SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 01 April 2026

Generated on 01 April 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-2026-30302	The command auto-approval module in CodeRider-Kilo contains an OS Command Injection vulnerability, rendering its whitelist security mechanism ineffective. The vulnerability stems from the incorrect use of an incompatible command parser (the Unix-based shell-quote library) to analyze commands on the Windows platform, coupled with a failure to correctly handle Windows CMD-specific escape sequences (^). Attackers can exploit this discrepancy between the parsing logic and the execution environment by constructing payloads such as git log ^" & malicious_command ^". The CodeRider-Kilo parser is deceived by the escape characters, misinterpreting the malicious command connector (&) as being within a protected string argument and thus auto-approving the command. However, the underlying Windows CMD interpreter ignores the escaped quotes, parsing and executing the subsequent malicious command directly. This allows attackers to achieve arbitrary Remote Code Execution (RCE) after bypassing what appears to be a legitimate Git whitelist check.	10.0	More Details
CVE-2026-33494	ORY Oathkeeper is an Identity & Access Proxy (IAP) and Access Control Decision API that authorizes HTTP requests based on sets of Access Rules. Versions prior to 26.2.0 are vulnerable to an authorization bypass via HTTP path traversal. An attacker can craft a URL containing path traversal sequences (e.g. `/public/../admin/secrets`) that resolves to a protected path after normalization, but is matched against a permissive rule because the raw, un-normalized path is used during rule evaluation. Version 26.2.0 contains a patch.	10.0	More Details
CVE-2026-34162	FastGPT is an AI Agent building platform. Prior to version 4.14.9.5, the FastGPT HTTP tools testing endpoint (/api/core/app/httpTools/runTool) is exposed without any authentication. This endpoint acts as a full HTTP proxy — it accepts a user-supplied baseUrl, toolPath, HTTP method, custom headers, and body, then makes a server-side HTTP request and returns the complete response to the caller. This issue has been patched in version 4.14.9.5.	10.0	More Details
CVE-2026-32536	Unrestricted Upload of File with Dangerous Type vulnerability in halfdata Green Downloads halfdata-paypal-green-downloads allows Using Malicious Files.This issue affects Green Downloads: from n/a through <= 2.08.	9.9	More Details
CVE-2026-32525	Improper Control of Generation of Code ('Code Injection') vulnerability in jetmonsters JetFormBuilder jetformbuilder allows Code Injection.This issue affects JetFormBuilder: from n/a through <= 3.5.6.1.	9.9	More Details
CVE-2026-32523	Unrestricted Upload of File with Dangerous Type vulnerability in denishua WPJAM Basic wpjam-basic allows Using Malicious Files.This issue affects WPJAM Basic: from n/a through <= 6.9.2.	9.9	More Details
CVE-2026-33396	OneUptime is an open-source monitoring and observability platform. Prior to version 10.0.35, a low-privileged authenticated user (ProjectMember) can achieve remote command execution on the Probe container/host by abusing Synthetic Monitor Playwright script execution. Synthetic monitor code is executed in VMRunner.runCodeInNodeVM with a live Playwright page object in context. The sandbox relies on a denylist of blocked properties/methods, but it is incomplete. Specifically, _browserType and launchServer are not blocked, so attacker code can traverse `page.context().browser()._browserType.launchServer(...)` and spawn arbitrary processes. Version 10.0.35 contains a patch.	9.9	More Details
CVE-2026-32482	Unrestricted Upload of File with Dangerous Type vulnerability in deothemes Ona ona allows Upload a Web Shell to a Web Server.This issue affects Ona: from n/a through < 1.24.	9.9	More Details
CVE-2026-33897	Incus is a system container and virtual machine manager. Prior to version 6.23.0, instance template files can be used to cause arbitrary read or writes as root on the host server. Incus allows for pongo2 templates within instances which can be used at various times in the instance lifecycle to template files inside of the instance. This particular implementation of pongo2 within Incus allowed for file read/write but with the expectation that the pongo2 chroot feature would isolate all such access to the instance's filesystem. This was allowed such that a template could theoretically read a file and then generate a new version of said file. Unfortunately the chroot isolation mechanism is entirely skipped by pongo2 leading to easy access to the entire system's filesystem with root privileges. Version 6.23.0 patches the issue.	9.9	More Details
CVE-2026-27044	Improper Control of Generation of Code ('Code Injection') vulnerability in TotalSuite Total Poll Lite totalpoll-lite allows Remote Code Inclusion.This issue affects Total Poll Lite: from n/a through <= 4.12.0.	9.9	More Details

CVE-2026-33945	Incus is a system container and virtual machine manager. Incus instances have an option to provide credentials to systemd in the guest. For containers, this is handled through a shared directory. Prior to version 6.23.0, an attacker can set a configuration key named something like `systemd.credential.../../../../../root/.bashrc` to cause Incus to write outside of the `credentials` directory associated with the container. This makes use of the fact that the Incus syntax for such credentials is `systemd.credential.XYZ` where `XYZ` can itself contain more periods. While it's not possible to read any data this way, it's possible to write to arbitrary files as root, enabling both privilege escalation and denial of service attacks. Version 6.23.0 fixes the issue.	9.9	More Details
CVE-2026-25413	Unrestricted Upload of File with Dangerous Type vulnerability in iqonicdesign WPBookit Pro wpbookit-pro allows Using Malicious Files.This issue affects WPBookit Pro: from n/a through <= 1.6.18.	9.9	More Details
CVE-2026-34156	NocoBase is an AI-powered no-code/low-code platform for building business applications and enterprise solutions. Prior to version 2.0.28, NocoBase's Workflow Script Node executes user-supplied JavaScript inside a Node.js vm sandbox with a custom require allowlist (controlled by WORKFLOW_SCRIPT_MODULES env var). However, the console object passed into the sandbox context exposes host-realm WritableWorkerStdio stream objects via console._stdout and console._stderr. An authenticated attacker can traverse the prototype chain to escape the sandbox and achieve Remote Code Execution as root. This issue has been patched in version 2.0.28.	9.9	More Details
CVE-2026-25345	Improper Validation of Specified Quantity in Input vulnerability in GalleryCreator SimpLy Gallery simply-gallery-block allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects SimpLy Gallery: from n/a through <= 3.3.2.	9.9	More Details
CVE-2026-25366	Improper Control of Generation of Code ('Code Injection') vulnerability in Themeisle Woody ad snippets insert-php allows Code Injection.This issue affects Woody ad snippets: from n/a through <= 2.7.1.	9.9	More Details
CVE-2026-32922	OpenClaw before 2026.3.11 contains a privilege escalation vulnerability in device.token.rotate that allows callers with operator.pairing scope to mint tokens with broader scopes by failing to constrain newly minted scopes to the caller's current scope set. Attackers can obtain operator.admin tokens for paired devices and achieve remote code execution on connected nodes via system.run or gain unauthorized gateway-admin access.	9.9	More Details
CVE-2026-30532	A SQL Injection vulnerability exists in SourceCodester Online Food Ordering System v1.0 in the admin/view_product.php file via the "id" parameter.	9.8	More Details
CVE-2026-33669	SiYuan is a personal knowledge management system. Prior to version 3.6.2, document IDs were retrieved via the /api/file/readDir interface, and then the /api/block/getChildBlocks interface was used to view the content of all documents. Version 3.6.2 patches the issue.	9.8	More Details
CVE-2026-32975	OpenClaw before 2026.3.12 contains a weak authorization vulnerability in Zalouser allowlist mode that matches mutable group display names instead of stable group identifiers. Attackers can create groups with identical names to allowlisted groups to bypass channel authorization and route messages from unintended groups to the agent.	9.8	More Details
