlier Spring Tools for VSCode / Cursor / Theia: 2.2.0 and earlier	3.3	More Details
CVE-2026-18581	A vulnerability was determined in ggml-org llama.cpp e15efe0. Affected by this issue is some unknown functionality of the file common/jinja/parser.cpp of the component Jinja Minja Template Parser. Executing a manipulation with the input {{9|9|{ can lead to reachable assertion. The attack requires local access. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-68744	A flaw was found in SSSD. The sss_nss_protocol_fill_initgr() function in the NSS responder pre-allocates reply space for all group entries but does not shrink the packet when groups are skipped, causing uninitialized heap bytes to be transmitted to the client. A local attacker can exploit this to disclose cached directory data and heap layout information from the sssd_nss process.	3.3	More Details
CVE-2026-17860	Insufficient validation of untrusted input in Mobile in Google Chrome on Android prior to 151.0.7922.72 allowed a local attacker to spoof the contents of the Omnibox (URL bar) via a malicious file. (Chromium security severity: Medium)	3.3	More Details
CVE-2026-54787	sigstore-go is a Go library for Sigstore signing and verification. Prior to 1.2.1, sigstore-go does not check a bundle signing timestamp against the validity window of an ExpiringKey wrapping a self-managed long-lived signing key without a certificate, which can allow an attacker holding expired key material to sign accepted bundles. This issue is fixed in version 1.2.1.	3.1	More Details
CVE-2026-17997	Inappropriate implementation in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	3.1	More Details
CVE-2026-17715	Inappropriate implementation in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-17732	Inappropriate implementation in SVG in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	3.1	More Details
CVE-2026-18000	Insufficient policy enforcement in USB in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	3.1	More Details
CVE-2025-14562	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 10.6 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user with developer-role permissions to commit changes to a project after being removed as a member, due to improper authorization checks on merge request collaboration settings.	3.1	More Details
CVE-2026-55825	Contao is an Open Source CMS. In versions 5.7.0 through 5.7.6, an authenticated backend user who can access one job can request an attachment identifier containing ../ segments and make the job attachment download endpoint read a file from another job directory inside var/job-attachments. The controller authorizes only the jobUuid route parameter. The later attachment lookup joins that authorized job UUID with the attacker-controlled identifier, then passes the combined path to the virtual filesystem. VirtualFilesystem::resolve() canonicalizes the whole path and only rejects paths that escape the filesystem mount, so authorized-job/../victim-job/debug_log.csv becomes victim-job/debug_log.csv. This is a cross-job authorization bypass for known job attachment paths. It is not a practical brute-force against unknown jobs because job directories are UUID v4 values.	3.1	More Details
CVE-2026-17980	Inappropriate implementation in UI in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	3.1	More Details
CVE-2026-	Inappropriate implementation in CORS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML	3.1	More Details

17957	page. (Chromium security severity: Low)		
CVE-2026-2482	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	3.1	More Details
CVE-2026-17720	Insufficient policy enforcement in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-57232	Contao is an Open Source CMS. From 5.3.35 through 5.3.47 and from 5.7.0-RC1 through 5.7.8, the Feed Reader front-end module passes configured RSS feed URLs from FeedReaderController::getResponse() to feedIo->read() without scheme or private-address validation, allowing a backend user with module-edit permissions to make the server request internal network services, loopback addresses, or cloud metadata endpoints. In core-bundle/src/Controller/FrontendModule/FeedReaderController.php, the getResponse() function iterates over the configured feed URLs and passes each one directly to the HTTP client (via $this->feedIo->read($url, new Feed())) with no validation, while the DCA field definition for rss_feed in tl_module.php carries no URL scheme or host validation and the HTTP client is wired as @psr18.http_client (Symfony HttpClient) with no SSRF protection configured, since NoPrivateNetworkHttpClient is not used. This issue is fixed in versions 5.3.48.	3.1	More Details
CVE-2026-17702	Inappropriate implementation in Skia in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-18682	A security flaw has been discovered in OpenAkita up to 1.27.12. This vulnerability affects unknown code of the file /api/upload of the component File Upload API. The manipulation of the argument File results in cross site scripting. The attack may be performed from remote. A high complexity level is associated with this attack. It is stated that the exploitability is difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2026-63241	An insecure direct object reference vulnerability in Koollab LMS allowed an authenticated user to query the course completion progress of any other user without authorisation, disclosing private learning progress information.	3.1	More Details
CVE-2026-70483	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.6 until 0.11.0, DELETE /api/v1/chats/{id} cancelled a chat's in-flight tasks before checking whether the caller could delete that chat. Any authenticated user who knew another user's chat id could abort that user's running model response, title generation, or tag generation, even though the delete was refused and no chat data was deleted, modified, or disclosed. This issue is fixed in 0.11.0.	3.1	More Details
CVE-2026-17826	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	3.1	More Details
CVE-2026-10684	In subsys/debug/coredump/coredump_shell.c, print_coredump_hdr() used the 16-bit tgt_code field of a stored Zephyr coredump header directly as an index into coredump_target_code2str[], a fixed 7-element array of string pointers, with no bounds check. A stored coredump whose tgt_code is >= 7 causes an out-of-bounds read of a char* up to ~64K entries past the array; that value is passed as the %s argument to shell_print, which dereferences and walks it as a string. The result is either disclosure of device memory contents to the shell user or a crash when the out-of-bounds pointer is unmapped. The defect is reached via the coredump print shell command (cmd_coredump_print_stored_dump -> pretty_print_coredump -> parse_and_print_coredump -> print_coredump_hdr). The tgt_code field is device-generated and in-range during normal crash handling, so triggering requires local shell access plus the ability to stage or corrupt the stored coredump in the flash/in-memory backend. Introduced in v4.2.0 (commit 13abd7fe730) and present through v4.4.0; fixed by clamping out-of-range codes to the 'unknown' (index 0) entry.	3.0	More Details
CVE-2026-16274	The Classified Listing WordPress plugin before 5.4.4 does not perform a capability or ownership check on an AJAX action that returns a post's content, allowing users with contributor-level access and above to read the content of any post, page, or custom post type on the site — including drafts, pending, and private posts owned by other users — regardless of ownership.	2.7	More Details

CVE-2026-16276	The Classified Listing WordPress plugin before 5.4.4 does not perform a capability check on an AJAX action that returns aggregated store revenue totals, allowing users with contributor-level access and above to read daily revenue figures normally restricted to administrators and report managers.	2.7	More Details
CVE-2026-14188	The Easy Appointments WordPress plugin through 3.12.26 does not perform a per-request capability or nonce check on one of its customer-listing handlers, allowing authenticated users with contributor-level access to read every stored customer's personal information.	2.7	More Details
CVE-2026-41709	VMware ESX contains an insufficient logging vulnerability. A malicious administrator could exploit this issue to perform certain operations without them being logged.	2.7	More Details
CVE-2026-16070	The Brizy WordPress plugin before 2.8.19 does not properly verify authorization on the object being modified before updating a template's type meta, validating a request parameter that is different from the one used in the write operation, allowing users with Contributor-level access and above to change the template-type assignment of templates owned by other users.	2.7	More Details
CVE-2026-15231	The Tag, Category, and Taxonomy Manager WordPress plugin before 3.51.0 does not verify that a user is authorized to access a referenced post before processing it and returning derived data, allowing users with contributor privileges to disclose data from private or draft posts they do not own.	2.7	More Details
CVE-2026-63228	An unrestricted image upload vulnerability in Koollab LMS allowed an authenticated attacker to upload malicious content disguised as an image file via the feedback mail registration endpoint, potentially enabling further attacks on the server.	2.6	More Details
CVE-2026-55824	Contao is an Open Source CMS. In versions 4.13.40 through 5.3.46 and 5.7.0-RC1 through 5.7.6, the crawler leaks auth credentials to external hosts. Contao's crawler tries to prevent confidential HTTP client options from being sent to external domains by creating a scoped client: full options for root page origins, cleaned options for everything else. The cleaner removes Cookie and Authorization headers, but it removes the non-Symfony option names basic_auth and bearer_auth instead of Symfony HttpClient's real auth_basic and auth_bearer options. When contao.crawl.default_http_client_options contains Basic or Bearer authentication for a protected staging/production site, those credentials remain in the "clean" client used for external links or configured additional URIs. An attacker who can get an external URL crawled, for example through a link on a crawled page while the broken-link checker is enabled, can receive the crawler credentials. This issue has been fixed in versions 5.3.47 and 5.7.7.	2.6	More Details
CVE-2026-18739	A flaw was found in popt, a command-line option parsing library. An off-by-one error in the poptStuffArgs function, when repeatedly called by a host application or through deep alias nesting, can lead to corruption of internal program data. This corruption could potentially enable a local attacker to execute arbitrary code if the host application then unsafely processes the altered data.	2.5	More Details
CVE-2026-10774	Zephyr's Bluetooth Mesh subnet key management leaks one PSA Crypto key slot on every subnet-key teardown. In subsys/bluetooth/mesh/subnet.c, net_keys_create() imports the Private Beacon Key into a PSA key slot under CONFIG_BT_MESH_PRIV_BEACONS (enabled by default), but subnet_keys_destroy() guarded the matching psa_destroy_key() with CONFIG_BT_MESH_V1d1. That Kconfig symbol was removed when explicit Mesh 1.0.1 support was dropped, so the destroy branch became permanently dead code and the import is never balanced by a destroy. The imbalanced teardown is reached every time subnet keys are destroyed: deleting a subnet (Config Server NetKey Delete), completing a Key Refresh Procedure (which retires the old key set), and resetting/re-provisioning the node. The over-the-air triggers are processed only under the node's device key, so they are exercisable by the provisioner or network administrator that owns the node, reachable over the Bluetooth Mesh network. With the default CONFIG_MBEDTLS_PSA_KEY_SLOT_COUNT of 16, repeated add/delete or key-refresh cycles exhaust the shared PSA key-slot pool after roughly a dozen rounds. Once exhausted, bt_mesh_private_beacon_key() and thus subnet creation fail: the node can no longer add subnets or complete key refresh, and other PSA crypto consumers on the device may be starved, until the device is rebooted. The fix aligns the destroy guard with the import guard (CONFIG_BT_MESH_PRIV_BEACONS) so each slot is freed.	2.4	More Details
CVE-2026-63545	Sharp and Toshiba Tec MFPs (multifunction printers) caches data internally when printing, and leave them uncleared. They may be accessed later by other users.	2.4	More Details

CVE-2026-18011	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a local attacker to obtain potentially sensitive information from process memory via physical access to the device. (Chromium security severity: Low)	2.4	More Details
CVE-2026-18817	A security flaw has been discovered in Baserow up to 2.3.2. Affected by this issue is the function BaserowImpersonateAuthTokenSerializer of the file backend/src/baserow/api/admin/users/serializers.py of the component Inactive Non-Staff User Handler. Performing a manipulation results in improper authorization. Remote exploitation of the attack is possible. The complexity of an attack is rather high. The exploitation is known to be difficult. The presence of this vulnerability remains uncertain at this time. Upgrading to version 2.3.3 can resolve this issue. The affected component should be upgraded. The project maintainer explains: "While the problem exists, I'm not really sure if it's a vulnerability. (....) Even though the back gives a token for a deactivate user, none of the endpoints actually work. That said, we will fix it, but so far it seems more like a bug instead of a vulnerability."	2.2	More Details
CVE-2026-66401	FreeRDP before 3.29.0 contains an out-of-bounds heap read vulnerability in the UVC H.264 extension-unit parser that fails to validate descriptor length before accessing the GUID field. A local attacker with a malicious USB video camera can trigger a heap read beyond allocated bounds during camera stream setup, causing denial of service.	2.1	More Details
CVE-2026-18591	A vulnerability was identified in Meesho Online Shopping App up to 20260607 on Android. Affected by this vulnerability is an unknown functionality of the component com.meesho.supply. Such manipulation of the argument user_id/phone number/email address/name leads to cleartext storage of sensitive information. The attack can be executed directly on the physical device. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure.	2.1	More Details
CVE-2026-65883	Joomla Extension - aimy-extensions.com - RCE via PHP object injection in Aimy Captcha-Less Form Guard 18.0 - 20.0 - A forged clfgd field allows PHP objection injection and thereby remote code execution.	N/A	More Details
CVE-2026-51401	An issue in Vim Project v9.2.0389 and earlier allows a local attacker to execute arbitrary code via the vms_fixfilename() function within file vim/src/os_vms.c	N/A	More Details
CVE-2026-54080	veraPDF PDF parser is a PDF parser for veraPDF. Prior to 1.30.2 and 1.31.23, veraPDF-parser contains a denial-of-service vulnerability in veraPDF-parser/src/main/java/org/verapdf/pd/font/cmap/CMapParser.java and veraPDF-parser/src/main/java/org/verapdf/parser/postscript/PSOperator.java, where a crafted Type 0 font /Encoding or /ToUnicode CMap stream can execute unbounded PostScript array allocation or a zero-increment for loop and exhaust validator memory or CPU. This issue is fixed in versions 1.30.2 and 1.31.23.	N/A	More Details
CVE-2026-16881	A code injection vulnerability exists in the LINE Android app prior to version 26.7.2. The profile rendering component does not adequately validate or sandbox externally supplied script content embedded in profile templates. As a result, an attacker who is able to place crafted content in a profile could cause unintended code to execute with the application's privileges when a victim views that profile. A server-side mitigation has been deployed that also protects existing Android clients that have not been updated to version 26.7.2.	N/A	More Details
CVE-2026-51400	An issue in Vim Project v9.2.0389 and earlier allows a local attacker to execute arbitrary code via the vms_fixfilename() function within file vim/src/os_vms.c	N/A	More Details
CVE-2026-64630	A vulnerability allowing a low-privileged user to retrieve report data outside the scope of a shared report link.	N/A	More Details
CVE-2026-8339	A SQL injection vulnerability exists in the Coverity Connect SOAP API for versions between 2024.6.0 and 2026.3.0 (inclusive). A malicious, authenticated threat actor who sends a specially crafted payload can achieve full read access to database contents and other unauthorized commands.	N/A	More Details
	Server-Side Request Forgery vulnerability in malach-it Boruta allows an unauthenticated remote attacker to cause the OAuth/OpenID authorization server to issue outbound HTTP requests to attacker-chosen URIs, including internal services and cloud metadata endpoints. Three code paths		

CVE-2026-54885	fetch remote URIs supplied by the requester without sufficient validation of the target. Boruta.Oauth.Request.Base.fetch_unsigned_request/1 in lib/boruta/oauth/request/base.ex dereferences the OAuth request_uri parameter from the authorization request via Finch.build(:get, request_uri) |> Finch.request(OpenIDHttpClient). Boruta.Openid.parse_registration_params/2 in lib/boruta/openid.ex dereferences the jwks_uri supplied in an OpenID Connect dynamic client registration request. Boruta.Ecto.Clients.refresh_jwk_from_jwks_uri/1 in lib/boruta/adapters/ecto/clients.ex later refreshes the stored jwks_uri for an existing client. In all three paths the only validation is that the URI parses with a scheme (and one of the two request_uri clauses does not even restrict the scheme to http or https). The implementations do not require HTTPS, do not enforce a host or IP allowlist, do not reject loopback, private, link-local, or other non-public ranges after DNS resolution, do not cap response size, and do not constrain redirects. An attacker can therefore steer the server's HTTP client at arbitrary network targets reachable from the Boruta host. This issue affects boruta: from 2.3.2 before 2.3.7.	N/A	More Details
CVE-2026-11836	Insufficient verification of data authenticity in Caliptra Core ROM and Core Firmware (validate_debug_unlock_token()) in subsystem mode allows an attacker with access to the integrator's debug unlock signing service to unlock production debug on an unintended device by presenting a valid token issued for a different device sharing the same debug unlock key hash. The 384-bit challenge nonce continues to prevent replay of previously issued tokens. Practical impact is limited to loss of per-device scope enforcement within a set of devices that share the same unlock authority by design; it does not enable debug unlock on devices outside that set. This issue affects Core ROM: 2.0.0 through 2.0.2, 2.1.0 through 2.1.1; Core Firmware: 2.0.0 through 2.0.1, 2.1.0.	N/A	More Details
CVE-2026-56850	A flaw in Node.js HTTPS Agent connection reuse can cause PFX object-array key collisions, allowing mutual TLS (mTLS) client identities to be reused across requests configured with different client certificates. This vulnerability affects Node.js **26.x**, **24.x**, and **22.x**.	N/A	More Details
CVE-2026-58040	An incomplete fix has been identified in Node.js: HTTPS Agent TLS session reuse skips hostname verification across identity policies (incomplete fix of CVE-2026-48934). This vulnerability affects Node.js **22.x**, **24.x**, and **26.x**.	N/A	More Details
CVE-2026-11835	Time-of-check time-of-use (TOCTOU) vulnerability combined with missing input validation in Caliptra Core ROM (UpdateResetFlow::run()) in subsystem mode allows a compromised local attacker to silently bypass secure boot by supplying an AXI staging address that is not validated against the strap-configured SS_EXTERNAL_STAGING_AREA_BASE_ADDR, enabling firmware to be modified between verification and loading into ICCM. Attestation continues to report the originally verified image digest, masking the compromise. Exploitation requires a compromised MCU firmware with AXI manager access to unprotected SRAM reachable by Caliptra. This issue affects Core ROM: 2.1.0 through 2.1.1.	N/A	More Details
CVE-2026-53431	Authentication Bypass by Capture-replay vulnerability in malach-it Boruta allows an attacker who has obtained a previously valid JWT client assertion to authenticate as the issuing OAuth client after the assertion has expired. Boruta accepts JWT-based client authentication (client_secret_jwt and private_key_jwt token endpoint authentication methods) but never enforces that the assertion's exp claim is in the future. The pre-check helper Boruta.Oauth.Request.Base.check_expiration/1 in lib/boruta/oauth/request/base.ex only verifies that an exp claim is present (it pattern-matches on the existence of the key and returns success), and the Joken token configuration used for signature verification, Boruta.Oauth.Authorization.Client.Token.token_config/0 in lib/boruta/oauth/authorization/client.ex, returns an empty map, so Joken's default exp claim validator is not engaged either. Any attacker who obtains a validly-signed client assertion (for example through logs, reverse proxies, browser tooling, or other observability surfaces) can replay it indefinitely to authenticate as the client and obtain access tokens with that client's privileges. This issue affects boruta: from 2.3.0 before 2.3.7.	N/A	More Details
CVE-2026-51144	Cross Site Scripting vulnerability in Soliton Systems MailZen Management Protal v.2.62, v.2.63 allows a remote attacker to execute arbitrary code via the Role Name, First Name, Last Name, and Username fields.	N/A	More Details
CVE-2026-64631	A vulnerability allowing a low-privileged user to inject SQL and extract database contents.	N/A	More Details
CVE-2026-	Incorrect access control in NASA cFS v7.0.1 allows attackers to arbitrarily remove low-index	N/A	More

67975	subscriptions and add new streams via sending TO_LAB add/remove subscription commands.		Details
CVE-2026-67969	An issue in the HS_MonitorApplications() component of NASA cFS v7.0.1 allows attackers to force the processor to reset via supplying a crafted HS.AppMon_Tbl entry.	N/A	More Details
CVE-2026-67970	Incorrect access control in the DS_SetDestPathCmd() component of NASA cFS v7.0.1 allows attackers to access sensitive components via a path traversal.	N/A	More Details
CVE-2026-13227	An Improper Authorization vulnerability exists in ERPNext version <v16.25.0 and <15.115.0 due to insufficient access control in the whitelisted API method erpnext.crm.doctype.prospect.prospect.get_opportunities. This issue affects ERPNext: before 15.115.0, before 16.26.0.	N/A	More Details
CVE-2026-67973	An issue in the CFDP receive path of NASA cFS v7.0.1 allows attackers to cause a Denial of Service (DoS) via replaying final CFDP PDUs.	N/A	More Details
CVE-2026-67974	A parser boundary flaw in the Software Bus Network (SBN) application's peer subscription message handling in NASA cFS v7.0.1 allows attackers to cause a Denial of Service (DoS) via sending a crafted packet.	N/A	More Details
CVE-2026-54079	veraPDF validation provides PDF/A and PDF/UA validation, feature reporting, and metadata repair. From 1.17.35 until 1.30.2 and 1.31.71, veraPDF-validation contains an XML External Entity (XXE) vulnerability in validation-model/src/main/java/org/verapdf/gf/model/impl/pd/GFPDAcroForm.java in the getdynamicRender() method, where a crafted PDF containing a malicious XFA stream can cause external entity expansion during PDF/UA-1 validation and allow local file disclosure or outbound server-side requests. This issue is fixed in versions 1.30.2 and 1.31.71.	N/A	More Details
CVE-2026-67977	An integer overflow in the Svc::FileDownlink::SendPartial component of fprime framework v4.2.2 allows attackers to cause a Denial of Service (DoS) via a crafted input.	N/A	More Details
CVE-2026-56848	A flaw in Node.js HTTP/2 handling allows `nghttp2_session_mem_send()` to be called re-entrantly while `nghttp2_session_mem_recv()` is executing, resulting in a heap-use-after-free. This vulnerability affects Node.js **26.x**, **24.x**, and **22.x**.	N/A	More Details
CVE-2026-69247	cryptography is a package designed to expose cryptographic primitives and recipes to Python developers. From 44.0.0 until 50.0.0, pkcs7_decrypt_der, pkcs7_decrypt_pem, and pkcs7_decrypt_smime reported the outcome of decrypting a RecipientInfo's encryptedKey in several distinguishable ways, one of which disclosed the exact length recovered from the RSA operation. The same distinction was also observable by timing. An application that decrypts attacker-supplied EnvelopedData and reflects the outcome gives the attacker a Bleichenbacher oracle against the content-encryption key. Decryption ran as RSA PKCS#1 v1.5 decrypt of encryptedKey, build an AES cipher from the result, then AES-CBC decrypt and PKCS#7 unpad. Invalid RSA padding, a valid padding with a bad key length, a correct length with a wrong key, and the real key each failed or succeeded differently. Case 1 is reachable only where the linked library lacks implicit rejection: OpenSSL 3.0 and 3.1, LibreSSL, and BoringSSL. Exploitation requires a service that auto-decrypts untrusted EnvelopedData matching the victim certificate and answers adaptively at high volume, such as an S/MIME gateway or mail filter. This issue is fixed in 50.0.0.	N/A	More Details
CVE-2026-69248	cryptography is a package designed to expose cryptographic primitives and recipes to Python developers. Prior to 49.0.0, if an intermediate constrained CA permits the DNS name foo.example.com, and the leaf certificate has a wildcard in its DNS SAN of *.example.com, python-cryptography's verifier accepts which allows escaping outside of the permitted names. The core issue is in DNSConstraint::matches, where a wildcard pattern was treated as matching a more-specific permitted constraint even though *.example.com can expand to sibling names such as bar.example.com outside foo.example.com. This allows acceptance of an invalid certificate chain. This issue is fixed in 49.0.0.	N/A	More Details
CVE-	python-cryptography is a package designed to expose cryptographic primitives and recipes to Python developers. Prior to 49.0.0, when resolving invalid certificate chains that include duplicate copies of self-signed certificates, the processing recursively invokes the same candidate, leading to an exponential blowup. Although the limitation that the chain depth cannot exceed a specified maximum depth prevents unbounded recursion and guarantees termination, an attacker-		More