CVE-2026-32987	OpenClaw before 2026.3.13 allows bootstrap setup codes to be replayed during device pairing verification in src/infra/device-bootstrap.ts. Attackers can verify a valid bootstrap code multiple times before approval to escalate pending pairing scopes, including privilege escalation to operator.admin.	9.8	More Details
CVE-2026-30457	An issue in the /parser/dwoo component of Daylight Studio FuelCMS v1.5.2 allows attackers to execute arbitrary code via crafted PHP code.	9.8	More Details
CVE-2017-20229	MAWK 1.3.3-17 and prior contains a stack-based buffer overflow vulnerability that allows attackers to execute arbitrary code by exploiting inadequate boundary checks on user-supplied input. Attackers can craft malicious input that overflows the stack buffer and execute a return-oriented programming chain to spawn a shell with application privileges.	9.8	More Details
CVE-2018-25220	Bochs 2.6-5 contains a stack-based buffer overflow vulnerability that allows attackers to execute arbitrary code by supplying an oversized input string to the application. Attackers can craft a malicious payload with 1200 bytes of padding followed by a return-oriented programming chain to overwrite the instruction pointer and execute shell commands with application privileges.	9.8	More Details
CVE-2026-0558	A vulnerability in parisneo/lollms, up to and including version 2.2.0, allows unauthenticated users to upload and process files through the `/api/files/extract-text` endpoint. This endpoint does not enforce authentication, unlike other file-related endpoints, and lacks the `Depends(get_current_active_user)` dependency. This issue can lead to denial of service (DoS) through resource exhaustion, information disclosure, and violation of the application's documented security policies.	9.8	More Details
CVE-2026-4176	Perl versions from 5.9.4 before 5.40.4-RC1, from 5.41.0 before 5.42.2-RC1, from 5.43.0 before 5.43.9 contain a vulnerable version of Compress::Raw::Zlib. Compress::Raw::Zlib is included in the Perl package as a dual-life core module, and is vulnerable to CVE-2026-3381 due to a vendored version of zlib which has several vulnerabilities, including CVE-2026-27171. The bundled Compress::Raw::Zlib was updated to version 2.221 in Perl blead commit c75ae9cc164205e1b6d6dbd57bd2c65c8593fe94.	9.8	More Details
CVE-2018-25221	EChat Server 3.1 contains a buffer overflow vulnerability in the chat.ghp endpoint that allows remote attackers to execute arbitrary code by supplying an oversized username parameter. Attackers can send a GET request to chat.ghp with a malicious username value containing shellcode and ROP gadgets to achieve code execution in the application context.	9.8	More Details
CVE-2026-4809	plank/laravel-mediable through version 6.4.0 can allow upload of a dangerous file type when an application using the package accepts or prefers a client-supplied MIME type during file upload handling. In that configuration, a remote attacker can submit a file containing executable PHP code while declaring a benign image MIME type, resulting in arbitrary file upload. If the uploaded file is stored in a web-accessible and executable location, this may lead to remote code execution. At the time of publication, no patch was available and the vendor had not responded to coordinated disclosure attempts.	9.8	More Details
CVE-2014-125112	Plack::Middleware::Session::Cookie versions through 0.21 for Perl allows remote code execution. Plack::Middleware::Session::Cookie versions through 0.21 has a security vulnerability where it allows an attacker to execute arbitrary code on the server during deserialization of the cookie data, when there is no secret used to sign the cookie.	9.8	More Details
CVE-2018-25223	Crashmail 1.6 contains a stack-based buffer overflow vulnerability that allows remote attackers to execute arbitrary code by sending malicious input to the application. Attackers can craft payloads with ROP chains to achieve code execution in the application context, with failed attempts potentially causing denial of service.	9.8	More Details
CVE-2026-4484	The Masteriyo LMS plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.1.6. This is due to the plugin allowing a user to update the user role through the 'InstructorsController::prepare_object_for_database' function. This makes it possible for authenticated attackers, with Student-level access and above, to elevate their privileges to that of an administrator.	9.8	More Details

CVE-2025-15604	Amon2 versions before 6.17 for Perl use an insecure random_string implementation for security functions. In versions 6.06 through 6.16, the random_string function will attempt to read bytes from the /dev/urandom device, but if that is unavailable then it generates bytes by concatenating a SHA-1 hash seeded with the built-in rand() function, the PID, and the high resolution epoch time. The PID will come from a small set of numbers, and the epoch time may be guessed, if it is not leaked from the HTTP Date header. The built-in rand function is unsuitable for cryptographic usage. Before version 6.06, there was no fallback when /dev/urandom was not available. Before version 6.04, the random_string function used the built-in rand() function to generate a mixed-case alphanumeric string. This function may be used for generating session ids, generating secrets for signing or encrypting cookie session data and generating tokens used for Cross Site Request Forgery (CSRF) protection.	9.8	More Details
CVE-2026-33942	Saloon is a PHP library that gives users tools to build API integrations and SDKs. Versions prior to 4.0.0 used PHP's unserialize() in AccessTokenAuthenticator::unserialize() to restore OAuth token state from cache or storage, with allowed_classes => true. An attacker who can control the serialized string (e.g. by overwriting a cached token file or via another injection) can supply a serialized "gadget" object. When unserialize() runs, PHP instantiates that object and runs its magic methods (__wakeup, __destruct, etc.), leading to object injection. In environments with common dependencies (e.g. Monolog), this can be chained to remote code execution (RCE). The fix in version 4.0.0 removes PHP serialization from the AccessTokenAuthenticator class requiring users to store and resolve the authenticator manually.	9.8	More Details
CVE-2026-33640	Outline is a service that allows for collaborative documentation. Outline implements an Email OTP login flow for users not associated with an Identity Provider. Starting in version 0.86.0 and prior to version 1.6.0, Outline does not invalidate OTP codes based on amount or frequency of invalid submissions, rather it relies on the rate limiter to restrict attempts. Consequently, identified bypasses in the rate limiter permit unrestricted OTP code submissions within the codes lifetime. This allows attackers to perform brute force attacks which enable account takeover. Version 1.6.0 fixes the issue.	9.8	More Details
CVE-2026-33670	SiYuan is a personal knowledge management system. Prior to version 3.6.2, the /api/file/readDir interface was used to traverse and retrieve the file names of all documents under a notebook. Version 3.6.2 patches the issue.	9.8	More Details
CVE-2026-30530	A SQL Injection vulnerability exists in SourceCodester Online Food Ordering System v1.0 in the Actions.php file (specifically the save_customer action). The application fails to properly sanitize user input supplied to the "username" parameter. This allows an attacker to inject malicious SQL commands.	9.8	More Details
CVE-2017-20227	JAD Java Decompiler 1.5.8e-1kali1 and prior contains a stack-based buffer overflow vulnerability that allows attackers to execute arbitrary code by supplying overly long input that exceeds buffer boundaries. Attackers can craft malicious input passed to the jad command to overflow the stack and execute a return-oriented programming chain that spawns a shell.	9.8	More Details
CVE-2017-20225	TiEmu 2.08 and prior contains a stack-based buffer overflow vulnerability that allows attackers to execute arbitrary code by exploiting inadequate boundary checks on user-supplied input. Attackers can trigger the overflow through command-line arguments passed to the application, leveraging ROP gadgets to bypass protections and execute shellcode in the application context.	9.8	More Details
CVE-2016-20049	JAD 1.5.8e-1kali1 and prior contains a stack-based buffer overflow vulnerability that allows attackers to execute arbitrary code by supplying oversized input that exceeds buffer boundaries. Attackers can craft malicious input strings exceeding 8150 bytes to overflow the stack, overwrite return addresses, and execute shellcode in the application context.	9.8	More Details
CVE-2026-22738	In Spring AI, a SpEL injection vulnerability exists in SimpleVectorStore when a user-supplied value is used as a filter expression key. A malicious actor could exploit this to execute arbitrary code. Only applications that use SimpleVectorStore and pass user-supplied input as a filter expression key are affected. This issue affects Spring AI: from 1.0.0 before 1.0.5, from 1.1.0 before 1.1.4.	9.8	More Details
CVE-2026-33937	Handlebars provides the power necessary to let users build semantic templates. In versions 4.0.0 through 4.7.8, `Handlebars.compile()` accepts a pre-parsed AST object in addition to a template string. The `value` field of a `NumberLiteral` AST node is emitted directly into the generated JavaScript without quoting or sanitization. An attacker who can supply a crafted AST to `compile()` can therefore inject and execute arbitrary JavaScript, leading to Remote Code Execution on the server. Version 4.7.9 fixes the issue. Some workarounds are available. Validate input type before calling `Handlebars.compile()`; ensure the argument is always a `string`, never a plain object or JSON-deserialized value. Use the Handlebars runtime-only build (`handlebars/runtime`) on the server if templates are pre-compiled at build time; `compile()` will be unavailable.	9.8	More Details
CVE-2025-70888	An issue in mtrojnar Osslsigncode affected at v2.10 and before allows a remote attacker to escalate privileges via the osslsigncode.c component	9.8	More Details
CVE-2026-32924	OpenClaw before 2026.3.12 contains an authorization bypass vulnerability where Feishu reaction events with omitted chat_type are misclassified as p2p conversations instead of group chats. Attackers can exploit this misclassification to bypass groupAllowFrom and requireMention protections in group chat reaction-derived events.	9.8	More Details
CVE-2026-33770	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `fixCleanTitle()` static method in `objects/category.php` constructs a SQL SELECT query by directly interpolating both `$clean_title` and `$id` into the query string without using prepared statements or parameterized queries. An attacker who can trigger category creation or renaming with a crafted title value can inject arbitrary SQL. Commit 994cc2b3d802b819e07e6088338e8bf4e484aae4 contains a patch.	9.8	More Details
CVE-2026-27650	OS Command Injection vulnerability exists in BUFFALO Wi-Fi router products. If this vulnerability is exploited, an arbitrary OS command may be executed on the products.	9.8	More Details
CVE-2026-32669	Code injection vulnerability exists in BUFFALO Wi-Fi router products. If this vulnerability is exploited, an arbitrary code may be executed on the products.	9.8	More Details
CVE-2026-33280	Hidden functionality issue exists in BUFFALO Wi-Fi router products, which may allow an attacker to gain access to the product's debugging functionality, resulting in the execution of arbitrary OS commands.	9.8	More Details
CVE-2026-32973	OpenClaw before 2026.3.11 contains an exec allowlist bypass vulnerability where matchesExecAllowlistPattern improperly normalizes patterns with lowercasing and glob matching that overmatches on POSIX paths. Attackers can exploit the ? wildcard matching across path segments to execute commands or paths not intended by operators.	9.8	More Details
CVE-2026-30303	The command auto-approval module in Axon Code contains an OS Command Injection vulnerability, rendering its whitelist security mechanism ineffective. The vulnerability stems from the incorrect use of an incompatible command parser (the Unix-based shell-quote library) to analyze commands on the Windows platform, coupled with a failure to correctly handle Windows CMD-specific escape sequences (^). Attackers can exploit this discrepancy between the parsing logic and the execution environment by constructing payloads such as git log ^" & malicious_command ^". The Axon Code parser is deceived by the escape characters, misinterpreting the malicious command connector (&) as being within a protected string argument and thus	9.8	More Details

	auto-approving the command. However, the underlying Windows CMD interpreter ignores the escaped quotes, parsing and executing the subsequent malicious command directly. This allows attackers to achieve arbitrary Remote Code Execution (RCE) after bypassing what appears to be a legitimate Git whitelist check.		
CVE-2026-30533	A SQL Injection vulnerability exists in SourceCodester Online Food Ordering System v1.0 in the admin/manage_product.php file via the "id" parameter.	9.8	More Details
CVE-2026-5121	A flaw was found in libarchive. On 32-bit systems, an integer overflow vulnerability exists in the zisofs block pointer allocation logic. A remote attacker can exploit this by providing a specially crafted ISO9660 image, which can lead to a heap buffer overflow. This could potentially allow for arbitrary code execution on the affected system.	9.8	More Details
CVE-2026-3256	HTTP::Session versions through 0.53 for Perl defaults to using insecurely generated session ids. HTTP::Session defaults to using HTTP::Session::ID::SHA1 to generate session ids using a SHA-1 hash seeded with the built-in rand function, the high resolution epoch time, and the PID. The PID will come from a small set of numbers, and the epoch time may be guessed, if it is not leaked from the HTTP Date header. The built-in rand function is unsuitable for cryptographic usage. The distribution includes HTTP::session::ID::MD5 which contains a similar flaw, but uses the MD5 hash instead.	9.8	More Details
CVE-2026-25030	Deserialization of Untrusted Data vulnerability in park_of_ideas Goldish goldish allows Object Injection.This issue affects Goldish: from n/a through < 3.47.	9.8	More Details
CVE-2026-25429	Deserialization of Untrusted Data vulnerability in wpdive Nexa Blocks nexa-blocks allows Object Injection.This issue affects Nexa Blocks: from n/a through <= 1.1.1.	9.8	More Details
CVE-2026-25032	Deserialization of Untrusted Data vulnerability in park_of_ideas Ricky ricky allows Object Injection.This issue affects Ricky: from n/a through < 2.31.	9.8	More Details
CVE-2026-25031	Deserialization of Untrusted Data vulnerability in park_of_ideas Tasty Daily tastydaily allows Object Injection.This issue affects Tasty Daily: from n/a through < 1.27.	9.8	More Details
CVE-2026-1579	The MAVLink communication protocol does not require cryptographic authentication by default. When MAVLink 2.0 message signing is not enabled, any message -- including SERIAL_CONTROL, which provides interactive shell access -- can be sent by an unauthenticated party with access to the MAVLink interface. PX4 provides MAVLink 2.0 message signing as the cryptographic authentication mechanism for all MAVLink communication. When signing is enabled, unsigned messages are rejected at the protocol level.	9.8	More Details
CVE-2026-25029	Deserialization of Untrusted Data vulnerability in park_of_ideas KIDZ kidz allows Object Injection.This issue affects KIDZ: from n/a through <= 5.24.	9.8	More Details
CVE-2025-59706	In N2W before 4.3.2 and 4.4.0 before 4.4.1, improper validation of API request parameters enables remote code execution.	9.8	More Details
CVE-2025-59707	In N2W before 4.3.2 and 4.4.x before 4.4.1, there is potential remote code execution and account credentials theft because of a spoofing vulnerability.	9.8	More Details
CVE-2026-34243	wenxian is a tool to generate BIBTEX files from given identifiers (DOI, PMID, arXiv ID, or paper title). In versions 0.3.1 and prior, a GitHub Actions workflow uses untrusted user input from issue_comment.body directly inside a shell command, allowing potential command injection and arbitrary code execution on the runner. At time of publication, there are no publicly available patches.	9.8	More Details
CVE-2026-24989	Deserialization of Untrusted Data vulnerability in FantasticPlugins SUMO Affiliates Pro affs allows Object Injection.This issue affects SUMO Affiliates Pro: from n/a through < 11.4.0.	9.8	More Details
CVE-2026-24971	Incorrect Privilege Assignment vulnerability in Elated-Themes Search & Go searchgo allows Privilege Escalation.This issue affects Search & Go: from n/a through <= 2.8.	9.8	More Details