2026-69249	controlled certificate chain can lead the processing to easily take more than 5s to reject in testing. This amplification could form the basis for a resource exhaustion denial of service attack. The core issue arises in the recursive nature of build_chain_inner, which does not de-duplicate against previously analyzed candidates. As the correctness of validation is not affected, the integrity of a system cannot be compromised through this vector, only its availability. This issue is fixed in 49.0.0.	N/A	Details
CVE-2026-64633	A vulnerability allowing remote unauthenticated code execution on the agent host.	N/A	More Details
CVE-2026-18236	A vulnerability in the Agent Development Kit (ADK) allows for continuation forgery in tool confirmations. An attacker who is able to manipulate or inject events into the session history can execute unauthorized tools by forging a tool confirmation response. This is possible because the framework did not verify if the target tool was registered to the executing agent, did not validate if the tool actually required confirmation, and did not match the confirmation arguments against the original tool call event in the history.	N/A	More Details
CVE-2026-67673	A stack-based buffer overflow vulnerability exists in the cmd_edl function of OreSat Firmware v1.0. The vulnerability is triggered when processing the edl fw_flash command, where the <filename> argument is copied to a 64-byte stack buffer via memcpy without proper length validation. An attacker with physical access to the UART3 serial interface can exploit this vulnerability by sending a maliciously crafted command with an oversized filename parameter,	N/A	More Details
CVE-2026-14266	7-Zip XZ Decompression Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of 7-Zip. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XZ chunked data. Crafted XZ-compressed data can trigger an overflow of a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-30169.	N/A	More Details
CVE-2026-65986	CVAT is an open source interactive video and image annotation tool for computer vision. Versions 2.5.0 through 2.66.0 contain a XSS vulnerability that can be accessed through annotation guide assets. When CVAT serves the files attached to an annotation guide, it labels them with a media type (Content-Type) that the attacker can influence, so instead of treating an uploaded file as plain data, the victim's browser can be told to treat it as an HTML page and run any JavaScript inside it. This issue has been fixed in version 2.67.0.	N/A	More Details
CVE-2026-56847	A flaw in Node.js Permission Model enforcement allows `trace_events.createTracing().enable()` Writes Trace Logs Outside `--allow-fs-write`. This can lead to confidentiality impact or bypass of the intended security boundary under affected configurations. This vulnerability affects Node.js **22.x**, **24.x**, and **26.x**.	N/A	More Details
CVE-2026-58072	A vulnerability in Veeam Service Provider Console allowing arbitrary file write on the management server, which can lead to remotecode execution.	N/A	More Details
CVE-2026-45084	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Versions 3.4.0 through 3.6.5 contain a denial of service vulnerability in the presence module. When the presence module's handle_publish() function processes a SIP PUBLISH request with an Event: presence header and a message body while the configuration option enable_sphere_check=1 is set, it invokes the get_content_type() macro without first calling parse_content_type_hdr(), causing it to dereference uninitialized or NULL Content-Type parsing state and crash. If a Content-Type header is present but unparsed, msg->content_type->parsed is NULL and is dereferenced as a content_t pointer; if the request lacks a Content-Type header entirely, msg->content_type itself is NULL, and both cases lead to a crash. A remote attacker can therefore cause a denial of service against an affected instance with a single PUBLISH request over UDP or TCP, using either a valid Content-Type: application/pidf+xml request or one with the header removed, and the vulnerable code path itself does not enforce authentication (though a deployment's routing configuration may require it before this route is reached). The issue has been fixed in version 3.6.6 and 4.0.0-rc1.	N/A	More Details
CVE-2026-67188	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details

CVE-2026-52370	A reflected cross-site scripting (XSS) vulnerability in the Forum posting function of O2OA v10 allows attackers to execute arbitrary Javascript in the context of the victim's browser via a crafted URL.	N/A	More Details
CVE-2026-64634	A vulnerability allowing local privilege escalation to the Reporter service context.	N/A	More Details
CVE-2026-56845	An unauthenticated path traversal (LFI) vulnerability exists under /custom-sounds/ when CustomSounds storage is configured to FileSystem. By including ../ sequences in the request path, an attacker can read arbitrary files outside the base directory.	N/A	More Details
CVE-2026-67855	open62541 contains a heap use-after-free in the GDS PushManagement certificate update workflow when UA_ENABLE_GDS_PUSHMANAGEMENT is enabled. This allows a remote attacker to cause a denial of service.	N/A	More Details
CVE-2026-67856	An issue in open62541 v.1.5.5 and before allows a remote attacker to cause a denial of service via crafted CreateSubscription, CreateMonitoredItems(Sampling), Publish, TransferSubscriptions, and DeleteSubscriptions requests	N/A	More Details
CVE-2026-52791	fuse-overlayfs is an implementation of overlayfs in FUSE for rootless containers. Prior to 1.17, the release-1.x C branch preserves SUID and SGID mode bits in main.c during open(O_TRUNC) and truncate handling on a copied-up file, allowing a low-privileged process to leave the upper-layer file with mode 4777. This issue is fixed in version 1.17.	N/A	More Details
CVE-2026-56846	A flaw in Node.js HTTP/2 handling can cause HTTP/2 retained header blocks evade maxSessionMemory and enable remote memory exhaustion. This vulnerability affects Node.js **24.x** and **22.x**.	N/A	More Details
CVE-2026-54693	ZITADEL is an open source identity management platform. From 2.43.0 through 2.71.19, from 3.0.0 until 3.4.11, and from 4.0.0 until 4.15.1, the email and phone self-management API paths in internal/command/user_v2_email.go, internal/command/user_v2_phone.go, and internal/command/user_v2_human.go allowed users to request returned verification codes without the required permission, allowing users to claim ownership of email addresses or phone numbers they do not control and bypass email-based or phone-based security policies. This issue is fixed in versions 3.4.11 and 4.15.1.	N/A	More Details
CVE-2026-58041	A flaw in Node.js node:sqlite allows a stale StatementSyncIterator created through DatabaseSync#createTagStore() to continue executing a cached prepared statement after it has been reset and rebound with new parameters. SQLTagStore resets cached statements using sqlite3_reset() directly, bypassing the iterator invalidation mechanism introduced for StatementSync in recent releases This vulnerability affects Node.js **22.x**, **24.x**, and **26.x**.	N/A	More Details
CVE-2026-58042	A flaw in Node.js can cause dns.resolveAny() Aborts the Node.js Process When a DNS Response Contains More Than 256 A Records. Repeated triggering of this condition can lead to denial of service. This vulnerability affects Node.js **26.x**, **24.x**, and **22.x**.	N/A	More Details
CVE-2026-58073	A vulnerability in Veeam Service Provider Console allowing an unauthenticated attacker to impersonate a managed agent andobtain that agent's credentials.	N/A	More Details
CVE-2026-58074	A vulnerability allowing a high-privileged user to execute arbitrary code on the server.	N/A	More Details
CVE-2026-	Google::Auth versions before 0.09 for Perl allow server side request forgery and credential exfiltration via unvalidated URLs taken from the credentials JSON. The URLs the library requests are read from the credentials JSON, and their hosts were not checked against the universe domain before the request. For an external_account configuration, retrieve_subject_token fetched credential_source.url with headers from the same JSON, and fetch_access_token posted the subject token to token_url, then sent the STS access token it received to service_account_impersonation_url in an Authorization: Bearer header. The authorized_user, impersonated_service_account and service_account configurations posted the client secret and refresh token, the source access token, and a signed JWT assertion to their own JSON-supplied token_uri or impersonation URL. Any caller that builds credentials from a configuration it does not fully control issues those requests from the application's network position, reaching hosts the	N/A	More

66901	configuration names, including internal services and link-local metadata endpoints, and hands them the credentials each request carries. The service_account assertion is bound to aud, so it is not replayable against Google. Version 0.06 added a _validate_url host check to the external_account class, keyed on a universe_domain read from the same credentials JSON. Version 0.07 gated a JSON-supplied universe domain behind GOOGLE_EXTERNAL_ACCOUNT_ALLOW_CUSTOM_UNIVERSES=1, deriving the pin flag from arguments that an earlier BUILDARGS pass had already merged on the make_creds path. Version 0.08 passed the pin decision through as an explicit constructor argument and moved _validate_url to Google::Auth::Credentials, adding the call to UserRefreshCredentials and ImpersonatedServiceAccountCredentials, and 0.09 added it to ServiceAccountCredentials.		Details
CVE-2026-58044	A flaw in Node.js HTTP client can cause a request desynchronization for Node.js-based forwarding proxies that rebuild outbound headers from the visible `IncomingMessage` headers while piping the original body to a reused backend connection. Node.js can omit headers beyond `maxHeadersCount` / `maxHeaderPairs` from `req.headers`, `req.rawHeaders`, and `req.headersDistinct`, while still using those omitted headers internally for HTTP message framing. In particular, `Content-Length` can be hidden from userland while the request body is still delivered. This vulnerability affects all supported release lines: **Node.js 22**, **Node.js 24**, and **Node.js 26**.	N/A	More Details
CVE-2026-41186	When Calico's shared debug server is enabled (disabled by default), the Calico kube-controllers and Goldmane components bind their Go pprof debug listener to 0.0.0.0 without authentication. Any pod with network reachability to the listener can retrieve the process heap, goroutine stacks (including function arguments), and command-line arguments. Depending on the process's in-memory state, the heap may contain sensitive material. The debug listener is opt-in but is unsafe when enabled because it offers no authentication and no safe localhost-only binding option.	N/A	More Details
CVE-2026-67860	open62541 1.5.5 contains a heap-based buffer overflow in the default HistoryRead path when the default history database is used with the memory backend.	N/A	More Details
CVE-2026-67862	open62541 1.5.5 contains a buffer-overflow in the high-level attribute reading logic in src/client/ua_client_highlevel.c. This allows a remote attacker to cause a denial of service.	N/A	More Details
CVE-2026-58045	A flaw in Node.js allows a spoofed `TypedArray` `byteLength` to trigger a reachable assertion in the synchronous `node:zlib` APIs, causing the entire process to crash. All 11 synchronous zlib functions are affected. Repeated exploitation of this condition can result in a denial of service. This vulnerability affects Node.js **22.x**, **24.x**, and **26.x**.	N/A	More Details
CVE-2026-58071	A vulnerability in Veeam Service Provider Console allowing an unauthenticated attacker to access the proxied appliance API asPortal Administrator during a short window after an administrator session begins.	N/A	More Details
CVE-2026-58067	A vulnerability in Veeam Service Provider Console allowing an unauthenticated attacker to exhaust host memory and cause adenial of service.	N/A	More Details
CVE-2026-67979	Incorrect access control in the Executive Services dynamic application start path component of NASA cFS v7.0.1 allows attackers to execute arbitrary code via placing a shared object on target storage.	N/A	More Details
CVE-2026-66051	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-66902	Google::Auth versions before 0.06 for Perl run a command named in an external_account credentials JSON via an ungated system call. The Pluggable subclass reads credential_source.executable.command from the credentials JSON and runs it as `system($command)`, a single argument call that passes the whole string to /bin/sh -c. The executable's environment_variables map from the same JSON is copied into %ENV first. No opt-in gate guards the call. make_creds selects the Pluggable subclass whenever credential_source.executable is present, so the path is reached from the standard Application Default Credentials flow, including a "type": "external_account" configuration read from the file named by GOOGLE_APPLICATION_CREDENTIALS. Configurations without credential_source.executable do not select this subclass and do not reach the call. Any caller that	N/A	More Details

	builds credentials from a configuration it does not fully control runs the embedded command with the privileges of the application process.		
CVE-2026-54081	veraPDF PDF parser is a PDF parser for veraPDF. Prior to 1.30.2 and 1.31.23, veraPDF-parser contains a denial-of-service vulnerability in veraPDF-parser/src/main/java/org/verapdf/pd/font/type1/Type1FontProgram.java and veraPDF-parser/src/main/java/org/verapdf/parser/postscript/PSOperator.java, where a crafted Type 1 font /FontDescriptor /FontFile program can execute unbounded PostScript array allocation, a zero-increment for loop, or self-recursive toExecute user dictionary lookups and exhaust validator memory, CPU, or stack. This issue is fixed in versions 1.30.2 and 1.31.23.	N/A	More Details
CVE-2026-41187	Calico's apiserver wraps tier-scoped resources so that every operation runs through AuthorizeTierOperation, but the Delete override on NetworkPolicy, GlobalNetworkPolicy, and their staged variants is not invoked for DeleteCollection requests. A user holding the deletecollection verb or wildcard verbs on tier-scoped policy resources can bulk-delete policies in tiers they otherwise have no rights on, breaking the tier authorization boundary.	N/A	More Details
CVE-2026-8338	A Spring Security authentication and authorization bypass exists in Coverity Connect versions between 2023.6.0 and 2026.3.0. An unauthenticated malicious threat actor that can send a specially crafted HTTP request is able to bypass authentication and authorization controls on certain API endpoints to access data within Coverity.	N/A	More Details
CVE-2026-54078	veraPDF validation model is an implementation of the veraPDF validation model. From 1.25.73 until 1.30.2 and 1.31.71, veraPDF-validation contains an XML External Entity (XXE) vulnerability in validation-model/src/main/java/org/verapdf/gf/model/tools/DictionaryKeysHelper.java in getRichTextStringOrStreamEntryStringRepresentation(), where a crafted PDF containing a malicious rich-text /RC or /RV entry can cause external entity expansion and reflect local file contents into the validation report. This issue is fixed in versions 1.30.2 and 1.31.71.	N/A	More Details
CVE-2026-56389	GNU Bison allows for an execution of an arbitrary program during HTML report generation due to improper handling of grammar-defined configuration variables. A grammar file can override the executable used for the XML-to-HTML transformation step via %define tool.xsltproc, which is accepted without restriction and passed directly to execvp(). When running bison --html on a attacker-provided grammar, this behavior allows execution of an arbitrary program with the privileges of the Bison process. Maintainers of this project were notified about this vulnerability, and fixed the issue in commit 3169c1e7a2c6acc4c59dfcf8b089896d6881925b. However, they did not provide vulnerable version range. Version 3.8.2 was tested and confirmed as vulnerable, other versions were not tested but might also be vulnerable.	N/A	More Details
CVE-2026-69255	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, the CSVAgent in packages/components/nodes/agents/CSVAgent/CSVAgent.ts extracted attacker-controlled CSV data with file.split(',').pop() and interpolated it directly into executable Python as base64_string = "${base64String}" before calling Pyodide. The validatePythonCodeForDataFrame() denylist only checked later LLM-generated code and did not validate this initial code block. An authenticated attacker could inject a closing quote followed by Python code, use Pyodide's js bridge to load Node.js child_process, and execute arbitrary operating system commands as root in the Flowise container. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-69256	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, the CSVAgent node allowed users to provide Python code that is executed through pyodide; although a denylist blocked dangerous Python constructs, pandas.read_pickle() could deserialize a pickled payload and achieve code execution without matching the denied words. The affected file is flowise-components/nodes/agents/CSVAgent/CSVAgent.ts, where user-supplied customReadCSVFunc is evaluated as pd.${customReadCSVFunc}. An authenticated user who can create or modify a chatflow can add a CSV Agent, place a malicious read_pickle payload in the Additional Parameters, save the chatflow, and trigger /api/v1/prediction/<UUID> to execute commands. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-12927	CWE-787 Out-of-bounds write vulnerability exists that could cause loss of data or potentially risk arbitrary code execution when a malicious CGF file is imported to IGSS Definition.	N/A	More Details
CVE-2026-15929	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in LG Electronics SmartShare allows SQL Injection. This issue affects SmartShare: through 2.3.1712.1202, which is supported on Microsoft Windows 10 and earlier versions.	N/A	More Details

CVE-2026-14337	Pega Platform versions 23.1.0 through 25.1.3 are affected by an Stored Cross-site scripting (XSS) vulnerability in a user interface component. Requires a high privileged user with a developer role.	N/A	More Details
CVE-2026-7260	Circular symbolic links in phar archives could lead to unbounded recursion, exhausting the C stack and crashing the PHP process, in PHP versions from 8.2.* before 8.2.33, from 8.3.* before 8.3.33, from 8.4.* before 8.4.24, and from 8.5.* before 8.5.9.	N/A	More Details
CVE-2026-59952	Valibot helps validate data using a schema. Versions prior to 1.4.2 can throw a TypeError inside its flatten() helper when validation issues contain attacker-controlled object keys such as toString, valueOf, or hasOwnProperty. The issue is reachable through normal record() validation. record() intentionally filters __proto__, prototype, and constructor, but it still accepts other own keys that collide with inherited Object.prototype properties. If the record key schema or value schema rejects such an entry, Valibot creates an issue path containing that key. Passing the resulting issues to Valibot's documented flatten() helper causes flatErrors.nested[dotPath] to resolve to the inherited method instead of an own error array, and the helper calls .push(...) on that function. This is not a global prototype pollution issue. The impact is availability/error handling: applications that validate user-controlled objects with record() and flatten validation errors for API responses can crash the request path with a TypeError instead of returning structured validation errors. This issue has been fixed in version 1.4.2.	N/A	More Details
CVE-2026-0667	CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability that could cause arbitrary code execution, denial of service and loss of confidentiality & integrity when communicating over the Modbus TCP protocol.	N/A	More Details
CVE-2026-9177	A Server-Side Template Injection (SSTI) vulnerability was identified in the mail template functionality of the Axway SecureTransport product in version 5.5-20260326. This flaw allows an attacker with admin privileges to inject arbitrary Java code expressions, which are executed server-side when the template is rendered (i.e., during email sending). Successful exploitation of this flaw allows an attacker to execute arbitrary code on the server that results in full host compromise. This issue affects all Axway SecureTransport versions prior 5.5-20260528 update.	N/A	More Details
CVE-2026-63252	In Eclipse Milo versions 0.6.0 through 1.1.4, UASC server transport handlers fail to release retained partial message chunks when a channel disconnects, allowing a remote unauthenticated client to exhaust pooled direct memory by repeatedly sending incomplete chunks and disconnecting, potentially terminating the server.	N/A	More Details
CVE-2026-63248	In Eclipse Milo versions 0.6.0 through 1.1.4, OPC UA server diagnostics nodes do not enforce access authorization. An anonymous client can enable diagnostics over a None/None endpoint without a certificate; with a trusted client application certificate over SignAndEncrypt, it can read security diagnostics for other active sessions, exposing usernames, login history, authentication mechanisms, security modes and policies, and public client certificates.	N/A	More Details
CVE-2026-62927	In Eclipse Milo versions 1.0.0 through 1.1.4, the Call service dispatches the original mixed batch to address-space handlers after calculating authorization, allowing an anonymous or otherwise low-privileged client to execute a denied method by batching it with an allowed method.	N/A	More Details
CVE-2026-61387	In Eclipse Milo versions 1.0.0 through 1.1.4, monitored-item quota accounting is not exception-safe: if item creation fails with an unchecked error, the server-global reservation is not restored. Deeply nested PubSub ExtensionObjects in a `CreateMonitoredItems` event filter can trigger a `StackOverflowError` during decoding, allowing an unauthenticated remote client to exhaust a finite global monitored-item quota and prevent all clients from creating new monitored items until restart. Existing monitored items and other server functions remain unaffected.	N/A	More Details
CVE-2026-60007	In Eclipse Milo versions 0.6.0 through 1.1.4, username-token processing returns distinguishable errors for invalid RSA PKCS#1 v1.5 padding and other authentication failures, allowing an on-path attacker who captures a victim's `Basic128Rsa15`-encrypted username token to use repeated unauthenticated `ActivateSession` requests as a padding oracle, recover the victim's password, and authenticate with the recovered credentials.	N/A	More Details
CVE-2026-58080	In Eclipse Milo versions 1.0.0 through 1.1.4, `OpcUaServerConfig.copy()` fails to preserve a configured `RoleMapper`. On servers that rely on role permissions and construct the running configuration through `copy()`, sessions receive no role IDs and the default access controller skips role-permission checks, allowing an anonymous client where anonymous sessions are permitted to read role-permission metadata, invoke protected methods, or delete protected nodes.	N/A	More Details
	pdm is a Python package and dependency manager supporting the latest PEP standards. In		