CVE-2026-24968	Incorrect Privilege Assignment vulnerability in Xagio SEO Xagio SEO xagio-seo allows Privilege Escalation.This issue affects Xagio SEO: from n/a through <= 7.1.0.30.	9.8	More Details
CVE-2026-24378	Deserialization of Untrusted Data vulnerability in Metagauss EventPrime eventprime-event-calendar-management allows Object Injection.This issue affects EventPrime: from n/a through <= 4.2.8.0.	9.8	More Details
CVE-2026-22507	Deserialization of Untrusted Data vulnerability in AncoraThemes Beelove beelove allows Object Injection.This issue affects Beelove: from n/a through <= 1.2.6.	9.8	More Details
CVE-2026-26830	pdf-image (npm package) through version 2.0.0 allows OS command injection via the pdfFilePath parameter. The constructGetInfoCommand and constructConvertCommandForPage functions use util.format() to interpolate user-controlled file paths into shell command strings that are executed via child_process.exec()	9.8	More Details
CVE-2026-22500	Deserialization of Untrusted Data vulnerability in axiomthemes m2 | Construction and Tools Store m2-ce allows Object Injection.This issue affects m2 | Construction and Tools Store: from n/a through <= 1.1.2.	9.8	More Details
CVE-2026-26831	textract through 2.5.0 is vulnerable to OS Command Injection via the file path parameter in multiple extractors. When processing files with malicious filenames, the filePath is passed directly to child_process.exec() in lib/extractors/doc.js, rtf.js, dxf.js, images.js, and lib/util.js with inadequate sanitization	9.8	More Details
CVE-2026-25035	Authentication Bypass Using an Alternate Path or Channel vulnerability in Wasiliy Strecker / ContestGallery developer Contest Gallery contest-gallery allows Authentication Abuse.This issue affects Contest Gallery: from n/a through <= 28.1.2.2.	9.8	More Details
CVE-2026-32917	OpenClaw before 2026.3.13 contains a remote command injection vulnerability in the iMessage attachment staging flow that allows attackers to execute arbitrary commands on configured remote hosts. The vulnerability exists because unsanitized remote attachment paths containing shell metacharacters are passed directly to the SCP remote operand without validation, enabling command execution when remote attachment staging is enabled.	9.8	More Details
CVE-2026-26833	thumbler through 1.1.2 allows OS command injection via the input, output, time, or size parameter in the thumbnail() function because user input is concatenated into a shell command string passed to child_process.exec() without proper sanitization or escaping.	9.8	More Details
CVE-2026-27049	Authentication Bypass Using an Alternate Path or Channel vulnerability in NooTheme Jobica Core jobica-core allows Authentication Abuse.This issue affects Jobica Core: from n/a through <= 1.4.2.	9.8	More Details

CVE-2026-33032	Nginx UI is a web user interface for the Nginx web server. In versions 2.3.5 and prior, the nginx-ui MCP (Model Context Protocol) integration exposes two HTTP endpoints: /mcp and /mcp_message. While /mcp requires both IP whitelisting and authentication (AuthRequired() middleware), the /mcp_message endpoint only applies IP whitelisting - and the default IP whitelist is empty, which the middleware treats as "allow all". This means any network attacker can invoke all MCP tools without authentication, including restarting nginx, creating/modifying/deleting nginx configuration files, and triggering automatic config reloads - achieving complete nginx service takeover. At time of publication, there are no publicly available patches.	9.8	More Details
CVE-2026-4851	GRID::Machine versions through 0.127 for Perl allows arbitrary code execution via unsafe deserialization. GRID::Machine provides Remote Procedure Calls (RPC) over SSH for Perl. The client connects to remote hosts to execute code on them. A compromised or malicious remote host can execute arbitrary code back on the client through unsafe deserialization in the RPC protocol. read_operation() in lib/GRID/Machine/Message.pm deserialises values from the remote side using eval() $arg .= '$VAR1'; my $val = eval "no strict; $arg"; # line 40-41 $arg is raw bytes from the protocol pipe. A compromised remote host can embed arbitrary perl in the Dumper-formatted response: $VAR1 = do { system("..."); }; This executes on the client silently on every RPC call, as the return values remain correct. This functionality is by design but the trust requirement for the remote host is not documented in the distribution.	9.8	More Details
CVE-2026-31946	OpenOlat is an open source web-based e-learning platform for teaching, learning, assessment and communication. From version 10.5.4 to before version 20.2.5, OpenOLAT's OpenID Connect implicit flow implementation does not verify JWT signatures. The JSONWebToken.parse() method silently discards the signature segment of the compact JWT (header.payload.signature), and the getAccessToken() methods in both OpenIdConnectApi and OpenIdConnectFullConfigurableApi only validate claim-level fields (issuer, audience, state, nonce) without any cryptographic signature verification against the Identity Provider's JWKS endpoint. This issue has been patched in version 20.2.5.	9.8	More Details
CVE-2026-32520	Incorrect Privilege Assignment vulnerability in Andrew Munro / AffiliateWP RewardsWP rewardswp allows Privilege Escalation.This issue affects RewardsWP: from n/a through <= 1.0.4.	9.8	More Details
CVE-2026-4257	The Contact Form by Supsystic plugin for WordPress is vulnerable to Server-Side Template Injection (SSTI) leading to Remote Code Execution (RCE) in all versions up to, and including, 1.7.36. This is due to the plugin using the Twig `Twig_Loader_String` template engine without sandboxing, combined with the `cfsPreFill` prefill functionality that allows unauthenticated users to inject arbitrary Twig expressions into form field values via GET parameters. This makes it possible for unauthenticated attackers to execute arbitrary PHP functions and OS commands on the server by leveraging Twig's `registerUndefinedFilterCallback()` method to register arbitrary PHP callbacks.	9.8	More Details
CVE-2026-32512	Deserialization of Untrusted Data vulnerability in Edge-Themes Pelicula pelicula-video-production-and-movie-theme allows Object Injection.This issue affects Pelicula: from n/a through < 1.10.	9.8	More Details
CVE-2026-32502	Deserialization of Untrusted Data vulnerability in Select-Themes Borgholm borgholm-marketing-agency-theme allows Object Injection.This issue affects Borgholm: from n/a through < 1.6.	9.8	More Details
CVE-2026-3300	The Everest Forms Pro plugin for WordPress is vulnerable to Remote Code Execution via PHP Code Injection in all versions up to, and including, 1.9.12. This is due to the Calculation Addon's process_filter() function concatenating user-submitted form field values into a PHP code string without proper escaping before passing it to eval(). The sanitize_text_field() function applied to input does not escape single quotes or other PHP code context characters. This makes it possible for unauthenticated attackers to inject and execute arbitrary PHP code on the server by submitting a crafted value in any string-type form field (text, email, URL, select, radio) when a form uses the "Complex Calculation" feature.	9.8	More Details
CVE-2026-32714	SciTokens is a reference library for generating and using SciTokens. Prior to version 1.9.6, the KeyCache class in scitokens was vulnerable to SQL Injection because it used Python's str.format() to construct SQL queries with user-supplied data (such as issuer and key_id). This allowed an attacker to execute arbitrary SQL commands against the local SQLite database. This issue has been patched in version 1.9.6.	9.8	More Details
CVE-2026-27095	Deserialization of Untrusted Data vulnerability in magepeopleteam Bus Ticket Booking with Seat Reservation bus-ticket-booking-with-seat-reservation allows Object Injection.This issue affects Bus Ticket Booking with Seat Reservation: from n/a through <= 5.6.0.	9.8	More Details
CVE-2026-27084	Deserialization of Untrusted Data vulnerability in ThemeREX Buisson buisson allows Object Injection.This issue affects Buisson: from n/a through <= 1.1.11.	9.8	More Details
CVE-2026-27083	Deserialization of Untrusted Data vulnerability in ThemeREX Work & Travel Company work-travel-company allows Object Injection.This issue affects Work & Travel Company: from n/a through <= 1.2.	9.8	More Details
CVE-2026-27082	Deserialization of Untrusted Data vulnerability in ThemeREX Love Story lovestory allows Object Injection.This issue affects Love Story: from n/a through <= 1.3.12.	9.8	More Details
CVE-2026-28858	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 26.4 and iPadOS 26.4. A remote user may be able to cause unexpected system termination or corrupt kernel memory.	9.8	More Details
CVE-2026-27051	Incorrect Privilege Assignment vulnerability in uxper Golo golo allows Privilege Escalation.This issue affects Golo: from n/a through <= 1.7.0.	9.8	More Details
CVE-2026-26832	node-tesseract-ocr is an npm package that provides a Node.js wrapper for Tesseract OCR. In all versions through 2.2.1, the recognize() function in src/index.js is vulnerable to OS Command Injection. The file path parameter is concatenated into a shell command string and passed to child_process.exec() without proper sanitization	9.8	More Details
CVE-2026-2275	The CrewAI CodeInterpreter tool falls back to SandboxPython when it cannot reach Docker, which can enable RCE through arbitrary C function calling.	9.6	More Details
CVE-2026-33976	Notesnook is a note-taking app. Prior to version 3.3.11 on Web/Desktop and 3.3.17 on Android/iOS, a stored XSS in the Web Clipper rendering flow can be escalated to remote code execution in the desktop app. The root cause is that the clipper preserves attacker-controlled attributes from the source page's root element and stores them inside web-clip HTML. When the clip is later opened, Notesnook renders that HTML into a same-origin, unsandboxed iframe using `contentDocument.write(...)`. Event-handler attributes such as `onload`, `onclick`, or `onmouseover` execute in the Notesnook origin. In the desktop app, this becomes RCE because Electron is configured with `nodeIntegration: true` and `contextIsolation: false`. Version 3.3.11 Web/Desktop and 3.3.17 on Android/iOS patch the issue.	9.6	More Details
CVE-2026-34205	Home Assistant is open source home automation software that puts local control and privacy first. Home Assistant apps (formerly add-ons) configured with host network mode expose unauthenticated endpoints bound to the internal Docker bridge interface to the local network. On Linux, this configuration does not restrict access to the app as intended, allowing any device	9.6	More Details

	on the same network to reach these endpoints without authentication. Home Assistant Supervisor 2026.03.02 addresses the issue.		
CVE-2026-33757	OpenBao is an open source identity-based secrets management system. Prior to version 2.5.2, OpenBao does not prompt for user confirmation when logging in via JWT/OIDC and a role with `callback_mode` set to `direct`. This allows an attacker to start an authentication request and perform "remote phishing" by having the victim visit the URL and automatically log-in to the session of the attacker. Despite being based on the authorization code flow, the `direct` mode calls back directly to the API and allows an attacker to poll for an OpenBao token until it is issued. Version 2.5.2 includes an additional confirmation screen for `direct` type logins that requires manual user interaction in order to finish the authentication. This issue can be worked around either by removing any roles with `callback_mode=direct` or enforcing confirmation for every session on the token issuer side for the Client ID used by OpenBao.	9.6	More Details
CVE-2026-30304	In its design for automatic terminal command execution, AI Code offers two options: Execute safe commands and execute all commands. The description for the former states that commands determined by the model to be safe will be automatically executed, whereas if the model judges a command to be potentially destructive, it still requires user approval. However, this design is highly susceptible to prompt injection attacks. An attacker can employ a generic template to wrap any malicious command and mislead the model into misclassifying it as a 'safe' command, thereby bypassing the user approval requirement and resulting in arbitrary command execution.	9.6	More Details
CVE-2026-34449	SiYuan is a personal knowledge management system. Prior to version 3.6.2, a malicious website can achieve Remote Code Execution (RCE) on any desktop running SiYuan by exploiting the permissive CORS policy (Access-Control-Allow-Origin: * + Access-Control-Allow-Private-Network: true) to inject a JavaScript snippet via the API. The injected snippet executes in Electron's Node.js context with full OS access the next time the user opens SiYuan's UI. No user interaction is required beyond visiting the malicious website while SiYuan is running. This issue has been patched in version 3.6.2.	9.6	More Details
CVE-2026-32916	OpenClaw versions 2026.3.7 before 2026.3.11 contain an authorization bypass vulnerability where plugin subagent routes execute gateway methods through a synthetic operator client with broad administrative scopes. Remote unauthenticated requests to plugin-owned routes can invoke runtime.subagent methods to perform privileged gateway actions including session deletion and agent execution.	9.4	More Details
CVE-2026-34361	HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. Prior to version 6.9.4, the FHIR Validator HTTP service exposes an unauthenticated "/loadIG" endpoint that makes outbound HTTP requests to attacker-controlled URLs. Combined with a startsWith() URL prefix matching flaw in the credential provider (ManagedWebAccessUtils.getServer()), an attacker can steal authentication tokens (Bearer, Basic, API keys) configured for legitimate FHIR servers by registering a domain that prefix-matches a configured server URL. This issue has been patched in version 6.9.4.	9.3	More Details
CVE-2026-30562	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the add_stock.php file via the "msg" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	9.3	More Details
CVE-2026-20688	A path handling issue was addressed with improved validation. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, visionOS 26.4. An app may be able to break out of its sandbox.	9.3	More Details
CVE-2026-33875	Gematik Authenticator securely authenticates users for login to digital health applications. Versions prior to 4.16.0 are vulnerable to authentication flow hijacking, potentially allowing attackers to authenticate with the identities of victim users who click on a malicious deep link. Update Gematik Authenticator to version 4.16.0 or greater to receive a patch. There are no known workarounds.	9.3	More Details
CVE-2026-22484	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in pebas Lisfinity Core lisfinity-core allows SQL Injection.This issue affects Lisfinity Core: from n/a through <= 1.5.0.	9.3	More Details
CVE-2026-28827	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to break out of its sandbox.	9.3	More Details
CVE-2026-24993	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPFactory Advanced WooCommerce Product Sales Reporting webd-woocommerce-advanced-reporting-statistics allows Blind SQL Injection.This issue affects Advanced WooCommerce Product Sales Reporting: from n/a through <= 4.1.3.	9.3	More Details
CVE-2026-25340	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NooTheme Jobmonster noo-jobmonster allows Blind SQL Injection.This issue affects Jobmonster: from n/a through < 4.8.4.	9.3	More Details
CVE-2026-25377	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in eyecix Addon Jobsearch Chat addon-jobsearch-chat allows SQL Injection.This issue affects Addon Jobsearch Chat: from n/a through <= 3.0.	9.3	More Details
CVE-2026-32539	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in PublishPress PublishPress Revisions revisionary allows Blind SQL Injection.This issue affects PublishPress Revisions: from n/a through <= 3.7.23.	9.3	More Details
CVE-2026-31920	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Devteam HaywoodTech Product Rearrange for WooCommerce products-rearrange-woocommerce allows Blind SQL Injection.This issue affects Product Rearrange for WooCommerce: from n/a through <= 1.2.2.	9.3	More Details
CVE-2026-32499	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in QuantumCloud ChatBot chatbot allows Blind SQL Injection.This issue affects ChatBot: from n/a through <= 7.7.9.	9.3	More Details
CVE-2026-34714	Vim before 9.2.0272 allows code execution that happens immediately upon opening a crafted file in the default configuration, because %{expr} injection occurs with tabpanel lacking P_MLE.	9.2	More Details