CVE-2026-47763	versions prior to 2.27.0, pdm writes several project-local state or configuration files without symlink protection. If a malicious repository places those files as symlinks, local PDM operations can overwrite the symlink targets. This creates an arbitrary file clobber primitive relative to the privileges of the invoking user. Config.__init__() resolves the project-local pdm.toml path and _save_config() writes to the resolved target. If PROJECT_ROOT/pdm.toml is a symlink to another file, pdm config -l ... updates the target file instead of refusing the write. The same general problem exists for other project-local persistence paths that are written directly with no lstat / O_NOFOLLOW protection. For the pdm.toml PoC specifically, the target file must already contain parseable TOML. Otherwise the load step fails before the write path is reached. That parser constraint does not apply to the .pdm-python or .python-version sinks. This issue has been fixed in version 2.27.0.	N/A	More Details
CVE-2026-69264	Prior to 3.1.3, Flowise CSVAgent interpolates an attacker-controlled segment of the csvFile data URI directly into a Python source-code template that is then executed by Pyodide. Because Pyodide is loaded with the default js bridge to globalThis, which on Node.js exposes eval and dynamic import, the attacker can break out of the Python string literal, hand a JavaScript string to js.eval, dynamically import Node built-in modules such as fs and child_process, and execute arbitrary file I/O or OS commands as the Flowise process. The two validator paths around this code, validatePythonCodeForDataFrame and validateCustomReadCSVFunction, are never applied to the bootstrap template. A workspace user with chatflows:create or agentflows/chatflows update permission can plant a CSV Agent node with a crafted csvFile; once the chatflow is exposed via POST /api/v1/prediction/:id, any unauthenticated request triggers host remote code execution. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-70470	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, Flowise validatePythonCodeForDataFrame in packages/components/src/pythonCodeValidator.ts can be bypassed with Unicode homoglyph identifiers, allowing arbitrary Python execution inside Pyodide and full OS command execution on the Flowise host via Pyodide js module interop. The validator gates pyodide.runPythonAsync in packages/components/nodes/agents/CSVAgent/CSVAgent.ts and packages/components/nodes/agents/AirtableAgent/AirtableAgent.ts with an ASCII word-boundary blacklist. JavaScript regex word boundaries are ASCII-only, while Python 3 NFKC-normalizes identifiers at parse time, so homoglyph forms such as __clss__, __subclsses__, __bse__, and __biltins__ bypass the blacklist and are parsed as their ASCII equivalents. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-13229	Zammad 7.1.0 contains an authenticated improper authorization vulnerability in the ticket article attachment cloning endpoint.	N/A	More Details
CVE-2026-47764	pdm is a Python package and dependency manager supporting the latest PEP standards. Versions prior to 2.27.0 are vulnerable to path traversal through write_to_fs. InstallDestination.write_to_fs() in src/pdm/installers/installers.py overrides the base class to add symlink/hardlink support but replaces the safe _path_with_destdir() (which validates via Path.resolve() + is_relative_to()) with a bare os.path.join() that performs no path validation. A malicious wheel with traversal entries can write arbitrary files. This issue has been fixed in version 2.27.0.	N/A	More Details
CVE-2026-47781	PDM is a Python package and dependency manager. In versions up to and including 2.26.9, PDM automatically loads project-local plugins from a .pdm-plugins directory during initialization, allowing an attacker-controlled file in an untrusted repository checkout to execute arbitrary Python code before any command is parsed. This happens because load_plugins() runs during Core.init() and adds .pdm-plugins via site.addsitedir(), which processes .pth files and immediately executes any line beginning with import, so the code runs with the privileges of the user invoking pdm and even a benign command such as pdm --version triggers it (making the impact strongest in CI, automation, and privileged contexts). The issue is fixed in version 2.27.0.	N/A	More Details
CVE-2026-12895	SQL injection in Frappe's ERPNext, versions ERPNext 15.107.0 and Frappe 15.107.2. The application constructs SQL queries through direct string interpolation using `str.format()` without employing parameterized queries, allowing the name (docname) of a Supplier record containing SQL metacharacters to be interpreted as part of the query. Exploitation of this vulnerability could allow an authenticated user with low privileges to execute arbitrary SQL queries, bypass Frappe’s access restrictions (DocPerm), extract confidential information from the database—including fragments of the administrator’s password hash—and access other sensitive data, such as credentials, integration tokens, or financial information.	N/A	More Details
CVE-	CWE-522 Insufficiently Protected Credentials vulnerability exists that could cause authentication		

2026-14354	bypass and unauthorized credential modification, potentially leading to compromise of managed devices, when a local privileged attacker leverages weaknesses in the handling and protection of stored credentials within the application.	N/A	More Details
CVE-2026-18401	The non-blocking (asynchronous) JSON parser in jackson-core does not enforce the maxNumberLength constraint defined in StreamReadConstraints (default: 1000 characters). An attacker able to submit JSON to an application that uses the async parser API can supply a number token of arbitrary length, leading to excessive memory allocation and potential CPU exhaustion, resulting in a denial of service. The synchronous parser enforces this limit correctly, so the constraint is applied inconsistently depending on which parsing API the application uses. Root cause: the async parsing path in NonBlockingUtf8JsonParserBase and related classes never invokes the number length validation methods. Number parsing methods such as _finishNumberIntegralPart() accumulate digits into the TextBuffer without any length check, then call _valueComplete() to finalize the token. _valueComplete() does not call resetInt() or resetFloat(), which are the methods in ParserBase where validateIntegerLength() and validateFPLength() are performed. Because that validation step is skipped, maxNumberLength is never enforced on the async code path. Impact: an attacker sending a JSON document containing an arbitrarily long number to an application using the async parser (for example a Spring WebFlux or other reactive application) can cause unbounded allocation in the TextBuffer and an OutOfMemoryError. If the application subsequently calls getBigIntegerValue() or getDecimalValue(), the JVM may additionally be tied up in O(n^2) BigInteger parsing, causing CPU-based denial of service. No privileges or user interaction beyond the ability to submit data for parsing are required. This issue affects com.fasterxml.jackson.core:jackson-core from version 2.15.0 through 2.18.5 and from 2.19.0 through 2.21.0, and tools.jackson.core:jackson-core from 3.0.0 through 3.0.x. Versions prior to 2.15.0 are not affected, because StreamReadConstraints -- which defines the maxNumberLength setting -- was first introduced in jackson-core 2.15.0, so no such constraint exists to be bypassed in earlier releases. Note that GHSA-72hv-8253-57qq records the lower bound of the affected 2.x range as 2.0.0.	N/A	More Details
CVE-2026-65890	Joomla Extension - balbooa.com - Unauthenticated SQL injection in Gridbox < 2.20.2 - Multiple SQLi vectors allow unauthenticated actors to inject SQL in queries.	N/A	More Details
CVE-2026-17544	Attacker-provided inputs to bccomp() could lead to an out-of-bounds write with stack and heap corruption in PHP versions from 8.4.* before 8.4.24 and from 8.5.* before 8.5.9.	N/A	More Details
CVE-2026-55995	A Double Free vulnerability in open-iscsi allows an unauthenticated MITM attacker to cause DoS. This issue affects open-iscsi: from ? through 56718d4e9d1a4f51c30697b5c0534144bb41c9bb.	N/A	More Details
CVE-2026-56390	GNU Bison improperly handles grammar-defined output paths. Grammar directives such as %output and %header allow specifying file paths, which are accepted without restriction and override caller-supplied output options. When processing attacker-supplied grammar, this behavior allows directing generated files to arbitrary writable locations on the filesystem, potentially overwriting existing files accessible to the Bison process. Maintainers of this project were notified about this vulnerability, and fixed the issue in commit 8d101c19d4d9aaedf83a448c925513742d4efcf0. However, they did not provide vulnerable version range. Version 3.8.2 was tested and confirmed as vulnerable, other versions were not tested but might also be vulnerable.	N/A	More Details
CVE-2026-17543	Improper escaping of backslashes in attacker-provided parameters would allow for trivial SQL injection in PHP versions from 8.2.* before 8.2.33, from 8.3.* before 8.3.33, from 8.4.* before 8.4.24, and from 8.5.* before 8.5.9.	N/A	More Details
	The fix released in jackson-core 2.18.6 and 2.21.1 for CVE-2026-18401 (GHSA-72hv-8253-57qq, number length constraint bypass in the non-blocking parser) is incomplete. This record covers the remaining bypass. The earlier fix wired validateIntegerLength() into a new _setIntLength() helper and invoked it wherever the integer portion of a number is decided: a terminator byte arrives, a . or e/E is seen, or input ends inside a fully buffered value. It was not invoked on the attacker-relevant path where the parser runs out of input while still inside the MINOR_NUMBER_INTEGER_DIGITS minor state and returns NOT_AVAILABLE to the caller. As a result, an attacker who streams JSON to a non-blocking parser in many small chunks, without ever sending a terminator byte, keeps the parser inside MINOR_NUMBER_INTEGER_DIGITS indefinitely. _textBuffer.expandCurrentSegment() grows the accumulator on every chunk while validateIntegerLength() is never called. The accumulator is bounded only by maxStringLength (20		

CVE-2026-68494	MiB by default) rather than by maxNumberLength (1000 by default), an amplification of roughly 20,000x over the documented limit. Because Java char values occupy two bytes, a single connection can be driven to approximately 40 MiB of heap before the validator finally fires when the value completes. The equivalent fraction-path code is correct: _finishFloatFraction() calls _setFractLength() before its NOT_AVAILABLE return. The missing call affects the integer-digit paths in _startPositiveNumber(), _startNegativeNumber() and _finishNumberIntegralPart() in NonBlockingUtf8JsonParserBase. Impact: reactive frameworks such as Spring WebFlux/Reactor, Quarkus, Helidon and Vert.x feed inbound HTTP or gRPC bytes to the async parser as they arrive, which is precisely the chunked-feed shape required. Operators who set StreamReadConstraints.maxNumberLength expecting it to cap memory per number value do not get that guarantee; memory accumulates per concurrent connection and attacker-controlled concurrency can exhaust the JVM heap. The synchronous parsers (UTF8StreamJsonParser, ReaderBasedJsonParser) and the async parser operating on complete input are not affected. Exploitation requires only the ability to stream data to a parsing endpoint; no privileges or user interaction are needed. This issue affects com.fasterxml.jackson.core:jackson-core from version 2.15.0 through 2.18.7, from 2.19.0 through 2.21.3, and from 2.22.0 through 2.22.0, and tools.jackson.core:jackson-core from 3.0.0 through 3.1.3 and from 3.2.0 through 3.2.0. Versions prior to 2.15.0 are not affected, because StreamReadConstraints -- which defines the maxNumberLength setting -- was first introduced in jackson-core 2.15.0, so no such constraint exists to be bypassed in earlier releases. Note that GHSA-r7wm-3cxj-wff9 states the affected 2.x range without a lower bound.	N/A	More Details
CVE-2026-69250	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, the OAuth2 token refresh endpoint POST /api/v1/oauth2-credential/refresh/:credentialId is unauthenticated by design and performs a server-side HTTP request to the credential-controlled accessTokenUrl without SSRF protections. Runtime validation confirmed that the endpoint was reachable without authentication, triggered outbound POST requests to an attacker-controlled server, reflected the full remote response body to the caller through tokenInfo, and sent client_id, client_secret, grant_type=refresh_token, and refresh_token in the request body. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-69251	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, Flowise record manager and agent memory nodes allowed users to set arbitrary TypeORM DataSource options through the additionalConfig input in packages/components/nodes/recordmanager/MySQLRecordManager/MySQLrecordManager.ts, packages/components/nodes/recordmanager/PostgresRecordManager/PostgresRecordManager.ts, packages/components/nodes/recordmanager/SQLiteRecordManager/SQLiteRecordManager.ts, packages/components/nodes/memory/AgentMemory/MySQLAgentMemory/MySQLAgentMemory.ts, and packages/components/nodes/memory/AgentMemory/AgentMemory.ts. TypeORM DataSource options such as entities, subscribers, and migrations can load local JavaScript files, allowing an authenticated user to execute arbitrary code on the server by uploading a JavaScript payload and referencing it from additionalConfig.entities. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-65889	Joomla Extension - balbooa.com - Unauthenticated recursive directory deletion < 2.20.2 - The generateNewApp method allows actors to recursively delete directories.	N/A	More Details
CVE-2026-10032	The openUrl function in @a2ui/web_core passes an agent-controlled URL directly to window.open() without validating the URI scheme. A malicious agent can supply a javascript: URI as the url argument of a Button component's functionCall action. When the user clicks the rendered button, arbitrary JavaScript executes in the victim application's browser origin, constituting a stored/reflected XSS with Critical severity. No non-default configuration is required; the Basic Catalog is enabled by default.	N/A	More Details
CVE-2026-33385	A Blind SQL injection vulnerability has been identified in Quick.CMS. Improper neutralization of input provided by a high-privileged user into multiple fields in administration panel allows for Blind SQL Injection attacks. The vendor states that this administration panel already allows for significant modification capabilities. The SQL injection vulnerability primarily enables bypassing front-end validation controls and potential database destruction. Given the trust model in which this application is designed to be administered, remediation of this issue was not deemed necessary by the vendor. This vulnerability has been found in version 6.8, but other versions might also be vulnerable.	N/A	More Details
	A logic vulnerability in the password reset token validation routine implemented by osTicket in versions prior to v1.17.8 and v1.18.4. During the password reset process, the application retrieves		

CVE-2026-18363	the timestamp associated with the provided token and checks whether the configured validity period has expired. Consequently, the expiry check is only performed if the timestamp lookup fails, allowing tokens with an existing timestamp to bypass the intended expiry validation. Therefore, an attacker able to obtain a valid password reset token could reuse it to perform an unauthorised password reset and compromise the affected account.	N/A	More Details
CVE-2026-16727	Concurrent Execution using Shared Resource with Improper Synchronization (“Race Condition”) in ASUS Armoury Crate allows a local user to execute arbitrary code with elevated privileges via a crafted file replacement. Refer to the ' Security Update for ASUS Armoury Crate ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-18801	OpenMeter contains a stored, or second-order, SQL injection vulnerability in the handling of customer usage-attribution values. An attacker who can create or update a customer can store a malicious value in the usageAttribution.key or usageAttribution.subjectKeys fields. When that customer is subsequently used in a meter or event query, OpenMeter inserts the stored value into a ClickHouse WITH map(...) expression using string concatenation. OpenMeter versions from v1.0.0-beta.218 through v1.0.0-beta.231 are affected.	N/A	More Details
CVE-2026-65885	Joomla Extension - balbooa.com - Authenticated arbitrary file upload in Gridbox < 2.20.2 - File upload methods allows authenticated attackers to upload arbitrary files. Turns into an authenticated RCE if combined with CVE-2026-65884 as the required account can be created by the attacker.	N/A	More Details
CVE-2026-65884	Joomla Extension - balbooa.com - Privilege Escalation in Gridbox < 2.20.2 - The registration method allows users provided usergroup IDs, allowing unauthenticated actors to register new accounts with administrative permissions.	N/A	More Details
CVE-2026-50641	Streamsoft Business Intelligence (BI) stores users' passwords in plaintext form in the database This issue was fixed in version 6.8.0.0, users were also requested to change their password on the first login.	N/A	More Details
CVE-2026-44944	An Incorrect Authorization vulnerability in open-iscsi allows unprivilidged local users to use the isscsiuio control socket. This issue affects open-iscsi: from ? through 668ca1df9c9a1e9bdd5c999ae1d67c9c8909237e.	N/A	More Details
CVE-2026-44943	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in open-iscsi allows remote MITM attackers to create root-owned files outside the database and inject lines into the record. This issue affects open-iscsi: from through 668ca1df9c9a1e9bdd5c999ae1d67c9c8909237e.	N/A	More Details
CVE-2026-58075	A vulnerability allowing an unauthenticated attacker to read arbitrary files from the host, which can be further leveraged toescalate privileges locally.	N/A	More Details
CVE-2026-69252	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, the /api/v1/files route was protected only by the feat:files feature gate and did not enforce checkPermission on GET or DELETE. A low-privileged authenticated API key with unrelated permissions could call GET /api/v1/files to list files under the organization storage root and DELETE /api/v1/files?path=... to delete files belonging to other workspaces in the same organization because getAllFiles and deleteFile used activeOrganizationId and a user-controlled path without restricting access by permissions or activeWorkspaceId. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-59247	Insufficient Verification of Data Authenticity vulnerability in Gleam allows an adversary in the middle to substitute forged Hex package contents during dependency resolution. During dependency resolution Gleam fetches package metadata from the signature-verified Hex repository, which covers each release's dependency requirements and SHA-256 outer_checksum. After resolving versions, gleam_cli::dependencies::lookup_package makes a second request to the unsigned Hex API through gleam_core::hex::get_package_release and records the outer_checksum and dependency names from that JSON response into manifest.toml, instead of the values from the verified repository metadata. The Hex repository signature does not cover the API response. An adversary in the middle who can intercept TLS with a certificate trusted by the Gleam process (for example a TLS-inspecting proxy using a CA in the operating system trust store or added through GLEAM_CACERTS_PATH), and who can modify both the API release response and the corresponding repository tarball, can supply a package archive with a matching forged checksum without the Hex repository signing key. Gleam verifies the forged tarball against the forged checksum, accepts it, and extracts it as a dependency source, resulting in loss of integrity of the downloaded package contents. Only projects that resolve or update Hex dependencies are	N/A	More Details

	affected, which happens when the manifest is missing, a dependency is added or updated, or dependency requirements change. Builds that reuse an unchanged, known-good manifest.toml continue to verify tarballs against its pinned checksum. This issue affects gleam: from 0.18.0 before 1.18.0.		
CVE-2026-70475	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, the PUT /api/v1/executions/:id endpoint in packages/server/src/routes/executions/index.ts lacks the checkAnyPermission() middleware that protects other execution endpoints. Any authenticated user, regardless of assigned permissions, can modify execution state, data, and metadata of any execution in their workspace, enabling privilege escalation and manipulation of workflow execution results. This issue is fixed in 3.1.3.	N/A	More Details
CVE-2026-64564	In the Linux kernel, the following vulnerability has been resolved: sctp: don't free the ASCONF's own transport in DEL-IP processing sctp_process_asconf() caches the transport the ASCONF chunk is processed against in asconf->transport (== chunk->transport, set once in sctp_rcv()). For an ASCONF located through its Address Parameter by __sctp_rcv_asconf_lookup(), that cached transport corresponds to the Address Parameter, which need not be the packet's source address. sctp_process_asconf_param() rejects a DEL-IP for the packet source address (ADDIP D8, SCTP_ERROR_DEL_SRC_IP), but nothing protects asconf->transport. A single ASCONF can therefore carry, in order: [Address Parameter L] [DEL-IP L] [DEL-IP 0.0.0.0] where L differs from the source. The DEL-IP for L passes the D8 check and calls sctp_assoc_rm_peer() on the transport that asconf->transport still points at, freeing it (RCU-deferred). The following wildcard DEL-IP then reuses the now-dangling asconf->transport in sctp_assoc_set_primary() and sctp_assoc_del_nonprimary_peers(): set_primary() dereferences the freed transport (->ipaddr, ->state) and plants the dangling pointer into asoc->peer.primary_path / active_path, and del_nonprimary_peers(), keeping only the pointer that is no longer on the list, removes every real transport, leaving the association with a transport_count of 0 and primary_path/active_path pointing at freed memory. Reject a DEL-IP that targets the transport the ASCONF is being processed against, mirroring the existing source-address guard, so the wildcard branch can never reuse a freed transport.	N/A	More Details
CVE-2026-64563	In the Linux kernel, the following vulnerability has been resolved: rhashtable: clear stale iter->p on table restart rhashtable_walk_start_check() has two restart paths when resuming a walk. When iter->walker.tbl is valid, it re-validates iter->p against the table and sets iter->p = NULL if the object is gone. When iter->walker.tbl is NULL (table was freed during resize), it resets slot and skip but forgets to clear iter->p. rhashtable_walk_next() then dereferences the stale iter->p, reading freed memory. This is a use-after-free. Any caller that does multi-fragment rhashtable walks across walk_stop/walk_start boundaries is affected. Concrete cases include netlink_diag (__netlink_diag_dump in net/netlink/diag.c) and TIPC (tipc_nl_sk_walk in net/tipc/socket.c). Crash stack (netlink_diag): BUG: KASAN: slab-use-after-free in rhashtable_walk_next+0x365/0x3c0 Read of size 8 at addr ffff88801a9d2438 (freed kmalloc-2k, offset 1080) Call Trace: rhashtable_walk_next+0x365/0x3c0 (lib/rhashtable.c:1016) __netlink_diag_dump+0x160/0x760 (net/netlink/diag.c:122) netlink_diag_dump+0xc2/0x240 netlink_dump+0x5bc/0x1270 netlink_recvmsg+0x7a3/0x980 sock_recvmsg+0x1bc/0x200 __sys_recvfrom+0x1d4/0x2c0	N/A	More Details
CVE-2026-64562	In the Linux kernel, the following vulnerability has been resolved: KVM: nVMX: Hide shadow VMCS right after VMCLEAR free_nested() frees the shadow VMCS while vmcs01 still points to it. But because it is asynchronous with respect to loaded_vmcs_clear(), the vCPU might migrate before the pointer is cleared and __loaded_vmcs_clear() may then execute VMCLEAR. The VMCS needs to stay attached until its explicit VMCLEAR completes, but then it can be hidden and the page safely freed.	N/A	More Details
CVE-2026-64561	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: Check for invalid/obsolete root *after* making MMU pages available Check for a "stale" page fault, i.e. for an invalid and/or obsolete root, after making MMU pages available for the shadow MMU. If reclaiming shadow pages zaps an in-use root, i.e. marks it invalid, then KVM will attempt to map memory into an invalid root. On its own, populating an invalid root is "fine", but because child shadow pages inherit their parent's role, any children created during the map/fetch will be created as invalid pages, thus violating KVM's invariant that invalid pages are never on the list of active MMU pages. Note, the underlying flaw has existed since KVM first started tracking invalid roots in 2008 (commit 2e53d63acba7, "KVM: MMU: ignore zapped root pagetables"), but the true badness only came along in 2020 (Linux 5.9) with the invariant that invalid shadow pages can't be on the list of active pages. Note #2, inheriting role.invalid when creating child shadow pages is also far from ideal; that flaw will be addressed separately.	N/A	More Details