CVE-2026-21861	baserCMS is a website development framework. Prior to version 5.2.3, baserCMS contains an OS command injection vulnerability in the core update functionality. An authenticated administrator can execute arbitrary OS commands on the server due to improper handling of user-controlled input that is directly passed to exec() without sufficient validation or escaping. This issue has been patched in version 5.2.3.	9.1	More Details
CVE-2026-25447	Improper Control of Generation of Code ('Code Injection') vulnerability in Jonathan Daggerhart Widget Wrangler widget-wrangler allows Code Injection.This issue affects Widget Wrangler: from n/a through <= 2.3.9.	9.1	More Details
CVE-2026-27071	Missing Authorization vulnerability in Arraytics WPCafe wp-cafe allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPCafe: from n/a through <= 3.0.7.	9.1	More Details

CVE-2025-15618	Business::OnlinePayment::StoredTransaction versions through 0.01 for Perl uses an insecure secret key. Business::OnlinePayment::StoredTransaction generates a secret key by using a MD5 hash of a single call to the built-in rand function, which is unsuitable for cryptographic use. This key is intended for encrypting credit card transaction data.	9.1	More Details
CVE-2026-30877	baserCMS is a website development framework. Prior to version 5.2.3, there is an OS command injection vulnerability in the update functionality. Due to this issue, an authenticated user with administrator privileges in baserCMS can execute arbitrary OS commands on the server with the privileges of the user account running baserCMS. This issue has been patched in version 5.2.3.	9.1	More Details
CVE-2026-33152	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. In versions prior to 2.6.0, Tandoor Recipes configures Django REST Framework with BasicAuthentication as one of the default authentication backends. The AllAuth rate limiting configuration (ACCOUNT_RATE_LIMITS: login: 5/m/ip) only applies to the HTML-based login endpoint at /accounts/login/. Any API endpoint that accepts authenticated requests can be targeted via Authorization: Basic headers with zero rate limiting, zero account lockout, and unlimited attempts. An attacker can perform high-speed password guessing against any known username. Version 2.6.0 patches the issue.	9.1	More Details
CVE-2026-34374	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `Live_schedule::keyExists()` method constructs a SQL query by interpolating a stream key directly into the query string without parameterization. This method is called as a fallback from `LiveTransmition::keyExists()` when the initial parameterized lookup returns no results. Although the calling function correctly uses parameterized queries for its own lookup, the fallback path to `Live_schedule::keyExists()` undoes this protection entirely. This vulnerability is distinct from GHSA-pvw4-p2jm-chjm, which covers SQL injection via the `live_schedule_id` parameter in the reminder function. This finding targets the stream key lookup path used during RTMP publish authentication. As of time of publication, no patched versions are available.	9.1	More Details
CVE-2026-34558	CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input within the Methods Management functionality when creating or managing application methods/pages. Multiple input fields accept attacker-controlled JavaScript payloads that are stored server-side without sanitization or output encoding. These stored values are later rendered directly into administrative interfaces and global navigation components without proper encoding, resulting in Stored DOM-Based Cross-Site Scripting (XSS). This issue has been patched in version 0.31.0.0.	9.1	More Details
CVE-2026-34557	CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input within group and role management functionality. Multiple input fields (three distinct group-related fields) can be injected with malicious JavaScript payloads, which are then stored server-side. These stored payloads are later rendered unsafely within privileged administrative views without proper output encoding, leading to stored cross-site scripting (XSS) within the role and permission management context. This issue has been patched in version 0.31.0.0.	9.1	More Details
CVE-2026-32524	Unrestricted Upload of File with Dangerous Type vulnerability in Jordy Meow Photo Engine wplr-sync allows Upload a Web Shell to a Web Server.This issue affects Photo Engine: from n/a through <= 6.4.9.	9.1	More Details
CVE-2026-32573	Improper Control of Generation of Code ('Code Injection') vulnerability in Nelio Software Nelio AB Testing nelio-ab-testing allows Code Injection.This issue affects Nelio AB Testing: from n/a through <= 8.2.7.	9.1	More Details
CVE-2026-33183	Saloon is a PHP library that gives users tools to build API integrations and SDKs. Prior to version 4.0.0, fixture names were used to build file paths under the configured fixture directory without validation. A name containing path segments (e.g. ../traversal or ../../etc/passwd) resulted in a path outside that directory. When the application read a fixture (e.g. for mocking) or wrote one (e.g. when recording responses), it could read or write files anywhere the process had access. If the fixture name was derived from user or attacker-controlled input (e.g. request parameters or config), this constituted a path traversal vulnerability and could lead to disclosure of sensitive files or overwriting of critical files. The fix in version 4.0.0 adds validation in the fixture layer (rejecting names with /, \, .., or null bytes, and restricting to a safe character set) and defense-in-depth in the storage layer (ensuring the resolved path remains under the base directory before any read or write).	9.1	More Details
CVE-2026-27815	EVerest is an EV charging software stack. Prior to versions to 2026.02.0, ISO15118_chargerImpl::handle_session_setup copies a variable-length payment_options list into a fixed-size array of length 2 without bounds checking. With schema validation disabled by default, oversized MQTT Cmd payloads can trigger out-of-bounds writes and corrupt adjacent EVSE state or crash the process. Version 2026.02.0 contains a patch.	9.1	More Details
CVE-2026-27816	EVerest is an EV charging software stack. Prior to versions to 2026.02.0, ISO15118_chargerImpl::handle_update_energy_transfer_modes copies a variable-length list into a fixed-size array of length 6 without bounds checking. With schema validation disabled by default, oversized MQTT Cmd payloads can trigger out-of-bounds writes and corrupt adjacent EVSE state or crash the process. Version 2026.02.0 contains a patch.	9.1	More Details
CVE-2026-30458	An issue in Daylight Studio FuelCMS v1.5.2 allows attackers to exfiltrate users' password reset tokens via a mail splitting attack.	9.1	More Details
CVE-2026-27876	A chained attack via SQL Expressions and a Grafana Enterprise plugin can lead to a remote arbitrary code execution impact (RCE). This is enabled by a feature in Grafana (OSS), so all users are always recommended to update to avoid future attack vectors going this path. Only instances with the sqlExpressions feature toggle enabled are vulnerable.	9.1	More Details
CVE-2026-33749	n8n is an open source workflow automation platform. Prior to versions 1.123.27, 2.13.3, and 2.14.1, an authenticated user with permission to create or modify workflows could craft a workflow that produces an HTML binary data object without a filename. The `/rest/binary-data` endpoint served such responses inline on the n8n origin without `Content-Disposition` or `Content-Security-Policy` headers, allowing the HTML to render in the browser with full same-origin JavaScript access. By sending the resulting URL to a higher-privileged user, an attacker could execute JavaScript in the victim's authenticated session, enabling exfiltration of workflows and credentials, modification of workflows, or privilege escalation to admin. The issue has been fixed in n8n versions 1.123.27, 2.13.3, and 2.14.1. Users should upgrade to one of these versions or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations: Limit workflow creation and editing permissions to fully trusted users only, and/or restrict network access to the n8n instance to prevent untrusted users from accessing binary data URLs. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	9.0	More Details
CVE-2026-30282	An arbitrary file overwrite vulnerability in UXGROUP LLC Cast to TV Screen Mirroring v2.2.77 allows attackers to overwrite critical internal files via the file import process, leading to arbtrary code execution or information exposure.	9.0	More Details
CVE-2025-32991	In N2WS Backup & Recovery before 4.4.0, a two-step attack against the RESTful API results in remote code execution.	9.0	More Details

CVE-2026-34448	SiYuan is a personal knowledge management system. Prior to version 3.6.2, an attacker who can place a malicious URL in an Attribute View mAsse field can trigger stored XSS when a victim opens the Gallery or Kanban view with “Cover From -> Asset Field” enabled. The vulnerable code accepts arbitrary http(s) URLs without extensions as images, stores the attacker-controlled string in coverURL, and injects it directly into an <img src="..."> attribute without escaping. In the Electron desktop client, the injected JavaScript executes with nodeIntegration enabled and contextIsolation disabled, so the XSS reaches arbitrary OS command execution under the victim’s account. This issue has been patched in version 3.6.2.	9.0	More Details
CVE-2026-32519	Incorrect Privilege Assignment vulnerability in Bit Apps Bit SMTP bit-smtp allows Privilege Escalation.This issue affects Bit SMTP: from n/a through <= 1.2.2.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Referer
CVE-2026-4905	A vulnerability was found in Tenda AC5 15.03.06.47. Impacted is the function formWifiWpsOOB of the file /goform/WifiWpsOOB of the component POST Request Handler. Performing a manipulation of the argument index results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-33413	etcd is a distributed key-value store for the data of a distributed system. Prior to versions 3.4.42, 3.5.28, and 3.6.9, unauthorized users may bypass authentication or authorization checks and call certain etcd functions in clusters that expose the gRPC API to untrusted or partially trusted clients. In unpatched etcd clusters with etcd auth enabled, unauthorized users are able to call MemberList and learn cluster topology, including member IDs and advertised endpoints; call Alarm, which can be abused for operational disruption or denial of service; use Lease APIs, interfering with TTL-based keys and lease ownership; and/or trigger compaction, permanently removing historical revisions and disrupting watch, audit, and recovery workflows. Kubernetes does not rely on etcd’s built-in authentication and authorization. Instead, the API server handles authentication and authorization itself, so typical Kubernetes deployments are not affected. Versions 3.4.42, 3.5.28, and 3.6.9 contain a patch. If upgrading is not immediately possible, reduce exposure by treating the affected RPCs as unauthenticated in practice. Restrict network access to etcd server ports so only trusted components can connect and/or require strong client identity at the transport layer, such as mTLS with tightly scoped client certificate distribution.	8.8	More Details
CVE-2026-32915	OpenClaw before 2026.3.11 contains a sandbox boundary bypass vulnerability allowing leaf subagents to access the subagents control surface and resolve against parent requester scope instead of their own session tree. A low-privilege sandboxed leaf worker can steer or kill sibling runs and cause execution with broader tool policies by exploiting insufficient authorization checks on subagent control requests.	8.8	More Details
CVE-2026-32914	OpenClaw before 2026.3.12 contains an insufficient access control vulnerability in the /config and /debug command handlers that allows command-authorized non-owners to access owner-only surfaces. Attackers with command authorization can read or modify privileged configuration settings restricted to owners by exploiting missing owner-level permission checks.	8.8	More Details
CVE-2026-5043	A weakness has been identified in Belkin F9K1122 1.00.33. The impacted element is the function formSetPassword of the file /goform/formSetPassword of the component Parameter Handler. This manipulation of the argument webpage causes stack-based buffer overflow. Remote exploitation of the attack is possible. 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.	8.8	More Details
CVE-2026-29180	Fleet is open source device management software. Prior to 4.81.1, a broken access control vulnerability in Fleet's host transfer API allows a team maintainer to transfer hosts from any team into their own team, bypassing team isolation boundaries. Once transferred, the attacker gains full control over the stolen hosts, including the ability to execute scripts with root privileges. Version 4.81.1 patches the issue.	8.8	More Details
CVE-2026-33687	Sharp is a content management framework built for Laravel as a package. Versions prior to 9.20.0 contain a vulnerability in the file upload endpoint that allows authenticated users to bypass all file type restrictions. The upload endpoint within the `ApiFormUploadController` accepts a client-controlled `validation_rule` parameter. This parameter is directly passed into the Laravel validator without sufficient server-side enforcement. By intercepting the request and sending `validation_rule[]=file`, an attacker can completely bypass all MIME type and file extension restrictions. This issue has been addressed in version 9.20.0 by removing the client-controlled validation rules and strictly defining upload rules server-side. As a workaround, ensure that the storage disk used for Sharp uploads is strictly private. Under default configurations, an attacker cannot directly execute uploaded PHP files unless a public disk configuration is explicitly used.	8.8	More Details
CVE-2026-5042	A security flaw has been discovered in Belkin F9K1122 1.00.33. The affected element is the function formCrossBandSwitch of the file /goform/formCrossBandSwitch of the component Parameter Handler. The manipulation of the argument webpage results in stack-based buffer overflow. 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.	8.8	More Details
CVE-2026-5036	A vulnerability was found in Tenda 4G06 04.06.01.29. This vulnerability affects the function fromDhcpListClient of the file /goform/DhcpListClient of the component Endpoint. Performing a manipulation of the argument page results in stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-33686	Sharp is a content management framework built for Laravel as a package. Versions prior to 9.20.0 have a path traversal vulnerability in the FileUtil class. The application fails to sanitize file extensions properly, allowing path separators to be passed into the storage layer. In `src/Utils/FileUtil.php`, the `FileUtil::explodeExtension()` function extracts a file's extension by splitting the filename at the last dot. This issue has been patched in version 9.20.0 by properly sanitizing the extension using `pathinfo(PATHINFO_EXTENSION)` instead of `strrpos()`, alongside applying strict regex replacements to both the base name and the extension.	8.8	More Details
CVE-2026-32484	Deserialization of Untrusted Data vulnerability in BoldGrid weForms weforms allows Object Injection.This issue affects weForms: from n/a through <= 1.6.26.	8.8	More Details
CVE-2026-33735	MyTube is a self-hosted downloader and player for several video websites Prior to version 1.8.69, an authorization bypass in the `/api/settings/import-database` endpoint allows attackers with low-privilege credentials to upload and replace the application's SQLite database entirely, leading to a full compromise of the application. The bypass is relevant for other POST routes as well. Version 1.8.69 fixes the issue.	8.8	More Details
CVE-2026-5024	A vulnerability was found in D-Link DIR-513 1.10. This issue affects the function formSetEmail of the file /goform/formSetEmail. Performing a manipulation of the argument curTime results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-5021	A flaw has been found in Tenda F453 1.0.0.3. This affects the function fromPPTPUserSetting of the file /goform/PPTPUserSetting of the component httpd. This manipulation of the argument delno causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been published and may be used.	8.8	More Details
	WWBN AVideo is an open source video platform. In versions up to and including 26.0, in `objects/like.php`, the `getLike()` method constructs a		

CVE-2026-33767	SQL query using a prepared statement placeholder (`?`) for `users_id` but directly concatenates `$this->videos_id` into the query string without parameterization. An attacker who can control the `videos_id` value (via a crafted request) can inject arbitrary SQL, bypassing the partial prepared-statement protection. Commit 0215d3c4f1ee748b8880254967b51784b8ac4080 contains a patch.	8.8	More Details