CVE-2026-50642	diff-so-fancy does not properly sanitize non-SGR terminal control sequences before outputting diff data. The application only strips ANSI SGR sequences while allowing other control characters, including carriage return (\r) and escape sequences (e.g., OSC, CSI), to pass through unsanitized. An attacker can embed malicious control sequences in filenames, diff metadata, or file content that are rendered directly in the terminal during diff viewing. This can lead to output manipulation, including filename spoofing, terminal screen clearing, and clipboard injection via supported escape sequences. Successful exploitation may mislead users during code review, alter terminal state, or result in unintended command execution through clipboard hijacking. This issue has been fixed in the commit 9c81294	N/A	More Details
CVE-2026-69259	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, the SQLite Record Manager node in packages/components/nodes/recordmanager/SQLiteRecordManager/SQLiteRecordManager.ts accepted user-controlled additionalConfig and spread it after the intended database setting, allowing additionalConfig.database to overwrite the SQLite database path. An authenticated attacker using the published Docker image, which ran as root, could write a SQLite database to paths such as /etc/chromium/exploit.conf; by controlling the table name and namespace value, the attacker could place shell syntax into the database file and trigger execution when Puppeteer launched Chromium and sourced /etc/chromium/*.conf. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-69258	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, the unauthenticated POST /api/v1/prediction/:id endpoint accepted an overrideConfig object and unconditionally spread it into internal flowConfig and flowData objects in packages/server/src/utils/buildChatflow.ts and packages/server/src/utils/index.ts without checking apiOverrideStatus. This allowed unauthenticated attackers to inject arbitrary properties into the flow execution context of any public chatflow, overwrite values such as chatId, sessionId, and chatHistory, and control values resolved through $flow.* template variables consumed by flow nodes. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-47682	CVAT is an open source interactive video and image annotation tool for computer vision. In versions 1.6.0 through 2.64.0, an attacker with write access to a cloud storage that's been added to a CVAT instance, or ability to add new cloud storages, is able to overwrite arbitrary files on the server's filesystem. This issue has been fixed in version 2.65.0.	N/A	More Details
CVE-2026-18353	PIA's `POST /v1/upload/sbom` endpoint accepts a Bearer JWT and checks its **unverified** `iss` claim against an issuer allowlist using Python's `urlparse` before performing OIDC discovery with `requests`. Because `urlparse` and `requests`/`urllib3` parse an authority string containing a backslash (e.g. `https://attacker-host\@ci.eclipse.org/`) into *different* hostnames, an attacker can craft an issuer that passes the allowlist check yet drives `requests` — and subsequently `urllib.request.urlopen` for JWKS retrieval — to connect to an arbitrary attacker-chosen host, port, and scheme.	N/A	More Details
CVE-2026-15228	Kong Kubernetes Ingress Controller (KIC) allows a user with namespace-scoped Secret creation privileges to cause a cluster-wide ingress configuration denial of service. KIC collects CA-certificate Secrets across all watched namespaces using a label selector alone, without ingress-class or namespace restrictions. The CA-certificate primary key is derived from a user-supplied field in the Secret. Duplicate CA-certificate IDs cause Kong Gateway to reject the entire configuration document and halting all ingress changes cluster-wide.	N/A	More Details
CVE-2026-16543	Kong Operator's embedded Kong Kubernetes Ingress Controller (KIC) allows a user with namespace-scoped Secret creation privileges to cause a cluster-wide ingress configuration denial of service. The embedded KIC collects CA-certificate Secrets across all watched namespaces using a label selector alone, without ingress-class or namespace restrictions. The CA-certificate primary key is derived from a user-supplied field in the Secret. Duplicate CA-certificate IDs cause Kong Gateway to reject the entire configuration document and halting all ingress changes cluster-wide.	N/A	More Details
CVE-2026-70476	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, several organization billing endpoints in packages/server/src/enterprise/routes/organization.route.ts and packages/server/src/enterprise/controllers/organization.controller.ts accept attacker-controlled Stripe subscriptionId values without verifying that the identifier belongs to the authenticated user's organization. An authenticated attacker can perform unauthorized Stripe subscription operations on other tenants, including changing subscription plans or modifying seat quantities, resulting in financial impact and service disruption. This issue is fixed in 3.1.3.	N/A	More Details
	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to		

CVE-2026-70477	3.1.3, a prompt injection sent to a chatflow using a CSV Agent node can cause the LLM to respond with a malicious Python script that bypasses the blocklist validator and executes in an unsandboxed Pyodide environment. The specific flaw exists within the run method of the CSV_Agents class, where untrusted data is used to construct an LLM prompt and the resulting pythonCode is validated by validatePythonCodeForDataFrame before execution. An attacker can leverage this to execute arbitrary code in the context of the service account. This issue is fixed in 3.1.3.	N/A	More Details
CVE-2026-70478	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, the POST /api/v1/oauth2-credential/refresh/:credentialId endpoint is included in WHITELIST_URLS and requires no authentication. The endpoint decrypts the stored credential, sends a refresh request to the configured OAuth provider with the client secret and refresh token, and returns the refreshed access_token in the response body. An attacker with a credential ID can use the token to access the victim's connected service and can also exhaust refresh-token quota. This issue is fixed in 3.1.3.	N/A	More Details
CVE-2026-18197	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Link Library allows Cross-Site Scripting (XSS). This issue affects Link Library: before 7.9.4.	N/A	More Details
CVE-2026-69257	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, Flowise's HTTP security module httpSecurity.ts did not normalize IPv4-mapped IPv6 addresses such as ::ffff:127.0.0.1 and ::ffff:169.254.169.254 before checking them against the deny list. Because ipaddr.js reports these addresses as ipv6 while IPv4 CIDR deny-list entries are ipv4, isDeniedIP() skipped the IPv4 CIDR checks. An attacker who controls DNS resolution for a hostname used by the HTTP Node, API Chain, Document Loader, MCP tool, or other paths using secureAxiosRequest(), secureFetch(), or checkDenyList() could return a AAAA record for an IPv4-mapped target and cause requests to reach localhost, internal services, or cloud metadata endpoints. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-58066	Rocket.Chat's SAML SSO before versions 8.7.0, 8.6.1, 8.5.2, 8.4.5, 8.3.7, 8.2.7, 8.1.7, 8.0.8, and 7.10.14 verified XML signatures but did not bind the validated signature to samlp:Response / saml:Assertion. An attacker could submit a wrapped document carrying forged identity attributes alongside any valid signature made by the trusted IdP certificate, and log in as an arbitrary user.	N/A	More Details
CVE-2026-58043	A flaw in Node.js Permission Model enforcement can over-grant filesystem access across radix-tree prefix boundaries. Under `--permission`, an attacker who is granted access to one path can abuse boundary handling to read from or write to paths outside the intended filesystem allowlist. This vulnerability affects Node.js **main**, **22.x**, **24.x**, and **26.x**.	N/A	More Details
CVE-2026-64565	In the Linux kernel, the following vulnerability has been resolved: Input: ims-pcu - fix heap-buffer-overflow in ims_pcu_process_data() The `ims_pcu_process_data()` processes incoming URB data byte by byte. However, it fails to check if the `read_pos` index exceeds IMS_PCU_BUF_SIZE. If a malicious USB device sends a packet larger than IMS_PCU_BUF_SIZE, `read_pos` will increment indefinitely. Moreover, since `read_pos` is located immediately after `read_buf`, the attacker can overwrite `read_pos` itself to arbitrarily control the index. This manipulated `read_pos` is subsequently used in `ims_pcu_handle_response()` to copy data into `cmd_buf`, leading to a heap buffer overflow. Specifically, an attacker can overwrite the `cmd_done.wait.head` located at offset 136 relative to `cmd_buf` in the `ims_pcu_handle_response()`. Consequently, when the driver calls `complete(&pcu->cmd_done)`, it triggers a control flow hijack by using the manipulated pointer. Fix this by adding a bounds check for `read_pos` before writing to `read_buf`. If the packet is too long, discard it, log a warning, and reset the parser state. [dtor: factor out resetting packet state, reset checksum as well]	N/A	More Details
CVE-2026-18759	The background service of ABP or AES runs as NT AUTHORITY\SYSTEM and implements a file-based inter-process communication (IPC) mechanism protected by AES encryption. Because the encryption key file is readable by standard users and protected using DPAPI. Any authenticated local user can recover the key and forge valid IPC requests. Furthermore, the service does not check the identity of the requesting process and validates destination paths using an insufficient substring check. A local attacker can submit crafted encrypted requests containing directory traversal sequences to perform arbitrary file reads and arbitrary file writes as NT AUTHORITY\SYSTEM, leading to full local privilege escalation. Affected products and versions include: ABP (ASUSTOR Backup Plan) 2.0.7.10171 and earlier as well as AES (ASUSTOR EZSync) 1.1.1.3113 and earlier.	N/A	More Details
CVE-			

2026-65886	Joomla Extension - balbooa.com - Unauthenticated arbitrary file read in Gridbox < 2.20.2 - The photo viewer allows unauthenticated attackers to view arbitrary files.	N/A	More Details
CVE-2026-15314	Tapo P110 v1 smart Wi-Fi Plug contains an improper boundary validation vulnerability in the handling of authenticated HTTP request bodies due to insufficient input validation before memory copy operations. This may lead to buffer overflow condition, causing the web service process to crash. Successful exploitation may cause the web service process to stop responding or restart, resulting in a denial-of-service condition.	N/A	More Details
CVE-2026-65887	Joomla Extension - balbooa.com - Unauthenticated arbitrary password reset in Gridbox < 2.20.2 - The resetPassword method allows actors to reset any user password, allowing to login and act as these users - excluding super admins.	N/A	More Details
CVE-2026-66884	Cross-Site Request Forgery vulnerability in Erlang Ecosystem Foundation oidcc_plug (Oidcc.Plug.AuthorizationCallback module) allows an attacker to make a victim's browser complete an authorization flow the victim never initiated. This vulnerability is associated with program file lib/oidcc/plug/authorization_callback.ex and program routine Oidcc.Plug.AuthorizationCallback.call/2. A callback request that carries no Oidcc.Plug.Authorize session is processed with every security check disabled rather than being rejected. call/2 substitutes permissive defaults for the absent session, and each downstream check treats its value as nothing to compare and returns :ok, so the nonce, state, PKCE, peer IP and user agent checks are all skipped. A separate clause of check_state/2 also accepts a state-less request when a verifier is present. An attacker obtains an authorization code for their own provider account, then induces the victim to visit the callback endpoint with that code and no state parameter. The application signs the victim in as the attacker, so the victim's subsequent actions occur in the attacker's account where the attacker can read them. Applications reusing one callback for both signing in and linking a provider account are further exposed to account takeover, the attacker's account becoming linked to the victim's. The permissive fallback serves no conforming flow. Third-party-initiated login reaches a relying party at a separate login initiation endpoint and causes it to send a fresh authentication request, and this library implements no such endpoint. Oidcc.Plug.Authorize always sends a state parameter, which an authorization server must echo, so no legitimate callback lacks one. This issue affects oidcc_plug: from 0.2.0-beta.1 before 0.5.0.	N/A	More Details
CVE-2026-66883	Improper Handling of Case Sensitivity vulnerability in Erlang Ecosystem Foundation oidcc_plug (Oidcc.Plug.Authorize module) renders the user agent session binding inert, removing a defense in depth control against replay of a stolen session. This vulnerability is associated with program files lib/oidcc/plug/authorize.ex and lib/oidcc/plug/authorization_callback.ex, and program routines Oidcc.Plug.Authorize.call/2 and Oidcc.Plug.AuthorizationCallback.call/2. Oidcc.Plug.Authorize.call/2 reads the initiating client's user agent with get_req_header(conn, "User-Agent"). Plug lowercases incoming header names, but get_req_header/2 matches the supplied key exactly and performs no normalization of its own, so the mixed-case lookup always returns an empty list and nil is written into the session. On the callback side, Oidcc.Plug.AuthorizationCallback treats a stored nil user agent as nothing to compare and returns :ok without inspecting the request. The two behaviours combine so that the check passes unconditionally on every request, including for deployments that explicitly opted in with check_useragent: true, and an authorization callback can be completed from a different user agent than the one that initiated the flow without detection. The check fails open silently, with no error and no log entry, so a deployment cannot tell the binding is absent. The impact is limited to defense in depth. The inert check does not by itself allow an attacker to complete an authorization flow; it removes one layer that would otherwise hinder use of a stolen or leaked session, such as an exfiltrated session cookie replayed from a different client. The CSRF/state, nonce, and PKCE checks are unaffected and continue to function. Deployments that never enabled check_useragent are not affected in practice, since they never expected the binding. The corresponding lookup in Oidcc.Plug.AuthorizationCallback correctly uses the lowercase key and is not affected. This issue affects oidcc_plug: from 0.1.0-alpha.3 before 0.5.0.	N/A	More Details
CVE-2026-48115	Misskey is an open source, federated social media platform. All Misskey servers running versions 2024.5.0 and later, but prior to 2026.5.4, contain a vulnerability in the Server Announcements API where insufficient permission checks allow attackers to access limited portions of data that they normally couldn't view. This vulnerability occurs whether or not federation is enabled. This issue has been fixed in version 2026.5.4.	N/A	More Details
CVE-	In Eclipse Jetty, the Digest authentication server-side component uses ISO-8859-1 to encode the password as bytes. This was done because the initial specification for HTTP did not specify explicitly a charset, and it was assumed to be ISO-8859-1 for historical reasons. If the password contains characters that cannot be represented in ISO-8859-1, they are silently replaced by `?`.		

2026-10050	This happens with passwords that contain Chinese, Cyrillic or Greek characters, for example: `αβ123` converts to `??123`. An attacker can send a request with a digest `Authorization` header crafted with a password made of only `?` characters; the server would match any password of the same length that contains non-ISO-8859-1 characters. Recent HTTP Digest [RFC-7616] (https://datatracker.ietf.org/doc/html/rfc7616) supports a `charset` parameters that defaults to UTF-8 that allows for correct encoding/decoding of passwords.	N/A	More Details
CVE-2026-69263	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, the mitigation for CVE-2025-8943 blocked -y and --yes flags on npx, but packages/components/nodes/tools/MCP/core.ts denied only PATH, LD_LIBRARY_PATH, DYLD_LIBRARY_PATH, and NODE_OPTIONS by exact environment-variable name. Because npm reads configuration from npm_config_* variables, setting npm_config_yes=true reproduced --yes behavior without using a blocked flag, causing npx to auto-install and execute the named package when a Custom MCP server launched. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-69254	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, executeJavaScriptCode() accepted caller-provided nodeVMOptions and merged them over the default NodeVM security settings in packages/components/src/utils.ts. An authenticated attacker reaching packages/server/src/routes/node-custom-functions/index.ts could run a custom function that imported flowise-components/dist/src/utils.js, called executeJavaScriptCode() again with nodeVMOptions.require.builtin set to allow all built-in modules, and then required child_process to execute arbitrary system commands as root on the Flowise server. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2022-4994	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: wean fast IN from emulator_pio_in Use __emulator_pio_in() directly for fast PIO instead of bouncing through emulator_pio_in() now that __emulator_pio_in() fills "val" when handling in-kernel PIO. vcpu->arch.pio.count is guaranteed to be '0', so this a pure nop. emulator_pio_in_emulated is now the last caller of emulator_pio_in. No functional change intended.	N/A	More Details
CVE-2026-70471	Flowise is a drag-and-drop user interface for building customized large language model (LLM) flows. Prior to 3.1.3, Flowise injects $vars into the code execution sandbox without requiring variables:view, bypassing the permission-protected Variables API. Variables for the active workspace are fetched at packages/components/src/utils.ts and runtime variables are resolved from server environment variables, while the official variables route enforces variables:view. A user or API key that is denied variables:view can call /api/v1/node-custom-function and receive $vars pre-populated with all variables for the workspace, including Variable.name to Variable.value static variables and Variable.name to process.env[Variable.name] runtime variables. This can expose secrets such as database passwords, JWT secrets, SMTP passwords, and cloud keys, depending on the workspace Variables configuration. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-67243	freo2 provided by refirio contains an unrestricted upload of file with dangerous type vulnerability. A user with the highest-level administrative privileges for the product may upload an executable file and execute arbitrary OS commands.	N/A	More Details
CVE-2026-70472	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, Flowise openai-assistants-vector-store endpoints accept a client-controlled credential parameter and load credentials by id without checking whether that credential belongs to the caller workspace. Route permissions assistants:* only check feature access. The controller passes req.query.credential straight to the service, and the service uses findOneBy({ id: credentialId }), decrypts the credential, and calls OpenAI APIs without a workspaceId check. If an attacker knows another workspace credentialId, the attacker can use that workspace OpenAI key, read, modify, or delete victim vector stores and files, cause billing impact on the victim OpenAI account, and violate multi-tenant boundaries. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-70473	Flowise is a drag-and-drop user interface for building customized large language model (LLM) flows. Prior to 3.1.3, Flowise GET /api/v1/upsert-history returns the entire server-wide upsert history instead of being scoped to the requesting user, tenant, or workspace. The response can exceed 100MB and includes sensitive configuration data, including Vector Store settings such as Qdrant Server URL and collection name. The observed behavior indicates missing or insufficient authorization checks, workspace/project/tenant isolation, and pagination or limits, exposing integration parameters and infrastructure details that may enable further targeted attacks. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-			

2026-65888	Joomla Extension - balbooa.com - Account takeover vulnerability in Gridbox < 2.20.2 - The socialLogin method allows actors to login as any given user on the target site.	N/A	More Details
CVE-2026-66723	MWDB Core versions >=2.2.0 and <2.19.0 contain a missing authorization vulnerability in the Remote Instances proxy API. The proxy API does not verify authentication for incoming requests, allowing an unauthenticated remote attacker to send arbitrary requests to a remote MWDB instance using the identity and permissions associated with the configured API key. This can result in unauthorized actions being performed on the remote instance as if executed by the user whose API key was used to set up the remote instance. The vulnerability is limited to deployments where Remote Instances have been configured.This issue has been fixed in version 2.19.0	N/A	More Details
CVE-2026-70474	Flowise is a drag-and-drop user interface for building customized large language model (LLM) flows. Prior to 3.1.3, Flowise has three OAuth2 credential endpoints that look up credentials by id alone with no workspaceId filter. The authorize, callback, and refresh handlers query the Credential table by id only; callback and refresh are whitelisted from authentication. This allows any authenticated user to initiate OAuth2 flows against credentials belonging to other workspaces, allows an unauthenticated attacker to forge OAuth2 callbacks to overwrite tokens in any credential, and allows an unauthenticated attacker to refresh tokens for any credential. The affected routes include /api/v1/oauth2-credential/authorize/<VICTIM_CREDENTIAL_UUID>, /api/v1/oauth2-credential/callback?code=ATTACKER_AUTH_CODE&state=<VICTIM_CREDENTIAL_UUID>, and /api/v1/oauth2-credential/refresh/<VICTIM_CREDENTIAL_UUID>. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-13584	Improper Enforcement of Message Integrity During Transmission in a Communication Channel vulnerability in Mitsubishi Electric MELSEC MX Controller MX-R model, MELSEC MX Controller MX-F model, Master/local module, CC-Link IE TSN interface board, Motion module, Motion Control Board, Block-type remote module, Block-type remote module with safety functions, Analog-Digital converter module, Digital-Analog converter module, CC-Link IE TSN compatible coupler, FPGA module, Tension meter, AC Servo MELSERVO-J5, AC Servo MELSERVO-JET, Liner Track System MTR-S series Linear track control module, Inverter FR-A800/F800/E800 Series, Industrial Robot CR800-D series controller Network Base Card, CC-Link IE TSN expansion unit, CC-Link IE TSN-CC-Link IE Field Network bridge module, CC-Link IE TSN-AnyWireASLINK bridge module, Energy Measuring Unit CC-Link IE TSN Communication Unit, Industrial Computer MELIPC series, GOT3000 Series, CC-Link IE TSN Communication Unit, Motion Control Software, CC-Link IE TSN Communication Software for Windows, Analysis Support Software MELSOFT VIMA, Master/Local module Designated communication LSI DeviceKit, Master/Local module Designated communication LSI, Remote Station Communication LSI with GbE-PHY, CC-Link IE TSN Master/Local module Designated communication LSI SDK, and Remote station software development kit allows an attacker with access to a CC-Link IE TSN network to tamper with communication data (control input/output values) by sending specially crafted packets under specific timing conditions. This could allow the attacker to cause a denial-of-service (DoS) condition in the affected product by interfering with its control function or causing it to operate incorrectly.	N/A	More Details
CVE-2026-69262	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, `DELETE /api/v1/chatflows/:id` authorized requests with checkAnyPermission('chatflows:delete,agentflows:delete'), so possession of either permission was sufficient to reach the delete path. The delete logic then resolved the target record only by id and workspaceId and did not validate the target resource type, allowing a caller with only agentflows:delete to delete a CHATFLOW and a caller with only chatflows:delete to delete an AGENTFLOW in the same workspace. This issue is fixed in version 3.1.3.	N/A	More Details
CVE-2026-66724	MWDB Core versions >=2.0.0 and <2.19.0 contain a missing authorization vulnerability in the deprecated config and blob upload endpoints. These endpoints accept the undocumented POST method, which bypasses the capability checks applied to the documented PUT method. This allows any authenticated user without the adding_configs or adding_blobs capabilities to upload config and text blob objects to the system. The impact is limited to adding new config and blob objects. This issue has been fixed in version 2.19.0	N/A	More Details
CVE-	Flowise is a drag-and-drop user interface for building customized large language model (LLM) flows. Prior to version 3.1.3, several custom-tool components — AgentAsTool, ChatflowTool, and ExecuteFlow — ran code in the in-process vm2 sandbox. To build that code, they inserted a user-controlled baseURL value straight into the JavaScript source, for example const url = "${baseURL}/..."; . The only check on baseURL was isValidURL , but a valid-looking URL can still contain characters that break out of a code string. An authenticated user could craft a baseURL		More

2026-69253	that passed this check, closed the surrounding string, and injected their own JavaScript into the sandboxed script (code injection, CWE-94). The `vm2` sandbox runs in the same Node.js process as Flowise and exposes risky dependencies. As a result, the injected code could escape the sandbox and run arbitrary code on the Flowise server as the Flowise process user. Exploitation only requires an authenticated session. The issue is fixed in version 3.1.3, which passes the URL to the sandbox as data instead of inserting it into code and adds stricter URL validation.	N/A	Details
CVE-2026-51233	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-47746	Misskey is an open source, federated social media platform. Versions 12.37.0 and later, but prior to 2026.5.4, are vulnerable to timing attacks during JSON-LD signature validation and the compaction process. Because the JSON-LD parsing context is not shared between signature verification and subsequent processing, the application may trust information that should not be trusted, resulting in a time-of-check to time-of-use (TOCTOU) flaw. This allows an attacker to have fraudulent activities accepted as valid, leading to a loss of integrity. This issue has been fixed in version 2026.5.4.	N/A	More Details
CVE-2026-14309	The Chat On Desk Order Notifications WordPress plugin before 1.0.9 does not verify that the one-time password has been validated before processing a password-reset request, allowing unauthenticated attackers to reset the password of arbitrary users, including administrators, and take over their accounts when SMS one-time-password password reset is enabled.	N/A	More Details
CVE-2026-67309	Traefik versions >= v3.7.0 and <= v3.7.7 contain a path traversal vulnerability in the Kubernetes Ingress NGINX provider's RewriteTarget middleware (generated from the nginx.ingress.kubernetes.io/rewrite-target annotation). When an Ingress path uses a regex that captures attacker-controlled text without requiring a path separator (e.g., path /api(.*) with rewrite target /$1), a crafted request such as /api../admin matches the public router, is rewritten to a dot-segment traversal path (/../admin), and is forwarded without post-replacement normalization validation. A backend that normalizes dot segments resolves the path to a protected endpoint (e.g., /admin) reachable only through a separate router secured with BasicAuth, DigestAuth, or ForwardAuth, resulting in route-level authentication bypass. The issue is fixed in v3.7.8.	N/A	More Details
CVE-2026-67308	Wazuh workflows before 44bf114 contain a shell injection vulnerability in GitHub Actions that allows attackers to execute arbitrary commands by submitting pull requests with crafted VERSION.json files. Attackers can inject shell metacharacters into environment variables that are directly interpolated into run steps, enabling command execution and exfiltration of secrets including GITHUB_TOKEN and AWS credentials on self-hosted runners.	N/A	More Details
CVE-2026-67305	FreeRDP Windows client before 3.29.0 contains a heap buffer overflow vulnerability in the clipboard virtual channel when processing CLIPRDR_FILE_CONTENTS_RESPONSE PDUs without validating the server-provided size against the destination buffer. A malicious RDP server can send a response with a data payload significantly larger than requested, causing arbitrary heap memory corruption that may enable remote code execution when a user performs a paste operation.	N/A	More Details
CVE-2026-10772	Rejected reason: ** DUPLICATE ** This CVE Record has been rejected by the Zephyr Project CNA. CVE-2026-10772 was assigned to a vulnerability already covered by CVE-2026-2411, which was assigned earlier for the same defect: the Bluetooth GATT notify/indicate paths check the permissions of the Characteristic Declaration attribute rather than the Characteristic Value attribute, so the encryption/authentication requirements configured on the value are not enforced. Both identifiers describe the same root cause in subsys/bluetooth/host/gatt.c, fixed by the same commit (c3386f92fe81bd10dc23e6a115e6a80a7d863546). Use CVE-2026-2411 instead.	N/A	More Details
CVE-2025-71404	better-auth versions after v0.0.2 and before 1.1.16 contain a reflected cross-site scripting (XSS) vulnerability on the /api/auth/error page, where the value of the 'error' URL parameter is reflected as HTML without proper neutralization. An attacker who coerces a user into visiting a specially-crafted URL can execute arbitrary JavaScript in the context of the user's browser. The issue is fixed in version 1.1.16.	N/A	More Details
CVE-2025-	better-auth versions greater than 1.3.34 and before 1.4.0 contain a vulnerability in the multi-session plugin's /sign-out after-hook, which trusts raw multi-session cookies and forwards extracted values to internalAdapter.deleteSessions without verifying the cookie signature (e.g.,	N/A	More Details

71402	via getSignedCookie). An attacker can supply a forged _multi-* cookie to trigger deletion of arbitrary session tokens.		
CVE-2026-15932	The Support Genix WordPress plugin before 1.4.48 does not prevent directory traversal in its ticket-attachment download route, allowing unauthenticated attackers to read arbitrary files with an allowlisted extension — including other users' private ticket attachments — from the server.	N/A	More Details
CVE-2026-15368	The User Profile Builder WordPress plugin before 3.16.4 does not correctly bind the automatic login performed after user registration to the newly created account, allowing unauthenticated attackers to obtain an authenticated session for an arbitrary existing user, including administrators, on sites using a supported but non-default configuration.	N/A	More Details
CVE-2026-15244	The HUSKY WordPress plugin before 1.4.1 does not sanitize a stored setting value against directory traversal before concatenating it into a file inclusion path, allowing users with the shop manager capability to cause the inclusion and execution of arbitrary local files, which is then triggered on every front-end request including for unauthenticated visitors.	N/A	More Details
CVE-2026-14840	The YOP Poll WordPress plugin before 7.0.6 does not validate the connection's origin IP address and instead trusts client-controlled forwarding headers when enforcing its per-IP vote restriction, allowing unauthenticated attackers to bypass the vote limit and cast unlimited votes on a public poll.	N/A	More Details
CVE-2026-14836	The Login & Register Forms WordPress plugin before 3.2.5 does not properly enforce the rate limit on its password-reset verification-code flow, keying both the verification code and the per-source attempt counter on an unauthenticated, client-controlled value, allowing unauthenticated attackers to reset the limit at will and brute-force the code to take over any account, including administrators, when the verification-code reset mode is enabled.	N/A	More Details
CVE-2026-14823	The Event Tickets and Registration WordPress plugin before 5.29.0.1 does not properly verify authorization on some of its seating actions, allowing users with contributor-level access and above to overwrite the seating layout, ticket inventory, and attendee seat assignments of events they do not own.	N/A	More Details
CVE-2026-14822	The Event Tickets and Registration WordPress plugin before 5.29.0.1 does not perform any authorization check on one of its order-management REST endpoints, allowing unauthenticated users to change the status of existing orders.	N/A	More Details
CVE-2026-14596	The DynamicKit for Elementor WordPress plugin before 1.0.3 does not validate the host of a user-supplied URL used as the base of the password-reset link it emails, allowing unauthenticated attackers to send a target user a legitimately-formatted reset email whose link points to an attacker-controlled host and carries a valid reset key, leading to account takeover when the victim clicks it.	N/A	More Details
CVE-2026-14214	The Booking for Appointments and Events Calendar WordPress plugin before 2.4.4 does not restrict which fields can be written through its customer import, allowing a user with the Amelia Manager role to modify arbitrary columns of any stored user record by supplying them in the import request.	N/A	More Details
CVE-2026-67313	axios versions 0.28.0 and later contain uncontrolled recursion in formDataToJSON when processing FormData field names with deeply nested bracket segments. Attackers can supply FormData with field names containing thousands of nested brackets to exhaust the JavaScript call stack and trigger RangeError, causing request failure or process termination in applications that do not handle the exception.	N/A	More Details
CVE-2026-14197	The Fluent Support WordPress plugin before 2.3.1 does not perform a per-ticket access check before reassigning a ticket's customer, allowing a restricted support agent to change the assigned customer of any ticket in the system, including tickets outside their granted scope.	N/A	More Details
CVE-2026-14195	The Brizy WordPress plugin before 2.8.18 does not properly verify authorization on a request handler before returning post content, allowing users with the Contributor role or higher to read the content of arbitrary posts, including other users' private, pending, and draft posts.	N/A	More Details
CVE-2026-13729	The Podlove Podcast Publisher WordPress plugin before 4.5.3 does not perform nonce validation on some of its administrative create and delete actions, allowing attackers to create rogue records or delete legitimate ones via a forged request (CSRF) when a logged-in administrator is tricked into visiting a crafted page.	N/A	More Details

CVE-2026-13725	The Dynamic Pricing With Discount Rules for WooCommerce WordPress plugin before 5.0.0 does not validate a nonce or user capabilities on one of its AJAX actions and reflects unsanitised user input in the response, allowing unauthenticated attackers to perform Reflected Cross-Site Scripting against a victim who is induced to send a crafted request.	N/A	More Details
CVE-2026-13604	The Pixelavo WordPress plugin before 1.5.4 registers an unauthenticated AJAX action, gated only by a nonce that it emits publicly on every front-end page, that forwards client-supplied event data to the configured Facebook Conversions API using the administrator's stored access token. This allows an unauthenticated visitor to inject arbitrary conversion events into the administrator's Facebook ads account and exhaust the configured API quota.	N/A	More Details
CVE-2026-13158	The Everest Toolkit WordPress plugin through 1.2.3 does not validate the type of files uploaded during demo-content import (the WordPress file-type test is disabled), allowing high-privilege users (Administrator by default, including non-super-admin site administrators on multisite) to upload executable PHP files to the uploads directory.	N/A	More Details
CVE-2026-13157	The Demo Import WordPress plugin through 1.1.3 does not validate the type of files uploaded during demo-content import (the WordPress file-type test is disabled), allowing high-privilege users (Administrator by default, including non-super-admin site administrators on multisite) to upload executable PHP files to the uploads directory.	N/A	More Details
CVE-2026-11882	The Builderall for WordPress plugin before 3.0.2 does not bind the state value of its public OAuth authentication routes to the initiating user session, allowing unauthenticated attackers to complete the connection flow and overwrite the stored third-party integration access token. A durable overwrite requires the site to already be connected to a paid account.	N/A	More Details
CVE-2026-10827	The Spectra Legacy WordPress plugin before 2.20.0 does not validate or escape several block style attributes before using them to build the CSS it outputs on the front end, allowing users with the Contributor role and above to inject arbitrary CSS into the pages that render the affected block. The injected styles are served to anonymous visitors of those pages and can force external resource loads, deface/redress the page, or exfiltrate data via CSS attribute selectors. JavaScript execution is not possible at this role (the script-tag breakout is removed by KSES), so the impact is limited to CSS injection.	N/A	More Details
CVE-2026-9044	An OS command injection vulnerability exists in the VPN module of TP-Link AXE75 V1 routers. This vulnerability allows an adjacent, authenticated attacker to execute arbitrary commands on the device by importing a specially crafted VPN client configuration file. The issue arises from improper filtering of special characters. Successful exploitation of this vulnerability may enable an attacker to gain full control of the affected device, potentially compromising configuration integrity, network security, and service availability.	N/A	More Details
CVE-2026-54768	WPGraphQL provides a GraphQL API for WordPress sites. From 2.0.0 until 2.15.1, the deprecated user field on SendPasswordResetEmailPayload lets an unauthenticated caller distinguish existing author-class accounts through the sendPasswordResetEmail mutation and obtain public profile fields. This issue is fixed in version 2.15.1.	N/A	More Details
CVE-2026-53573	GeoNetwork is a catalog application to manage spatially referenced resources. From 3.12.0 until 4.2.16 and 4.4.11, unsafe redirect validation in GeonetworkOAuth2LoginAuthenticationFilter and KeycloakAuthenticationProcessingFilter permits an attacker-controlled external redirect after login. This issue is fixed in versions 4.2.16 and 4.4.11.	N/A	More Details
CVE-2025-67649	A SQL injection vulnerability has been identified in PHP Jabbers - Car Rental Script . Improper neutralization of input provided by user into parameters responsible for sorting functions allows an unauthenticated attacker to perform SQL Injection attacks. This issue was fixed in version 4.1.	N/A	More Details
CVE-2025-67650	An authenticated SQL injection vulnerability has been identified in multiple PHP Jabbers scripts. Improper neutralization of input provided by an authenticated user into parameters responsible for sorting functions allows an attacker to perform SQL Injection attacks. This issue was fixed in the versions specified in the affected products list.	N/A	More Details
CVE-2026-67312	axios versions from 0.28.0 before 0.33.0 and from 1.0.0 before 1.18.0 contain uncontrolled recursion in formDataToJSON (exposed as axios.formToJSON() and used internally when serializing FormData with Content-Type: application/json). When an application passes attacker-controlled FormData field names, a field name with thousands of nested bracket-delimited segments causes unbounded recursion in buildPath(), exhausting the JavaScript call stack (RangeError: Maximum call stack size exceeded) and causing denial of service for that request, or process termination in	N/A	More Details

	applications without appropriate error handling.		
CVE-2026-67314	axios versions >=1.15.2 and <1.18.0 contain prototype-pollution read-side gadgets in Basic auth subfield handling (lib/adapters/http.js and lib/helpers/resolveConfig.js). When an application is already affected by a separate prototype-pollution primitive and makes an axios request with an own auth object that omits the username and/or password properties, axios reads the inherited Object.prototype.username and Object.prototype.password values and uses them to construct an outbound 'Authorization: Basic ...' header. axios itself does not pollute prototypes. The practical impact is outbound request tampering: an attacker who controls the polluted prototype values can inject attacker-chosen Basic auth credentials or replace an existing Authorization header. Credential disclosure is only possible under additional application-specific conditions.	N/A	More Details
CVE-2026-46714	Misskey is an open source, federated social media platform. IVersions 8.63.0 and later, but prior to 2026.5.4, contain a vulnerability that can cause the Misskey web client to slow down or crash when it applies a malformed theme. This issue has been fixed in version 2026.5.4.	N/A	More Details
CVE-2026-9335	A vulnerability in keras-team/keras versions <= 3.14.0 allows arbitrary local HDF5 file content disclosure due to improper handling of HDF5 ExternalLinks. The `KerasFileEditor` and `keras.saving.load_weights` functions bypass the `safe_get_h5_group` and `safe_get_h5_dataset` helpers, which are designed to reject ExternalLinks and SoftLinks. This results in automatic dereferencing of links to external HDF5 files, enabling attackers to disclose sensitive data from the victim's local filesystem. Specifically, `KerasFileEditor` extracts attributes and datasets from linked files into its internal structures, while `keras.saving.load_weights` loads weights from linked files into the user's model. This issue can be exploited by providing a malicious `.h5`, `.weights.h5`, or `.keras` file containing ExternalLinks.	N/A	More Details
CVE-2026-12185	In Bouncy Castle for Java before 1.85, BKS/UBER keystore allocates from untrusted lengths before integrity check. This issue also affects Bouncy Castle for Java LTS before 2.73.12.	N/A	More Details
CVE-2026-55777	GoAccess is a real-time web log analyzer and interactive viewer that runs in a terminal in *nix systems or through the browser. Prior to 1.11, the parse_ios() function uses an attacker-controlled keyword-to-OS offset as both the source offset and copy length for memmove, allowing a crafted User-Agent in a processed access log to read up to approximately 4 KB beyond the heap allocation and conditionally crash GoAccess. This issue is fixed in version 1.11.	N/A	More Details
CVE-2026-9856	A vulnerability in huggingface/transformers versions <=5.8.0.dev0 allows an attacker to perform arbitrary file writes via path traversal. The issue resides in the `save_pretrained()` methods of `PreTrainedTokenizerBase` and `ProcessorMixin`, where keys from the `chat_template` dictionary are used directly as filenames without proper validation. An attacker can exploit this by publishing a malicious Hugging Face Hub repository with a crafted `tokenizer_config.json` file. When a victim downloads and saves the tokenizer or processor, the attacker-controlled keys can escape the intended save directory, enabling arbitrary file writes with attacker-controlled content. This vulnerability affects multiple processors inheriting from `ProcessorMixin`, including Idefics, Florence, Gemma, Phi, and Qwen-VL.	N/A	More Details
CVE-2026-17735	Insufficient validation of untrusted input in BFCache in Google Chrome prior to 151.0.7922.72 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)	N/A	More Details
CVE-2026-16256	The POUCO Import Users WordPress plugin through 1.0.0 does not perform any capability or nonce checks on AJAX actions available to unauthenticated users that create and update WordPress accounts, and it trusts an attacker-supplied role value, allowing unauthenticated attackers to create a new administrator account and take over the site.	N/A	More Details
CVE-2026-15939	The Simple Restrict WordPress plugin before 1.2.9 does not enforce its content-restriction permission check on the REST API the way it does on the front end, relying there on a generic capability check instead of the Simple Restrict WordPress plugin before 1.2.9's own permission system, allowing users with contributor-level access or above to read the content of restricted posts and pages they were never granted access to.	N/A	More Details
CVE-2026-17913	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	N/A	More Details
CVE-	The Meta Box WordPress plugin before 5.13.1 does not verify that a user is authorized to delete		More

2026-15248	the supplied attachment before deleting it, allowing users with a low-privilege role such as Contributor to permanently delete arbitrary media attachments belonging to other users.	N/A	Details
CVE-2026-58039	A flaw in Node.js Permission Model enforcement allows process.report writes (and overwrites) files outside --allow-fs-write paths. This can lead to confidentiality impact or bypass of the intended security boundary under affected configurations. This vulnerability affects Node.js **22.x**, **24.x**, and **26.x**.	N/A	More Details
CVE-2026-14938	The FluentBoards WordPress plugin before 1.95.3 does not verify that the items selected for a board import operation belong to a board the requesting user is authorized to access, allowing any authenticated user with member access to a single board to copy and read the stages and tasks (including titles, descriptions and file attachments) of any other board on the site.	N/A	More Details
CVE-2026-14537	Incorrect Authorization in the direct HTTP API tool invocation endpoint in Google mcp-toolbox versions v1.3.0 and v1.4.0 allows an unauthenticated attacker to invoke tools protected by the scopeRequired feature via sending tool invocation requests through legacy HTTP endpoints when the --enable-api flag is active.	N/A	More Details
CVE-2026-14538	An improper authorization and security-boundary bypass vulnerability in the bigquery-execute-sql tool component of Google mcp-toolbox versions 0.16.1 through 1.4.0 allows an authenticated attacker to bypass allowedDatasets validation checks. The toolbox relies on the BigQuery dry-run API to enforce dataset restrictions, but due to a fail-open logic flaw, it bypasses validation when the API returns an empty array for specialized constructs. This allows the attacker to extract structural DDL schemas for explicitly excluded datasets via INFORMATION_SCHEMA, and access downstream federated row data via EXTERNAL_QUERY connections.	N/A	More Details
CVE-2026-14539	An allocation of resources without limits vulnerability in the HTTP handler component of Google mcp-toolbox versions up to and including 1.4.0 allows an unauthenticated attacker to cause a denial of service (DoS). The /mcp endpoint handler reads incoming payloads directly into system memory using an unrestricted buffer loop (io.ReadAll) without applying defensive constraints such as http.MaxBytesReader or pre-read Content-Length enforcement. By submitting a single, massive HTTP request body, an attacker can linearly consume available host memory until the runtime process is terminated by an Out-Of-Memory (OOM) error.	N/A	More Details
CVE-2026-11872	The Clever Mega Menu for Visual Composer WordPress plugin through 1.0.1 does not perform a nonce or capability check in an AJAX action that updates navigation menu item metadata, allowing any authenticated user, including Subscribers, to overwrite menu item content and settings that are rendered in the site's public navigation.	N/A	More Details
CVE-2026-14540	A Server-Side Request Forgery (SSRF) vulnerability exists in the generic HTTP source and tool components of Google mcp-toolbox versions 0.3.0 through 1.4.0. While the toolbox implements baseline input sanitization for user-controlled parameters, the underlying HTTP client (internal/sources/http/http.go) fails to safely regulate request redirection boundaries. Specifically, the client is initialized without a restrictive CheckRedirect policy hook and lacks target IP validation. An attacker or a malicious data-driven prompt can supply a crafted path parameter that triggers an open redirect or a direct destination swap on the target backend, coercing the mcp-toolbox into blindly following the redirection and making unauthorized requests to internal or arbitrary external endpoints.	N/A	More Details
CVE-2026-67315	axios versions 0.31.0 before 0.33.0 and 1.15.0 before 1.18.0 fail to recognize 0.0.0.0 as a loopback address in shouldBypassProxy.js, allowing requests to 0.0.0.0 to bypass NO_PROXY rules. Attackers can supply 0.0.0.0 URLs to route requests through configured proxies, potentially exposing local services when the proxy can reach the destination.	N/A	More Details
CVE-2026-17002	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-14541	An authentication bypass and audience confusion vulnerability exists in the Google OAuth provider component of Google mcp-toolbox version 1.4.0. When a Google authService is initialized with mcpEnabled: true but lacks an explicitly defined audience or clientId, the ValidateMCPAuth pipeline for opaque tokens skips audience validation entirely. As a result, the toolbox will accept any valid Google OAuth access token—even those minted for unrelated ecosystem applications—granting unauthorized clients access to protected tools and data backends.	N/A	More Details
	Improper Verification of Cryptographic Signature in ueberauth guardian allows an unauthenticated attacker to revoke a victim's session with a forged token. Guardian.revoke/3 in lib/guardian.ex		

CVE-2026-55735	decodes the supplied token with peek/1, which performs no signature verification (it only base64-decodes the JWT header and payload). The resulting unverified claims are forwarded directly to the configured token module's revoke callback and the implementation's on_revoke callback, a state-mutating sink. The sibling operations refresh/2 and exchange/4 both call decode_and_verify first, so the signature is checked before anything acts on the claims; revoke/3 is the only state-mutating path that acts on claims without verifying the signature. An attacker who knows or guesses a victim's identifying claim values (jti, sub) can forge a JWT carrying those claims, sign it with an arbitrary key, and submit it to any endpoint that funnels a caller-supplied token into Guardian.revoke/3 (the standard logout / session-revocation pattern). When the token module mutates state keyed by the claims (whitelist deletion or blacklist insertion, for example a GuardianDb-style store), the victim's legitimate session is evicted. This is an unauthenticated session-revocation denial of service; the attacker never needs the signing secret. This issue affects guardian: from 1.0.0 before 2.4.1.	N/A	More Details
CVE-2026-55734	Allocation of Resources Without Limits or Throttling vulnerability in ueberauth guardian (Guardian.Permissions module) allows a denial of service via BEAM atom-table exhaustion. This vulnerability is associated with program file lib/guardian/permissions.ex and program routines 'Elixir.Guardian.Permissions':encode_permissions!/1, 'Elixir.Guardian.Permissions':encode_permissions_into_claims!/2, 'Elixir.Guardian.Permissions':do_encode_permissions!/2. The Guardian.Permissions mixin installs a public encode_permissions!/1 function on every module that does use Guardian.Permissions. For each key of the supplied map, encode_permissions!/1 calls String.to_atom(to_string(k)) before any validation runs. The integer-value clause of do_encode_permissions!/2 then short-circuits straight to encoding without validating the key against the configured permission set, so a key with an integer value is interned as a fresh atom with no exception raised. Atoms are never garbage collected and the BEAM atom table is a fixed-size resource (default roughly 1,048,576 entries), so each unique attacker-chosen key permanently consumes one slot. An attacker who can influence a permission map that reaches encode_permissions!/1 (for example a permissions map read from a request body and passed into token issuance via encode_permissions_into_claims!/2) can mint an unbounded number of atoms and exhaust the atom table, crashing the entire BEAM node and every service running on it. The sibling decode_permissions/1 is not affected because it skips keys absent from the configured permission set. This issue affects guardian: from 2.0.0 before 2.4.1.	N/A	More Details
CVE-2026-55733	Allocation of Resources Without Limits or Throttling in ueberauth guardian allows denial of service via unbounded atom creation from attacker-controlled binary input. Guardian.Permissions.AtomEncoding encodes permission scopes by passing arbitrary binaries to String.to_atom/1. When encode/3 in lib/guardian/permissions/atom_encoding.ex is called with a list, each binary entry is handled by the encode_value/3 binary clause, which calls String.to_atom(value) with no allow-list check. The perm_set argument (the application's small, finite set of legitimate permission names) is discarded, so any external string flows straight into atom creation. This encoder is selected with use Guardian.Permissions, encoding: Guardian.Permissions.AtomEncoding and reached through the imported encode/3 entry point. String.to_atom/1 creates a brand-new atom for every previously unseen binary, atoms are never garbage collected, and the BEAM atom table is fixed at roughly 1,048,576 entries by default. An application that funnels attacker-influenced permission scopes (from a request body, a JWT claim, or other external input) into encode/3 therefore mints one permanent atom per distinct value. A modest stream of varied, unauthenticated input permanently consumes the atom table and crashes the BEAM node with system_limit, taking down every application running on it. The default encoder is Guardian.Permissions.BitwiseEncoding, which is not affected. This issue affects guardian: from 2.0.0 before 2.4.1.	N/A	More Details
CVE-2026-54894	Allocation of Resources Without Limits or Throttling in ueberauth guardian allows denial of service via unbounded atom creation from attacker-influenced binary input. Guardian.Plug.Keys derives connection and session namespace keys by passing arbitrary binaries to String.to_atom/1. base_key/1 in lib/guardian/plug/keys.ex converts any binary into the atom :"guardian_<input>", and the derived helpers claims_key/1, resource_key/1, and token_key/1 create a second atom on top of that. key_from_other/1 likewise converts a regex-captured binary through String.to_atom/1. The public specs advertise String.t() as a valid argument, so passing a string is documented usage, and higher-level entry points such as Guardian.Plug.current_token(conn, key: key) thread the caller-supplied key straight into these functions. String.to_atom/1 creates a brand-new atom for every previously unseen binary, atoms are never garbage collected, and the BEAM atom table is fixed at roughly 1,048,576 entries by default. An application that routes attacker-influenced data (a tenant identifier, header, or other request input) into a Guardian key therefore mints one permanent atom per distinct value. A modest stream of varied, unauthenticated input	N/A	More Details

	permanently consumes the atom table and crashes the BEAM node, taking down every application running on it. This issue affects guardian: from 0.1.0 before 2.4.1.		
CVE-2026-6889	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-6890	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-67321	axios versions 0.31.1 before 0.33.0 and 1.15.1 before 1.18.0 contain an incomplete depth-limit bypass in toFormData.js when serializing objects with top-level keys ending in '{}'. Attackers who control object keys and nested values passed to axios form or parameter serialization can trigger a RangeError from JSON.stringify, causing denial of service in the affected request path.	N/A	More Details
CVE-2026-67320	axios in a Node.js deployment using the HTTP adapter can route requests through an attacker-controlled proxy. axios hardens merged request configuration by creating a null-prototype object, but request interceptors run after the merge; a common immutable interceptor pattern such as {...config} or Object.assign({}, config) converts the hardened config back into a regular object. axios then dispatches that object without re-hardening it, and the Node HTTP adapter reads config.proxy through the prototype chain. If an attacker can pollute Object.prototype.proxy, affected requests can be routed through an attacker-controlled proxy. For plaintext HTTP requests, the proxy can observe Authorization headers, Basic auth from config.auth, method, absolute URL, Host, and request body, and can return its own response. This does not establish browser impact or HTTPS header/body disclosure under normal TLS validation. Affected versions are >=0.31.1 (fixed in 0.33.0) and >=1.15.2 (fixed in 1.18.0).	N/A	More Details
CVE-2026-67319	axios before 0.33.0 (and 1.x before 1.18.0) can consume inherited properties from nested request option objects when the JavaScript process's Object.prototype has already been polluted by another component. While the top-level merged config uses a null prototype, nested plain objects such as auth and paramsSerializer are cloned into ordinary objects and read without own-property checks. When an application passes placeholder nested objects such as auth: {} or paramsSerializer: {}, inherited username/password values can cause silent injection of an Authorization: Basic header, and inherited encode/serialize values can alter query-string serialization (full serializer replacement requires a function-valued pollution primitive). This is exploitable only in the presence of pre-existing prototype pollution.	N/A	More Details
CVE-2026-67318	axios versions >=1.13.0 (Node.js HTTP adapter) fail to enforce the configured maxBodyLength limit on streamed request bodies when requests are sent with httpVersion: 2. Because Node's HTTP/2 request API does not honor the maxBodyLength option and axios's byte-counting stream wrapper is gated on maxRedirects === 0, an attacker who controls a stream passed to axios can cause the application to transmit outbound data exceeding the configured finite maxBodyLength. Impact is limited to resource consumption and policy bypass (excess egress, upstream quota consumption, limited availability); it does not enable code execution, credential disclosure, or request-destination control. Calls using the default maxBodyLength: -1 and browser adapters are not affected.	N/A	More Details
CVE-2026-67317	axios versions 1.7.0 before 1.18.0 fail to enforce maxBodyLength for WHATWG ReadableStream request bodies in the fetch adapter when Content-Length cannot be determined. Attackers can supply unknown-length stream data to bypass upload size limits and cause uncontrolled network egress or resource exhaustion.	N/A	More Details
CVE-2026-67316	axios is vulnerable to read-side prototype-pollution gadgets that can alter request construction when Object.prototype has already been polluted by a separate vulnerability or dependency. In the bodyless method aliases (axios.get(), axios.delete(), axios.head(), axios.options()), inherited data is read via (config || {}).data before config normalization, causing an attacker-controlled body to be sent on requests that did not set one. Additional low-level paths, only reachable when calling exported adapters/helpers (e.g. lib/adapters/http.js, unsafe/helpers/resolveConfig.js) directly with plain configs and no own proxy or paramsSerializer, can inherit polluted proxy values (routing requests through an attacker-controlled proxy) or paramsSerializer values (attacker-controlled URL serialization). These low-level gadgets do not reproduce through normal high-level axios calls on 1.15.2+. The issue is fixed in axios 1.18.0 and 0.33.0.	N/A	More Details
CVE-2026-	Jodit Editor is a WYSIWYG editor with a built-in file browser & image editor. Prior to 4.13.6, Jodit's clean-html denyTags filter does not normalize foreign SVG or MathML script node names, allowing a script element nested directly in SVG or MathML to remain in editor.value and execute when	N/A	More Details

65841	content is loaded. This issue is fixed in version 4.13.6.		
CVE-2025-67651	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in multiple PHP Jabbers scripts. The lack of CSRF tokens or appropriate SameSite attributes allows an attacker to send unauthorized requests in the context of an authenticated user, leading to unauthorized administrative actions, such as creating new admin accounts. This issue was fixed in the versions specified in the affected products list.	N/A	More Details
CVE-2026-62959	Coturn is a free open source implementation of TURN and STUN Server. From 4.5.2 through 4.14.0, when Coturn is started with --acme-redirect <URL> and exposes a plaintext-TCP listener, an unauthenticated remote client can send a single ordinary HTTP GET request and receive a 301 response whose Location header contains up to ~870 bytes of adjacent process heap memory. The leaked region is a recycled network receive buffer that is reused without being zeroed, so on a busy server it can contain data from other clients' requests (TURN credentials, OAuth tokens, relayed payloads). Root cause is a signed→unsigned conversion. This issue is fixed in version 4.15.0.	N/A	More Details
CVE-2026-51255	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51283	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51282	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51281	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51280	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51279	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51278	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51277	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51276	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51265	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51264	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51262	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was	N/A	More

51258	withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.		Details
CVE-2026-51257	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51256	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51253	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-46593	A SQL injection vulnerability has been identified in the PHP Jabbers - PHP Poll Script. Improper neutralization of input provided by user to pjAdminPolls.controller.php endpoint allows an authenticated attacker to perform SQL Injection attacks. This issue was fixed in version 4.1.	N/A	More Details
CVE-2026-51250	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51249	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51248	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51247	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51246	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51245	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51243	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51242	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51241	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51240	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51239	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51238	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was	N/A	More

51237	withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.		Details
CVE-2026-51236	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51284	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51285	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51286	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51287	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-46594	A reflected cross-site scripting (XSS) vulnerability has been identified in the PHP Jabbers - PHP Poll Script. A malicious attacker can craft a specially crafted URL that, when opened, results in arbitrary JavaScript execution in the victim's browser. This issue was fixed in version 4.1.	N/A	More Details
CVE-2026-53551	free5GC is an open-source implementation of the 5G core network. Prior to 1.4.5, the free5GC AUSF (Authentication Server Function) does not validate the supiOrSuci field in UE authentication requests. Null bytes (\x00) and other control characters pass through JSON parsing unchanged and are forwarded to the UDM in an unescaped URL path. This causes Go's net/url.Parse() to fail, returning HTTP 500 "System failure" and leaking internal stack traces. An unauthenticated attacker can trigger this at scale causing denial of service for all subscribers attempting authentication through the affected AUSF. This vulnerability is fixed in 1.4.5.	N/A	More Details
CVE-2026-15227	Missing authorization in Checkmk <2.5.0p10, <2.4.0p35, <2.3.0p49, and 2.2.0 (EOL) allows an authenticated user lacking the "Edit foreign Reports" permission to modify reports owned by other users.	N/A	More Details
CVE-2026-17592	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-68574	Rejected reason: Reserved via standalone CLI outside the OSIM flaw workflow; releasing so the CVE ID can be properly reserved and linked through OSIM when the flaw is worked.	N/A	More Details
CVE-2026-53502	Thumbor is an open-source photo thumbnail service by globo.com. Prior to 7.8.0, file_loader decodes percent-encoded path segments after its root-boundary validation, allowing traversal outside FILE_LOADER_ROOT_PATH through watermark or frame filter input. This issue is fixed in 7.8.0.	N/A	More Details
CVE-2026-68575	Rejected reason: Reserved via standalone CLI outside the OSIM flaw workflow; releasing so the CVE ID can be properly reserved and linked through OSIM when the flaw is worked.	N/A	More Details
CVE-2026-68576	Rejected reason: Reserved via standalone CLI outside the OSIM flaw workflow; releasing so the CVE ID can be properly reserved and linked through OSIM when the flaw is worked.	N/A	More Details
CVE-2026-55100	hashi-vault-js is a Node.js module for interacting with the HashiCorp Vault API. Prior to 0.5.2, src/Vault.js concatenates unencoded identifier values including name, username, group, role, and version into Vault request paths and query strings instead of using encodeURIComponent() and URLSearchParams, allowing path traversal and query parameter injection. This issue is fixed in version 0.5.2.	N/A	More Details
CVE-2026-	Rejected reason: Reserved via standalone CLI outside the OSIM flaw workflow; releasing so the	N/A	More

68577	CVE ID can be properly reserved and linked through OSIM when the flaw is worked.		Details
CVE-2026-54729	DSSRF is a Node.js library that provides a wide range of utilities and advanced SSRF defense checks. Prior to 1.0.5, is_url_safe can treat localhost as safe when DNS resolver 1.1.1.1 returns NXDOMAIN because dns.resolve4 yields no address and no dns.lookup fallback occurs, allowing server-side request forgery. This issue is fixed in version 1.0.5.	N/A	More Details
CVE-2026-34497	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in Johnson Controls FM Systems Employee allows Cross-Site Scripting (XSS). This issue affects FM Systems Employee: before 2025.3.1.	N/A	More Details
CVE-2026-34495	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Johnson Controls FM Systems Employee allows Stored XSS. This issue affects FM Systems Employee: before 2025.3.1.	N/A	More Details
CVE-2026-34490	Cleartext storage of sensitive information vulnerability in Johnson Controls XAAP Application on Android allows an attacker on a jailbroken or otherwise compromised device to Retrieve Sensitive Data. This issue affects XAAP Application: before 1.53.	N/A	More Details
CVE-2026-21662	Unrestricted upload of file with dangerous type vulnerability in Johnson Controls FM Systems Employee allows Using Malicious Files. This issue affects FM Systems Employee: before 2025.3.1.	N/A	More Details
CVE-2026-58048	Improper preservation of SQL mode when renaming databases in cPanel allows execution of SQL in root context.	N/A	More Details
CVE-2026-58047	HTTP Smuggling in cPanel allows potential leak of credentials.	N/A	More Details
CVE-2026-9611	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-59232	Cross-site Scripting in the lead index view in Roskus Prospero Flow CRM before 5.3.7 allows authenticated users holding the create or update lead permission to execute arbitrary JavaScript in the application origin via HTML markup stored in the lead name field, which the view renders through Blade's unescaped output directive and inside a JavaScript string literal in an onclick attribute.	N/A	More Details
CVE-2026-59231	Server-Side Request Forgery in the PDF export component in maalfer Pentestify before 1.1.0 allows authenticated users to cause outbound HTTP GET requests from the server to arbitrary attacker-chosen destinations via unvalidated URLs stored in the finding images field or the report client_logo field, which the server-side headless browser fetches while rendering the report.	N/A	More Details
CVE-2026-65636	Improper Neutralization of CRLF Sequences vulnerability in ufirstgroup ymlr (Elixir.Ymlr module) allows attackers to inject arbitrary content into generated YAML documents through document comments. Ymlr.document!/2 interpolates each caller-supplied comment string into the output behind a single # prefix without validating it or escaping line breaks. Because a YAML comment is terminated by a line break, the first carriage return or line feed in the comment string ends the comment context and everything after it is emitted at column 0 of the document body. An attacker who controls text that the host application passes as a comment can forge top-level mapping keys, override values the application itself set, and emit --- or ... markers that split the output into additional documents. Downstream consumers of the generated YAML, such as configuration loaders, deployment manifests, CI pipelines and data importers, parse the injected content as legitimate data. The same clause backs Ymlr.document/2, Ymlr.documents!/2 and Ymlr.documents/2, so every document encoding entry point is affected. This vulnerability is associated with program files lib/ymlr.ex and program routines 'Elixir.Ymlr':document!/2, 'Elixir.Ymlr':documents!/2. This issue affects ymlr from 0.0.1 before 5.1.6.	N/A	More Details
CVE-2026-51229	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was	N/A	More

51230	withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.		Details
CVE-2026-51231	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51232	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51301	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51299	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51289	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51288	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-15055	In Bouncy Castle for Java before 1.85, PKCS#8 / PBES2 decryptors honour unbounded KDF cost from input. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bcpkix-fips 1.0.12 (1.0.X series), 2.0.12 (2.0.X series) and 2.1.12 (2.1.X series).	N/A	More Details
CVE-2026-59638	In Bouncy Castle for Java before 1.85, JSSE hostname verifier CN-fallback enabled by default despite documented opt-in. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bctls-fips 1.0.24 (1.0.X series), 2.0.24 (2.0.X series) and 2.1.24 (2.1.X series).	N/A	More Details
CVE-2026-59639	In Bouncy Castle for Java before 1.85, CMS verifySignatures returns true for SignedData with zero signers. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bcpkix-fips 1.0.12 (1.0.X series), 2.0.12 (2.0.X series) and 2.1.12 (2.1.X series).	N/A	More Details
CVE-2026-68869	Rejected reason: This CVE ID was assigned in error. Upon further review, the reported issue does not represent a security vulnerability and does not require a CVE record.	N/A	More Details
CVE-2026-66737	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-12357	Heimdall Data Database Proxy generateFileContent CRLF Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Heimdall Data Database Proxy. Authentication is required to exploit this vulnerability. The specific flaw exists within the generateFileContent function. The issue results from the lack of proper neutralization of CRLF sequences. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-29251.	N/A	More Details
CVE-2025-15631	A cryptographic weakness exists in affected Omada devices where site credentials are protected using a legacy hashing algorithm that does not provide sufficient protection. An attacker who obtains access to stored credential data may be able to recover valid credentials to gain unauthorized access to affected devices or management environments.	N/A	More Details
CVE-2025-15630	A race condition exists in the cloud-based Omada device adoption process when an attacker may be able to interact with the adoption workflow before a legitimate device completes registration, resulting in provisioning information being delivered to an attacker. Successful exploitation may allow disclosure of provisioning information intended for a legitimate device.	N/A	More Details
	A cryptographic weakness exists in the Omada adoption protocol where session encryption keys		

CVE-2025-15629	used to protect communications between controllers and managed devices may be predictable due to insufficient entropy in session key generation. An attacker who successfully intercepts adoption-related communications may be able to recover session encryption keys and decrypt affected communications.	N/A	More Details
CVE-2025-15628	Affected Omada devices rely on embedded certificates that are shared across deployments to establish trust between controllers and managed devices. An attacker who obtains the embedded certificates may be able to impersonate trusted controllers or devices and intercept affected communications.	N/A	More Details
CVE-2025-15627	A cryptographic weakness exists in the Omada adoption protocol. The protocol relies on hard-coded cryptographic keys to establish trust and protect authentication exchanges between controllers and managed devices during device adoption. An attacker may be able to impersonate trusted controllers or managed devices and gain access to sensitive adoption-related communications.	N/A	More Details
CVE-2025-15544	A cryptographic weakness exists in the Omada device adoption process. During adoption, authentication credentials associated with site management are transmitted using a weak hashing algorithm that does not provide sufficient protection. An attacker who successfully intercepts adoption-related authentication traffic may be able to recover valid credentials and gain unauthorized access to managed devices or controller-managed environments.	N/A	More Details
CVE-2026-13268	G DATA Total Security Backup Service Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of G DATA Total Security. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Backup Service. By creating a symbolic link, an attacker can abuse the service to delete a file. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-28665.	N/A	More Details
CVE-2025-9291	A certification validation weakness exists in communication between affected Omada devices and cloud controllers. Certificate identity verification does not adequately validate that a presented certificate corresponds to the expected cloud controller hostname, which may allow certificate validation protections to be bypassed under specific conditions. Successful exploitation may allow interception or modification of communication between affected devices and cloud controllers.	N/A	More Details
CVE-2026-69153	PostCSS takes a CSS file and provides an API to analyze and modify its rules by transforming the rules into an Abstract Syntax Tree. Prior to 8.5.19, if from is unset, an attacker can cause PreviousMap.loadFile() to read an unintended source-map file by supplying an absolute or directory-traversal sourceMappingURL. The resulting map’s sources and sourcesContent may then be exposed to the application. This issue is fixed in version 8.5.19.	N/A	More Details
CVE-2026-69151	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 20.3.27, 21.2.19, and 22.0.1, the Angular compiler i18n pipeline permits i18n-onerror and other i18n-on event-handler attributes, allowing a lower-trust translation file to replace a static handler with executable JavaScript. This issue is fixed in versions 20.3.27, 21.2.19, and 22.0.1.	N/A	More Details
CVE-2026-69149	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 20.3.27, 21.2.19, and 22.0.7, a Cross-Site Scripting (XSS) vulnerability exists in @angular/platform-server's DOM emulation dependency (domino) when serializing the content of fallback raw-content elements (<iframe>, <noembed>, <noframes>, and <noscript>). This issue is fixed in versions 20.3.27, 21.2.19, and 22.0.7.	N/A	More Details
CVE-2026-68945	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 20.3.27, 21.2.19, and 22.0.2, HttpTransferCache comma-joins repeated request parameters, allowing semantically distinct HttpClient requests to use the same transfer-cache key and reuse a wrong backend response. This issue is fixed in versions 20.3.27, 21.2.19, and 22.0.2.	N/A	More Details
CVE-2026-18266	Dify AI Workflow oauth_redirect_url Open Redirect Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Dify. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the OAuth flow handling in the AppInitializer component. An attacker can force a redirection to a site that serves malicious content. An attacker can leverage this vulnerability to disclose information in the context of the application.	N/A	More Details

	Was ZDI-CAN-29196.		
CVE-2026-6102	MSI Center NTIOLib_X64 Origin Validation Error Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of MSI Center. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the NTIOLib_X64.sys driver. The issue results from insufficient validation of the origin of commands. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-28935.	N/A	More Details
CVE-2026-5056	GStreamer qtdemux Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GStreamer. Interaction with this library is required to exploit this vulnerability but attack vectors may vary depending on the implementation. The specific flaw exists within the parsing of UncompressedFrameConfigBox structures. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-29392.	N/A	More Details
CVE-2026-5057	ATEN Unizon RpcProvider Missing Authentication Denial-of-Service Vulnerability. This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of ATEN Unizon. Authentication is not required to exploit this vulnerability. The specific flaw exists within the RpcProvider class. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-29041.	N/A	More Details
CVE-2026-5487	DriveLock Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of DriveLock. Authentication is not required to exploit this vulnerability. The specific flaw exists within the web service, which listens on TCP port 4568 by default. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of the service account. Was ZDI-CAN-28746.	N/A	More Details
CVE-2026-5489	DriveLock Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of DriveLock. Authentication is not required to exploit this vulnerability. The specific flaw exists within the web service, which listens on TCP port 4568 by default. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of the service account. Was ZDI-CAN-28719.	N/A	More Details
CVE-2026-5490	DriveLock SQL Injection Privilege Escalation Vulnerability. This vulnerability allows remote attackers to escalate privileges on affected installations of DriveLock. Authentication is required to exploit this vulnerability. The specific flaw exists within the web service, which listens on TCP port 4568 by default. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from the user. . Was ZDI-CAN-28726.	N/A	More Details
CVE-2026-18243	Certain HP DesignJet products may be potentially vulnerable to cross-site scripting (XSS), which may allow unauthenticated HTTP requests to view print job previews.	N/A	More Details
CVE-2026-11771	OpenVPN version 2.1.0 through 2.6.20 and 2.7_alpha1 through 2.7.4 allows attackers via an off-by-one buffer write in the NTLM proxy authentication to potentially cause a crash via a crafted NTLM response from a malicious proxy server	N/A	More Details
CVE-2026-5491	DriveLock Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of DriveLock. Authentication is not required to exploit this vulnerability. The specific flaw exists within the web service, which listens on TCP port 6067 by default. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of the service account. Was ZDI-CAN-28722.	N/A	More Details
CVE-2026-12932	A memory leak in the tls-crypt-v2 client key extraction in OpenVPN 2.5.0 through 2.6.20 and 2.7_alpha1 through 2.7.4 allows remote attackers to cause a denial of service (memory exhaustion) via a flood of crafted packets	N/A	More Details
	DriveLock Directory Traversal Information Disclosure Vulnerability. This vulnerability allows		

CVE-2026-5492	remote attackers to disclose sensitive information on affected installations of DriveLock. Authentication is required to exploit this vulnerability. The specific flaw exists within the web service, which listens on TCP port 4568 by default. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of the service account. Was ZDI-CAN-28713.	N/A	More Details
CVE-2026-63118	MCP Ruby SDK is the official Ruby SDK for Model Context Protocol servers and clients. Prior to 0.23.0, MCP::Server::Transports::StreamableHTTPTransport in the mcp gem does not validate the HTTP Host or Origin request headers, which allows a malicious browser page to use DNS rebinding to reach a locally running MCP server and invoke exposed tools. This issue is fixed in version 0.23.0.	N/A	More Details
CVE-2026-67431	MCP Ruby SDK is the official Ruby SDK for Model Context Protocol servers and clients. Prior to 0.23.0, MCP::Server::Transports::StreamableHTTPTransport in the mcp gem does not bind a session ID to a session owner, allowing an attacker with a stolen session ID to send tools/call requests that execute in the victim's session. This issue is fixed in version 0.23.0.	N/A	More Details
CVE-2026-67433	Linuxfabrik monitoring-plugins provides Python monitoring plugins for Icinga, Nagios, and related monitoring systems. In version 6.0.0, the logfile check legacy database migration moved a predictable path from /tmp with os.rename() and allowed a local user controlling the plugin account to place a symlink that would be followed by sqlite3.connect() during a root-run check.	N/A	More Details
CVE-2026-67435	linuxfabrik-lib provides Python modules for database access, caching, shell execution, and API integrations. Prior to version 6.0.0, lib.url.fetch() followed cross-origin redirects while forwarding caller-supplied credential headers other than Authorization and Cookie, allowing a malicious redirect-capable server to receive headers such as X-Auth-Token from authenticated monitoring requests. This issue is fixed in version 6.0.0.	N/A	More Details
CVE-2026-62995	joserfc is a Python library that provides an implementation of several JSON Object Signing and Encryption (JOSE) standards. in versions 1.7.1 and prior, joserfc accepts JWTs with trailing padding (==) which are not conforming to the JOSE specifications. This leads to malleability of the JWTs when consumed by joserfc. Depending on this application this might or not be an issue. This could lead to bypass of token revocation or anti-replay protection when implemented as a deny list of tokens or a deny list of token hashes. Note that ECDSA JWS are always malleable because of the malleability of ECDSA signatures (first test case in the code bellow). This makes a scheme which assumes that JWTs are not malleable brittle. However for other signatures (or MAC) schemes it might make sense to assume non malleability of the token. This issue has been fixed in version 1.7.2.	N/A	More Details
CVE-2026-47211	Ouroboros is a local-first runtime for AI coding agents that records their actions and applies user-defined policies to constrain behavior. In versions prior to 0.39.0, if a user clones a malicious repository and runs Ouroboros commands within that directory, it can lead to arbitrary code execution and potential system takeover. The vulnerability stems from Ouroboros loading the .env file from the current working directory. Execution-affecting environment variables such as OUROBOROS_CLI_PATH, OPENCODE_CLI_PATH, and other backend selectors are accepted directly from this local .env. An attacker can include a malicious script in the repository and point the CLI path variable to it (e.g., OUROBOROS_CLI_PATH=./malicious_script.sh). When the user executes a command like ouroboros init or any command that instantiates the adapter, the malicious script is executed instead of the intended CLI. This issue has been fixed in version 0.39.0.	N/A	More Details
CVE-2026-59898	Netty is an asynchronous, event-driven network application framework. Prior to versions 4.1.136.Final and 4.2.16.Final, ab attacker can force WebSocket upgrade via the lax V07 (or V08) handshaker by sending `Sec-WebSocket-Version: 7` and omitting `Connection: Upgrade` / `Upgrade: websocket` headers, completing a protocol switch that a proxy would not recognize as an Upgrade request and enabling HTTP request smuggling / protocol-confusion attacks. This issue has been fixed in versions 4.1.136.Final and 4.2.16.Final.	N/A	More Details
CVE-2026-62354	Authorization handling for Parameter Context validation requests in Apache NiFi 1.10.0 through 2.10.0 allows clients with read access to submit proposed Parameter values. The proposed values override current configuration, enabling users with read access to invoke predefined component validation methods with alternative settings. Apache NiFi installations that do not implement different levels of authorization for viewing and modifying Parameter Context configuration are not subject to this vulnerability. Upgrading to Apache NiFi 2.11.0 is the recommended mitigation, requiring write access to submit Parameter Context validation requests.	N/A	More Details
CVE-	Misskey is an open source, federated social media platform. Versions 12.37.0 and later, but prior		

2026-46713	to 2026.5.4, contain a vulnerability in the JSON-LD signature validation and compaction process that allows spoofed activities to be accepted as valid. This issue has been fixed in version 2026.5.4.	N/A	More Details
CVE-2026-46712	Misskey is an open source, federated social media platform. Versions 2025.3.2 and later, but prior to 2026.5.4, contain a vulnerability where a lack of proper permission checks allows access to certain data points from the Direct Messages (formerly Chat) feature, regardless of account permissions. This vulnerability occurs whether or not federation is enabled. Notes created with "specified" visibility (formerly "direct" visibility) are not affected. This issue has been fixed in version 2026.5.4.	N/A	More Details
CVE-2026-65635	Improper Isolation or Compartmentalization vulnerability in malach-it boruta (Elixir.Boruta.Openid module) allows attackers to register OpenID Connect clients with administrative privileges through the dynamic client registration entry point. Boruta.Openid.register_client/3 forwards caller-supplied registration parameters to the administrative client creation path without a public/admin field-level allowlist, so an unauthenticated registrant can set security-sensitive attributes including supported grant types, authorized scopes, PKCE enforcement, public refresh and revocation behavior, token lifetimes, and signing settings. The library does not distinguish between metadata a public registrant is allowed to set and administrative controls that should require operator approval. This vulnerability is associated with program files lib/boruta/openid.ex and program routines 'Elixir.Boruta.Openid':register_client/3, 'Elixir.Boruta.Openid':parse_registration_params/2. This issue affects boruta from 2.3.0 before 2.3.7.	N/A	More Details
CVE-2026-59899	Netty is an asynchronous, event-driven network application framework. Prior to versions 4.1.136.Final and 4.2.16.Final, `HttpContentEncoder` (the superclass of the production handler `HttpContentCompressor`) maintains a per-channel `ArrayDeque<CharSequence>` named `acceptEncodingQueue` that accumulates attacker-controlled data without any size limit. The queue is filled on the I/O thread for every inbound HTTP request and drained only when the application later writes a non-1xx response. This creates a resource exhaustion vulnerability when an attacker exploits HTTP/1.1 pipelining to flood the connection with requests faster than the application produces responses. This issue has been fixed in versions 4.1.136.Final and 4.2.16.Final.	N/A	More Details
CVE-2026-59900	Netty is an asynchronous, event-driven network application framework. Prior to versions 4.1.136.Final and 4.2.16.Final, Netty's HTTP/2-to-HTTP/1.x translation layer (`Http2StreamFrameToHttpObjectCodec` and `InboundHttp2ToHttpAdapter`) fails to deduplicate or validate `Host` headers when an HTTP/2 client supplies both the `:authority` pseudo-header and a literal `host` header in a single HEADERS frame. The translator maps `:authority` to `Host` and separately copies the literal `host` header, producing an `HttpRequest` object containing two `Host` headers with attacker-controlled differing values. This issue has been fixed in versions 4.1.136.Final and 4.2.16.Final.	N/A	More Details
CVE-2026-69244	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.3, an out-of-bounds heap read could occur in the C response parser while building an error message for a malformed response. An attacker controlled server, or possibly an accidental response, could trigger a DoS in the client. The vulnerable path was error message construction in aiohttp/_http_parser.pyx, where an llhttp error-position pointer was used to build a snippet for malformed chunked responses and malformed request or response bytes at the buffer end. This issue is fixed in version 3.14.3.	N/A	More Details
CVE-2026-69243	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.2, the HTTP parsers were vulnerable to a request smuggling attack relating to WebSocket upgrades. If using the server-side component, an attacker may be able to execute a request smuggling vulnerability using an edge case in the WebSocket upgrade procedure. A WebSocket upgrade request with a body could cause the parser to switch protocols before the complete request body was received, leaving trailing bytes to be handled as upgraded-protocol or pipelined data rather than normal HTTP body data. This issue is fixed in version 3.14.2.	N/A	More Details
CVE-2026-67976	The Ref::SignalGen component of fprime framework v4.2.2 does not validate the safety of user-controlled parameters, allowing attackers to cause a Denial of Service (DoS) via inputting unsafe parameters.	N/A	More Details
CVE-2026-67972	An issue in the CF_CFDP_RecvMd() component of NASA cFS v7.0.1 allows attackers to contrl where received content and data is stored, possibly leading to an information disclosure.	N/A	More Details

CVE-2026-66065	Ouroboros is a local-first runtime for AI coding agents that records their actions and applies user-defined policies to constrain behavior. Versions prior to 0.42.1 have an incomplete denylist. Several execution-routing keys of the same RCE class were omitted, so a malicious cloned repo can still reach arbitrary command execution by shipping a .env (auto-loaded at import, with no review step). The CVE-2026-47211 fix added _UNTRUSTED_ENV_DENYLIST to stop an untrusted project-directory .env from redirecting execution, but it did not account for all keys. The backend config-home and MCP/plugin roots bypass the approval gate by pointing the nested agent, MCP servers, and plugin roster at attacker config. Other variables re-enable blocked local transports, replace sub-agent prompts, switch backends, and lower tool approval classes, further weakening the approval gate. This issue has been fixed in version 0.42.1.	N/A	More Details
CVE-2026-52521	A SQL injection vulnerability in Z-BlogPHP 1.7.5 allows authenticated attackers to execute arbitrary SQL commands via the id parameter in the CommentBat feature.	N/A	More Details
CVE-2026-52520	Emlog CMS <= 2.6.14 contains a stored cross-site scripting (XSS) vulnerability in the article publishing module (/admin/article.php). A remote authenticated attacker can inject arbitrary JavaScript code via the article content. When an administrator reviews or previews the submitted article in the backend, the malicious script executes in the admin's browser session, allowing the attacker to perform administrative actions such as creating a backdoor administrator account.	N/A	More Details
CVE-2026-52102	An OS command injection vulnerability in the openmediavault-md plugin of OpenMediaVault v8.0.4-1 allows attackers to execute arbitrary commands as root via injecting shell metacharacters.	N/A	More Details
CVE-2026-51775	SQL injection vulnerability in Fastadmin v.1.6.1.20250430 allows an attacker to exectue arbitrary code via the application/common/controller/Backend.php component	N/A	More Details
CVE-2026-51190	The "s init" command in Serverless-Devs @serverless-devs/s <= 3.1.11 passes unsanitized user input to child_process.spawn() with shell: true. A URL ending in ".git" bypasses the only input check, allowing OS command injection when a user runs "s init" with an attacker-controlled argument.	N/A	More Details
CVE-2026-6540	Calico's Application Layer Policy (disabled by default), which enforces HTTP rules through Dikastes, fails to perform URL path normalization. As a result, HTTP requests using path-traversal segments, encoded slashes, or repeated slashes are not correctly evaluated by Prefix path rules. Dikastes authorizes the request under the permitted prefix while the downstream workload or a fronting proxy normalizes the path and serves the restricted endpoint. An attacker with network access and no special RBAC can potentially reach HTTP endpoints the policy was intended to restrict.	N/A	More Details
CVE-2026-48113	Chisel is a TCP/UDP tunnel, transported over HTTP and secured via SSH. In versions prior to 1.11.5, authenticated clients can bypass --authfile ACL restrictions and tunnel traffic to arbitrary destinations reachable from the server. The ACL is enforced only during the initial handshake against declared remotes, but never on subsequent SSH channels that carry actual traffic. A malicious client can authenticate with a permitted remote, then open channels to any host:port it wants. This issue has been fixed in version 1.11.5.	N/A	More Details
CVE-2026-48063	Baileys is a cocket-based TS/JavaScript API for WhatsApp Web. In versions prior to both 6.7.22 and 7.0.0-rc12, any Baileys session can be sent a malicious payload via the placeholderResendMessage and trigger a fake messages.upsert event with a fake message key and payload. This allows anyone to spoof messages. The same exploit also allows an attacker to corrupt the app state sync system by sending fake key shares, and also allows for history sync spoofing which also serves the same problem, injecting fake previous context or "on-demand" sync. This issue has been fixed in versions 6.7.22 and 7.0.0-rc12.	N/A	More Details
CVE-2026-59901	Netty is an asynchronous, event-driven network application framework. Prior to versions 4.1.136.Final and 4.2.16.Final, the `Bzip2Decoder` handler in Netty's compression codec pipeline is vulnerable to a denial-of-service attack through a malformed bzip2 stream that permanently captures the event-loop thread in an infinite loop. The vulnerability exists in the run-length encoding (RLE) state machine within [`Bzip2BlockDecompressor.read()`]. This issue has been fixed in versions 4.1.136.Final and 4.2.16.Final.	N/A	More Details
	An Improper Authorization vulnerability exists in Apache Superset allowing an authenticated user with permissions to update charts to modify dashboards they do not own. When updating a chart's		

CVE-2026-23981	properties via the REST API, a user can provide a list of dashboard IDs (dashboards) to associate the chart with. The validation logic in the UpdateChartCommand failed to verify that the user had write permissions for the target dashboards specified in the request body. This issue affects Apache Superset: before 6.0.0. Users are recommended to upgrade to version 6.0.0, which fixes the issue.	N/A	More Details
CVE-2026-23985	A Regular Expression Denial of Service (ReDoS) vulnerability exists in Apache Superset versions 1.5.0 through 5.0.0. The vulnerability is located in the sql_parse.py component, specifically within the SQL_REGEX used for parsing SQL statements in the sqlparse library integration. The affected regular expression contains overlapping disjunctions that share a common outer quantifier. An authenticated attacker can exploit this by sending a maliciously crafted input string (specifically a long sequence of backslashes or similar characters) to endpoints that process SQL queries This issue affects Apache Superset: before 6.0.0. Users are recommended to upgrade to version 6.0.0, which fixes the issue. Workarounds: ● WAF Rules: Implement Web Application Firewall (WAF) rules to detect and block requests containing excessively long sequences of backslashes or suspicious repeated patterns in the queries.extras.where parameter. ● Rate Limiting: Ensure strict rate limiting is applied to the /api/v1/chart/data endpoint to reduce the impact of potential attacks.	N/A	More Details
CVE-2026-69198	ip-address is a library for parsing and manipulating IPv4 and IPv6 addresses in JavaScript. From 10.1.1 until 10.2.2, every special-use classification method is built on isInSubnet, which short-circuits to false whenever the address's own subnet mask is shorter than the reference range's mask. That mask comes verbatim from the CIDR suffix on the parsed input, so appending a suffix such as /0 suppresses classification entirely: isLoopback(), isPrivate(), isLinkLocal(), isCGNAT(), isMulticast(), isUnspecified(), isBroadcast(), isULA(), and getType() all report an internal address as unremarkable, while correctForm() and address still return the real internal target. An application that builds a network trust-boundary decision on these checks, for example a filter intended to block Server-Side Request Forgery, or SSRF, may therefore treat an internal target as external and allow the request. The underlying bit comparison is correct, and mask(n) already returns the first n bits of the full parsed address independently of subnetMask; the defect is solely that the containment guard sits in the classification path. This issue is fixed in version 10.2.2.	N/A	More Details
CVE-2026-69192	ip-address is a library for parsing and manipulating IPv4 and IPv6 addresses in JavaScript. Prior to 10.3.1, Address4 accepts an octet written with a leading zero and decodes it as decimal, while the WHATWG URL host parser, inet_aton, and getaddrinfo all decode a leading zero as octal. The library and the network stack therefore disagree about which host a string names. new Address4('012.0.0.1') reports correctForm() of 12.0.0.1 and isPrivate() of false, but fetch('http://012.0.0.1/') connects to 10.0.0.1. An application that builds a network trust-boundary decision on these checks, for example a filter intended to block Server-Side Request Forgery, or SSRF, will classify an internal target as external and allow the request. The defect is in the parse gate rather than in any one classifier, so every consumer of Address4 inherits it: isPrivate(), isLoopback(), isLinkLocal(), isCGNAT(), isInSubnet(), isHostInSubnet(), and correctForm() are all computed from the mis-decoded octets. This issue is fixed in version 10.3.1.	N/A	More Details
CVE-2026-12935	The TL-WR940N v6 router contains a vulnerability in its RTSP connection tracking module that can lead to a stack-based buffer overflow. The issue occurs when a LAN client initiates a connection to a malicious RTSP server controlled by an attacker. A specially crafted RTSP message may trigger improper memory handling within the kernel module Successful exploitation of this vulnerability may result in a denial-of-service (DoS) condition or allow remote code execution (RCE), potentially leading to full compromise of the device. This vulnerability can be exploited by an unauthenticated attacker under the device's default configuration.	N/A	More Details
CVE-2026-68981	Apache NiFi 1.5.0 through 2.10.0 support gzip-encoded HTTP requests for the application REST API using a Jersey encoding filter. The framework enforced a configurable maximum request size on the compressed payload rather than the decompressed output, allowing a malicious client to send crafted requests that could consume excessive amounts of memory. Upgrading to Apache NiFi 2.11.0 is the recommended mitigation, which relocates response compression to Jetty Server and disables decompression of gzip-encoded HTTP requests.	N/A	More Details
CVE-2026-68980	Apache NiFi 2.0.0 through 2.10.0 support creating, reading, and deleting Assets associated with Parameter Contexts through the REST API. The framework authorizes asset deletion against the owning Parameter Context using the supplied Parameter Context Identifier and Asset Identifier. The framework performed authorized based on the supplied Parameter Context Identifier without verifying the requested Identifier against the stored Identifier. Apache NiFi installations that do not implement different levels of authorization across Parameter Contexts are not subject to this	N/A	More Details

	vulnerability, because the framework enforces write permissions as the security boundary. Upgrading to Apache NiFi 2.11.0 is the recommended mitigation, which verifies Parameter Context ownership of the requested Asset before deletion using the same strategy applied to Asset read operations.		
CVE-2026-68979	Apache NiFI 1.10.0 through 2.10.0 provide a Parameter Context update REST API method that does not enforce authorization checking on components referencing Parameter values. Updating a Parameter Context can change parameter values that affect referencing components, but framework authorization was limited to read and write privileges on the Parameter Context itself. As a result of the missing authorization, an authenticated user authorized to modify a Parameter Context, but not authorized on referencing components, could alter Parameter values affecting those components. In deployments where a Parameter value contains executable scripting content, updating a Parameter can result in code execution during automatic component validation, without starting the referencing component. The impact was limited to stopped components by existing verification checks, and the issue applies only to deployments that use component-level authorization policies. Upgrading to Apache NiFi 2.11.0 is the recommended mitigation, which aligns the Parameter Context update method authorization with other methods, adding authorization checking on affected components.	N/A	More Details
CVE-2026-13346	pip would incorrectly handle doubly-encoded package URLs from indexes allowing for files to be installed to arbitrary locations on disk even when installing wheels. This vulnerability requires downloading or installing a package from a malicious package index to succeed, malicious packages alone are not able to exploit this vulnerability. Note that this vulnerability only materially impacts users running `pip download` with the `--only-binary` option as installing source distributions from an untrusted index is already an unsafe operation that executes code during install time.	N/A	More Details
CVE-2026-66296	Improper Neutralization of Input During Web Page Generation (XSS) vulnerability in lud oaskit allows reflected cross-site scripting via the default HTML error handler. Oaskit.ErrorHandler.Default.format_reason/4 and Oaskit.ErrorHandler.Default.reason_to_html/1 in lib/oaskit/error_handler/default.ex render request-validation failures as an HTML page whenever the request's Accept header contains html, interpolating request-controlled strings into that page without HTML escaping. The unescaped values are object keys taken from a request body or from an object or deepObject query parameter, which appear in the JSON Schema error's instance path when a schema rejects them (for example under additionalProperties: false), and the raw Content-Type header, reflected in unsupported-media-type errors when it fails to parse. Because browsers send Accept: text/html on ordinary top-level navigation, a crafted GET link is sufficient to trigger the error page; no form submission, custom Content-Type, or attacker-controlled script on the victim's side is required. A payload such as filter[</code></h2><script>alert(document.domain)</script>]=x terminates the enclosing markup and the injected script executes in the origin of the application using oaskit, giving it access to that origin's cookies, session, and same-origin responses. Both HTML error rendering and the vulnerable handler are enabled by default: Oaskit.Plugs.ValidateRequest defaults :html_errors to true and :error_handler to Oaskit.ErrorHandler.Default, so applications following the documented usage are affected without any opt-in. This issue affects oaskit: from 0.1.0 before 0.14.1.	N/A	More Details
CVE-2026-67436	Linuxfabrik monitoring-plugins provides Python monitoring plugins for Icinga, Nagios, and related monitoring systems. In 6.0.0 and earlier, the redfish-* plugins built request URLs by concatenating an operator-supplied base URL with response-supplied @odata.id links, allowing a malicious or compromised BMC to redirect authenticated Redfish requests and disclose X-Auth-Token or HTTP Basic credentials.	N/A	More Details
CVE-2026-12996	A use-after-free in OpenVPN 2.6.0 through 2.6.20 and 2.7_alpha1 through 2.7.4 allows remote authenticated peers to potentially cause a denial of service or leak memory via crafted packets during TLS session promotion or expiry	N/A	More Details
CVE-2026-59640	In Bouncy Castle for Java before 1.85, OpenPGP CFB quick-check oracle active on symmetric/session-key paths. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bcpg-fips 1.0.13 (1.0.X series), 2.0.13 (2.0.X series) and 2.1.13 (2.1.X series).	N/A	More Details
CVE-2026-66756	Improper Protection of Alternate Path vulnerability in Apache Tika. This issue affects Apache Tika: from 4.0.0-alpha-1 before 4.0.0-beta-1. Users are recommended to upgrade to version 4.0.0-beta-1, which fixes the issue.	N/A	More Details
CVE-			

2026-12816	In Bouncy Castle for Java before 1.85, IESEngine stream-mode MAC forgery via length-dependent KDF split. This issue also affects Bouncy Castle for Java LTS before 2.73.12.	N/A	More Details
CVE-2026-12803	In Bouncy Castle for Java before 1.85, KCCMBlockCipher MAC does not bind nonce when AAD is absent (cross-nonce AEAD forgery). This issue also affects Bouncy Castle for Java LTS before 2.73.12.	N/A	More Details
CVE-2026-12802	In Bouncy Castle for Java before 1.85, CMS AuthEnvelopedData fails to enforce tag-length on decryption. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bcpkix-fips 1.0.12 (1.0.X series), 2.0.12 (2.0.X series) and 2.1.12 (2.1.X series).	N/A	More Details
CVE-2026-58063	In Bouncy Castle for Java before 1.85, BCFKS keystore load honours unbounded KDF cost from untrusted file. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bc-fips 1.0.2.7 (1.0.X series), 2.0.2 (2.0.X series) and 2.1.3 (2.1.X series).	N/A	More Details
CVE-2026-58062	In Bouncy Castle for Java before 1.85, Stapled OCSP response accepted without binding to the checked certificate. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bc-fips 2.0.2 (2.0.X series) and 2.1.3 (2.1.X series).	N/A	More Details
CVE-2026-58061	In Bouncy Castle for Java before 1.85, CCM-family modes write plaintext to caller buffer before tag check. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bc-fips 1.0.2.7 (1.0.X series), 2.0.2 (2.0.X series) and 2.1.3 (2.1.X series).	N/A	More Details
CVE-2026-58060	In Bouncy Castle for Java before 1.85, HSS public-key level count unbounded, enabling huge allocation on verify. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bc-fips 2.0.2 (2.0.X series) and 2.1.3 (2.1.X series).	N/A	More Details
CVE-2026-58059	In Bouncy Castle for Java before 1.85, Quadratic-time escaping when stringifying X.500 distinguished names. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bc-fips 1.0.2.7 (1.0.X series), 2.0.2 (2.0.X series) and 2.1.3 (2.1.X series).	N/A	More Details
CVE-2026-48499	Activepieces is an open source AI workflow automation platform. Prior to 0.84.0, an unsanitized path segment in the Code piece sandbox can let an authenticated flow author reach read-write cached flow and code files belonging to other tenants on the same worker, exposing embedded data and allowing modified code to execute on a victim tenant's next flow run. This issue is fixed in version 0.84.0.	N/A	More Details
CVE-2026-51272	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-59881	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.2, the WebSocket client accepts and decompresses frames with the RSV1 bit set even when the permessage-deflate extension was not negotiated, allowing a malicious server to cause unexpected CPU and memory consumption. This issue is fixed in version 3.14.2.	N/A	More Details
CVE-2026-64870	MaxKB is an open-source AI assistant for enterprise. In versions 2.0.0 through 2.10.4-lts, UpdateStoreTool.update_tool passes caller-supplied download_url and download_callback_url values to requests.get without equivalent trusted-host and redirect validation, allowing an authenticated workspace user to make the server request internal, loopback, link-local, or cloud metadata URLs. A fix is present on the v2 branch but has not yet been included in a published release.	N/A	More Details
CVE-2026-66066	Action Pack is a framework for handling and responding to web requests. In versions prior to 7.2.3.2, 8.0.5.1 and 8.1.3.1, Active Storage does not disable libvips operations marked unsafe for untrusted content, allowing a crafted upload to invoke such an operation. Consuming applications are affected when configured to use libvips and accept image uploads from untrusted users. An unauthenticated attacker may exploit this behavior to read arbitrary files accessible to the Rails process, including environment variables and application secrets. Exposure of credentials such as secret_key_base or external-service tokens may enable remote code execution or lateral movement. This issue has been fixed in versions 7.2.3.2, 8.0.5.1 and 8.1.3.1.	N/A	More Details
	Relative Path Traversal in the ISA-Tab parser in Apache Software Foundation Apache Tika from 1.8		

CVE-2026-66755	through 3.3.1, and 4.0.0-alpha-1, allows an attacker who can place files in a directory that the application subsequently parses to read arbitrary files accessible to the Tika process and have their contents emitted into the extracted text output, via a "Study Assay File Name" value in the ISA-Tab investigation file that traverses outside the dataset directory. Users are recommended to upgrade to version 3.3.2 or 4.0.0-beta-1, which fixes this issue.	N/A	More Details
CVE-2026-54715	GoAccess is a real-time web log analyzer and interactive viewer that runs in a terminal in *nix systems or through the browser. In version 1.10.2, parse_browser assumes the matched browser token begins with Opera and moves a trailing version substring to match plus five, allowing a crafted User-Agent in a processed access log to write one to four attacker-influenced bytes beyond the heap allocation and corrupt or crash GoAccess. This issue is fixed in version 1.11.	N/A	More Details
CVE-2026-13305	Autel MaxiCharger AC Elite Home Software Update Improper Verification of Cryptographic Signature Arbitrary Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Autel MaxiCharger AC Elite Home EV chargers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of software updates. The issue results from the lack of proper validation of a user-supplied software update image. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-29062.	N/A	More Details
CVE-2026-8763	In Bouncy Castle for Java before 1.85, Name Constraints bypass via trailing dot in rfc822Name and URI. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bc-fips 1.0.2.7 (1.0.X series), 2.0.2 (2.0.X series) and 2.1.3 (2.1.X series).	N/A	More Details
CVE-2026-55768	GoAccess is a real-time web log analyzer and interactive viewer that runs in a terminal in *nix systems or through the browser. Prior to version 1.11, the built-in WebSocket server narrows a 64-bit extended frame length into the signed 32-bit WSFrame.payloadlen field before enforcing the maximum frame size, allowing an unauthenticated remote client to bypass the guard and force an approximately 18-exabyte allocation request that terminates the process. This issue is fixed in version 1.11.	N/A	More Details
CVE-2026-59652	In Bouncy Castle for Java before 1.85, LDAP filter injection in legacy jdk1.4 LDAPStoreHelper.	N/A	More Details
CVE-2026-59651	In Bouncy Castle for Java before 1.85, BKS keystore accepts legacy version with 16-bit integrity MAC key. This issue also affects Bouncy Castle for Java LTS before 2.73.12.	N/A	More Details
CVE-2026-59650	In Bouncy Castle for Java before 1.85, MTI/A0 DH agreement exponentiates unvalidated peer value. This issue also affects Bouncy Castle for Java LTS before 2.73.12.	N/A	More Details
CVE-2026-59649	In Bouncy Castle for Java before 1.85, OpenPGP user-attribute subpacket length bounded only by JVM max memory. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bcpg-fips 1.0.13 (1.0.X series), 2.0.13 (2.0.X series) and 2.1.13 (2.1.X series).	N/A	More Details
CVE-2026-59648	In Bouncy Castle for Java before 1.85, OpenPGP Argon2 S2K honours attacker-chosen memory and passes. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bcpg-fips 1.0.13 (1.0.X series), 2.0.13 (2.0.X series) and 2.1.13 (2.1.X series).	N/A	More Details
CVE-2026-59647	In Bouncy Castle for Java before 1.85, CRMF/CMP password-MAC honours unbounded iteration count. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bcpkix-fips 1.0.12 (1.0.X series), 2.0.12 (2.0.X series) and 2.1.12 (2.1.X series).	N/A	More Details
CVE-2026-59646	In Bouncy Castle for Java before 1.85, DTLS handshake reassembler allocates buffer from unchecked 24-bit length. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bctls-fips 1.0.24 (1.0.X series), 2.0.24 (2.0.X series) and 2.1.24 (2.1.X series).	N/A	More Details
CVE-2026-59645	In Bouncy Castle for Java before 1.85, OER parser recurses without depth limit on self-referential IEEE 1609.2 schema. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bcutil-fips 2.0.7 (2.0.X series) and 2.1.7 (2.1.X series).	N/A	More Details

CVE-2026-59644	In Bouncy Castle for Java before 1.85, MLS hash-ratchet honours arbitrary 32-bit generation counter from sender.	N/A	More Details
CVE-2026-59643	In Bouncy Castle for Java before 1.85, OpenPGP inline-signature policy failures silently ignored. This issue also affects Bouncy Castle for Java FIPS (BC-FJA) before bcpg-fips 2.0.13.	N/A	More Details
CVE-2026-59642	In Bouncy Castle for Java before 1.85, CMS AuthenticatedData content not bound to MAC when authAttrs present. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bcpkix-fips 1.0.12 (1.0.X series), 2.0.12 (2.0.X series) and 2.1.12 (2.1.X series).	N/A	More Details
CVE-2026-59641	In Bouncy Castle for Java before 1.85, S/MIME validator trusts signer-asserted signingTime for path validation. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bcmail-fips and bcjmail-fips 1.0.7 (1.0.X series), 2.0.7 (2.0.X series) and 2.1.7 (2.1.X series).	N/A	More Details
CVE-2026-12817	In Bouncy Castle for Java before 1.85, OpenPGP AEAD decryption skips final tag on chunk-aligned data. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bcpg-fips 1.0.13 (1.0.X series), 2.0.13 (2.0.X series) and 2.1.13 (2.1.X series).	N/A	More Details
CVE-2026-12852	In Bouncy Castle for Java before 1.85, MLS wire decoder allocates attacker-declared opaque length before bounds check.	N/A	More Details
CVE-2026-12860	In Bouncy Castle for Java before 1.85, RSA PKCS#1 verification skips last two hash bytes in NULL-omitted path. This issue also affects Bouncy Castle for Java LTS before 2.73.12.	N/A	More Details
CVE-2026-13506	In Bouncy Castle for Java before 1.85, Lazy ASN.1 sequence forcing resets nesting-depth guard. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bc-fips 1.0.2.7 (1.0.X series), 2.0.2 (2.0.X series) and 2.1.3 (2.1.X series).	N/A	More Details
CVE-2026-13117	An incomplete guard in OpenVPN 2.6.0 through 2.6.20 and 2.7_alpha1 through 2.7.4 allows remote authenticated peers to trigger a use-after-free during TLS session promotion, potentially leading to a denial of service or memory leakage	N/A	More Details
CVE-2026-13306	Autel MaxiCharger AC Elite Home USB Authentication Bypass Vulnerability. This vulnerability allows physically present attackers to bypass authentication on affected installations of Autel MaxiCharger AC Elite Home EV chargers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the exposed USB interface. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-29046.	N/A	More Details
CVE-2026-13307	Autel MaxiCharger AC Elite Home USB Heap-based Buffer Overflow Arbitrary Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Autel MaxiCharger AC Elite Home EV chargers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of custom USB packets. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length, heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-29048.	N/A	More Details
CVE-2026-13308	Autel MaxiCharger AC Elite Home WebSockets Integer Underflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Autel MaxiCharger AC Elite Home EV chargers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of WebSocket messages related to the OCPP service. The issue results from the lack of proper validation of user-supplied data, which can result in an integer underflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-29113.	N/A	More Details
CVE-2026-13309	Autel MaxiCharger AC Elite Home NFC Stack-based Buffer Overflow Arbitrary Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Autel MaxiCharger AC Elite Home EV chargers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of card responses via the NFC interface. A crafted card response can trigger an overflow of a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the	N/A	More Details

	device. Was ZDI-CAN-29044.		
CVE-2026-13379	The Windows interactive service in OpenVPN 2.7_alpha1 through 2.7.4 allows remote attackers to cause persistent DNS state pollution or a service crash via a crafted search domain during the disconnection process	N/A	More Details
CVE-2026-51290	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-18574	An authentication bypass vulnerability in Check Point Security Management Server and Multi-Domain Security Management Server (MDS) could allow an unauthenticated remote attacker with network access to Management services to execute arbitrary commands on the Security Management Server. Successful exploitation could result in full compromise of the Security Management system. Check Point discovered this issue internally and has no indication of active exploitation.	N/A	More Details
CVE-2026-69082	CTI-Transmute contained a cross-site request forgery vulnerability in the administrative user deletion functionality. The /account/delete/<id> endpoint accepted HTTP GET requests for an operation that modified application state. An unauthenticated remote attacker could construct a malicious link or embed a request targeting this endpoint and induce an authenticated CTI-Transmute administrator to visit the attacker-controlled content. If the administrator had an active session, the browser would automatically include the administrator’s session credentials, causing the selected user account to be deleted without the administrator intentionally confirming the operation. Successful exploitation requires interaction from a currently authenticated administrator who has permission to delete users. The attacker does not need a CTI-Transmute account or administrative privileges because the forged request executes using the victim administrator’s session. The vulnerability could allow an attacker to delete arbitrary user accounts, resulting in unauthorized modification of application state and denial of access for affected users. Depending on whether administrators can delete other administrators or the final administrative account, exploitation could also disrupt administration of the CTI-Transmute instance. The patch resolves the issue by restricting the deletion endpoint to HTTP POST requests and submitting the deletion through a form containing a CSRF token.	N/A	More Details
CVE-2026-69079	CTI-Transmute contains an uncontrolled resource-consumption vulnerability in the unauthenticated /activity_timeline endpoint. The endpoint accepts a user-controlled days query parameter that was not restricted to a reasonable range. A remote, unauthenticated attacker could submit an excessively large value for this parameter, causing the application to retrieve and process activity data over an arbitrarily large period. This could consume excessive database, CPU, or memory resources, delay the processing of concurrent requests, or trigger an internal server error. Repeated requests could further degrade the availability of the CTI-Transmute website. The vulnerability is corrected by clamping the requested timeline range to a minimum of one day and a maximum of 1,095 days.	N/A	More Details
CVE-2026-69078	CTI-Transmute is affected by a server-side request forgery vulnerability in the evaluation report PDF-generation functionality. User-controlled CTI content, including conversion names, descriptions, and comments, is converted from Markdown to HTML and rendered as a PDF using WeasyPrint. Before the patch, the renderer used WeasyPrint’s default URL-fetching behavior without restricting the protocols or destinations that could be referenced by the generated HTML. An attacker able to supply content included in an evaluation report could inject crafted resource references using schemes such as http://, https://, or file://. When the report was rendered, CTI-Transmute could fetch these resources using the application server’s network connectivity and filesystem privileges. Successful exploitation could allow an attacker to: * access services available only from the CTI-Transmute server or its internal network; * probe internal hosts and service endpoints; * retrieve local files readable by the application process; and * expose fetched content through the generated PDF, depending on the referenced resource type and rendering context. The vulnerability is corrected by providing WeasyPrint with a restrictive URL fetcher that permits only self-contained data: URIs. The externally hosted Google Fonts stylesheet was also removed so that PDF generation performs no intentional network or filesystem fetches.	N/A	More Details
CVE-2026-51291	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-	A vulnerability in Wapt Server before version 2.6.1.17813 allows a remote unauthenticated attacker to bypass security restriction using a specially crafted packet and retrieve a valid session	N/A	More

33591	token for the targeted account.		Details
CVE-2026-0392	eParakstītājs 3.0 for Windows before version 1.10.0 retrieves and executes its automatic updates over a channel that is not authenticated or integrity-protected. On each launch the application fetches an update descriptor (XML) over TLS but accepts any TLS certificate (a permissive TrustManager and a HostnameVerifier that always returns true), does not verify any digital signature on the update descriptor, and does not verify the Authenticode signature or a checksum of the downloaded installer before running it. A man-in-the-middle attacker able to redirect www.eparaksts.lv can serve a crafted update descriptor pointing to an attacker-controlled executable, which the client downloads and executes, resulting in arbitrary code execution on the victim host.	N/A	More Details
CVE-2026-69075	FlowIntel is affected by a stored cross-site scripting vulnerability through multiple user-controlled or administrator-controlled fields. Persisted values—including case titles, ticket identifiers, recurring-case information, user profile attributes, organisation names, and role names—were rendered inside DOM elements subsequently compiled by Vue. Although normal HTML escaping could neutralize direct HTML markup, it did not prevent an attacker from injecting Vue interpolation expressions using the configured [[...]] delimiters. An authenticated attacker able to modify one of the affected fields could store a malicious Vue expression. When another user viewed an affected case, report, profile, recurring-case page, or navigation component, Vue could evaluate the injected expression in the context of the FlowIntel application. Successful exploitation could allow arbitrary JavaScript execution in the victim's browser under the FlowIntel origin. This could expose information available to the victim, perform actions using the victim's authenticated session, or modify application data within the victim's privileges. The patch introduces a dedicated vue_escape filter that escapes HTML-sensitive characters and breaks Vue interpolation delimiters before the values are rendered. The filter is applied to the affected case, account, organisation, role, configuration, and navigation fields.	N/A	More Details
CVE-2026-8794	PaperCut NG/MF contains an observable timing discrepancy in its authentication component. An unauthenticated remote attacker can exploit this vulnerability to perform username enumeration by measuring response times during login attempts. The system executes a password hash comparison only when a valid account is supplied, creating a measurable timing oracle that reveals account existence.	N/A	More Details
CVE-2026-8793	PaperCut NG/MF does not properly restrict excessive authentication attempts within its login component. An unauthenticated remote attacker can exploit this vulnerability to perform unrestricted brute-force or credential-stuffing attacks without triggering account lockout or rate-limiting mechanisms in some configurations.	N/A	More Details
CVE-2026-51292	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-18060	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-51234	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51293	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-51294	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-12259	In nltk version 3.9.4, the `nltk.downloader.Downloader._download_package()` function writes downloaded package bytes to disk and may extract them before enforcing SHA-256 or MD5 checksum validation. This allows an attacker to tamper with the package response body for `info.url` through a compromised mirror, malicious proxy, or other source-substitution condition, leading to the installation of attacker-controlled package bytes. The vulnerability can result in malicious corpus or model content being trusted by downstream users or applications.	N/A	More Details

CVE-2026-51295	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-54522	MessagePack for Ruby is an implementation of the MessagePack binary serialization format. Prior to 1.8.2, MessagePack::Buffer#clear in ext/msgpack/buffer.c leaves rmem_last, rmem_end, and rmem_owner stale after _msgpack_buffer_shift_chunk returns an rmem page to the shared pool, allowing a subsequent Buffer#write and a second MessagePack::Buffer to alias the page and disclose or corrupt cross-buffer data. This issue is fixed in version 1.8.2.	N/A	More Details
CVE-2026-54722	DSSRF is a Node.js library that provides a wide range of utilities and advanced SSRF defense checks. Prior to 1.0.4, is_url_safe in src/helpers.ts strips the @ userinfo delimiter with remove_at_symbol_in_string before new URL parses the URL, allowing an attacker-controlled URL to bypass internal-IP validation and cause a client using the original URL to reach an internal service. This issue is fixed in version 1.0.4.	N/A	More Details
CVE-2026-12872	The Webinfos WordPress plugin through 1.2 does not validate the type or name of uploaded files, nor restrict the upload action with any authentication, capability, or nonce check, allowing unauthenticated attackers to upload arbitrary files (including PHP) to a web-accessible directory, leading to remote code execution on servers that execute PHP from the uploads path.	N/A	More Details
CVE-2026-14682	In Bouncy Castle for Java before 1.85, Possible OOM from unbounded up-front allocation on a definite-length read. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bc-fips 1.0.2.7 (1.0.X series), 2.0.2 (2.0.X series) and 2.1.3 (2.1.X series), and before bctls-fips 1.0.24.	N/A	More Details
CVE-2026-13586	In Bouncy Castle for Java before 1.85, PKCS#12 MAC and bag-decryption KDF iteration-count bound (DoS). This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bc-fips 1.0.2.7 (1.0.X series), 2.0.2 (2.0.X series) and 2.1.3 (2.1.X series).	N/A	More Details
CVE-2026-16339	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details