CVE-2026-5004	A vulnerability was determined in Wavlink WL-WN579X3-C 231124. This impacts the function sub_4019FC of the file /cgi-bin/firewall.cgi of the component UPNP Handler. Executing a manipulation of the argument UpnpEnabled can lead to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-4976	A vulnerability was found in Totolink LR350 9.3.5u.6369_B20220309. This vulnerability affects the function setWiFiGuestCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ssid results in buffer overflow. The attack can be launched remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-4906	A vulnerability was determined in Tenda AC5 15.03.06.47. The affected element is the function decodePwd of the file /goform/WizardHandle of the component POST Request Handler. Executing a manipulation of the argument WANT/WANS can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2024-51348	A stack-based buffer overflow vulnerability in the P2P API service in BS Producten Petcam with firmware 33.1.0.0818 allows unauthenticated attackers within network range to overwrite the instruction pointer and achieve Remote Code Execution (RCE) by sending a specially crafted HTTP request.	8.8	More Details
CVE-2026-25414	Incorrect Privilege Assignment vulnerability in iqonicdesign WPBookit Pro wpbookit-pro allows Privilege Escalation.This issue affects WPBookit Pro: from n/a through <= 1.6.18.	8.8	More Details
CVE-2026-25406	Authentication Bypass Using an Alternate Path or Channel vulnerability in Themeum Tutor LMS Pro tutor-pro allows Authentication Abuse.This issue affects Tutor LMS Pro: from n/a through <= 3.9.4.	8.8	More Details
CVE-2026-4815	A SQL Injection vulnerability has been found in Support Board v3.7.7. This vulnerability allows an attacker to retrieve, create, update and delete database via 'calls[0][message_ids][]' parameter in '/supportboard/include/ajax.php' endpoint.	8.8	More Details
CVE-2026-23514	Kiteworks is a private data network (PDN). Versions 9.2.0 and 9.2.1 of Kiteworks Core have an access control vulnerability that allows authenticated users to access unauthorized content. Upgrade Kiteworks Core to version 9.2.2 or later to receive a patch.	8.8	More Details
CVE-2026-25400	Deserialization of Untrusted Data vulnerability in thememount Apicona apicona allows Object Injection.This issue affects Apicona: from n/a through <= 24.1.0.	8.8	More Details
CVE-2026-33622	PinchTab is a standalone HTTP server that gives AI agents direct control over a Chrome browser. PinchTab `v0.8.3` through `v0.8.5` allow arbitrary JavaScript execution through `POST /wait` and `POST /tabs/{id}/wait` when the request uses `fn` mode, even if `security.allowEvaluate` is disabled. `POST /evaluate` correctly enforces the `security.allowEvaluate` guard, which is disabled by default. However, in the affected releases, `POST /wait` accepted a user-controlled `fn` expression, embedded it directly into executable JavaScript, and evaluated it in the browser context without checking the same policy. This is a security-policy bypass rather than a separate authentication bypass. Exploitation still requires authenticated API access, but a caller with the server token can execute arbitrary JavaScript in a tab context even when the operator explicitly disabled JavaScript evaluation. The current worktree fixes this by applying the same policy boundary to `fn` mode in `/wait` that already exists on `/evaluate`, while preserving the non-code wait modes. As of time of publication, a patched version is not yet available.	8.8	More Details
CVE-2026-22790	EVerest is an EV charging software stack. Prior to version 2026.02.0, `HomeplugMessage::setup_payload` trusts `len` after an `assert`; in release builds the check is removed, so oversized SLAC payloads are `memcpy`'d into a ~1497-byte stack buffer, corrupting the stack and enabling remote code execution from network-provided frames. Version 2026.02.0 contains a patch.	8.8	More Details
CVE-2026-33943	Happy DOM is a JavaScript implementation of a web browser without its graphical user interface. In versions 15.10.0 through 20.8.7, a code injection vulnerability in `ECMAScriptModuleCompiler` allows an attacker to achieve Remote Code Execution (RCE) by injecting arbitrary JavaScript expressions inside `export { }` declarations in ES module scripts processed by happy-dom. The compiler directly interpolates unsanitized content into generated code as an executable expression, and the quote filter does not strip backticks, allowing template literal-based payloads to bypass sanitization. Version 20.8.8 fixes the issue.	8.8	More Details
CVE-2026-5204	A vulnerability was determined in Tenda CH22 1.0.0.1. Affected is the function formWebTypeLibrary of the file /goform/webtypelibrary of the component Parameter Handler. This manipulation of the argument webSiteId causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-26060	Fleet is open source device management software. Prior to 4.81.0, a vulnerability in Fleet’s password management logic could allow previously issued password reset tokens to remain valid after a user changes their password. As a result, a stale password reset token could be reused to reset the account password even after a defensive password change. Version 4.81.0 patches the issue.	8.8	More Details
CVE-2026-28228	OpenOlat is an open source web-based e-learning platform for teaching, learning, assessment and communication. Prior to versions 19.1.31, 20.1.18, and 20.2.5, an authenticated user with the Author role can inject Velocity directives into a reminder email template. When the reminder is processed (either triggered manually or via the daily cron job), the injected directives are evaluated server-side. By chaining Velocity's #set directive with Java reflection, an attacker can instantiate arbitrary Java classes such as java.lang.ProcessBuilder and execute operating system commands with the privileges of the Tomcat process (typically root in containerized deployments). This issue has been patched in versions 19.1.31, 20.1.18, and 20.2.5.	8.8	More Details
CVE-2026-33898	Incus is a system container and virtual machine manager. Prior to version 6.23.0, the web server spawned by `incus webui` incorrectly validates the authentication token such that an invalid value will be accepted. `incus webui` runs a local web server on a random localhost port. For authentication, it provides the user with a URL containing an authentication token. When accessed with that token, Incus creates a cookie persisting that token without needing to include it in subsequent HTTP requests. While the Incus client correctly validates the value of the cookie, it does not correctly validate the token when passed int the URL. This allows for an attacker able to locate and talk to the temporary web server on localhost to have as much access to Incus as the user who ran `incus webui`. This can lead to privilege escalation by another local user or an access to the user's Incus instances and possibly system resources by a remote attack able to trick the local user into interacting with the Incus UI web server. Version 6.23.0 patches the issue.	8.8	More Details
CVE-2026-	A vulnerability was detected in Tenda CH22 1.0.0.1. Impacted is the function formCreateFileName of the file /goform/createFileName. Performing a manipulation of the argument fileNameMit results in stack-based buffer overflow. The attack may be initiated remotely. The	8.8	More

5152	exploit is now public and may be used.		Details
CVE-2026-27893	vLLM is an inference and serving engine for large language models (LLMs). Starting in version 0.10.1 and prior to version 0.18.0, two model implementation files hardcode `trust_remote_code=True` when loading sub-components, bypassing the user's explicit `--trust-remote-code=False` security opt-out. This enables remote code execution via malicious model repositories even when the user has explicitly disabled remote code trust. Version 0.18.0 patches the issue.	8.8	More Details
CVE-2026-4961	A vulnerability was identified in Tenda AC6 15.03.05.16. Affected by this vulnerability is the function formQuickIndex of the file /goform/QuickIndex of the component POST Request Handler. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-4903	A flaw has been found in Tenda AC5 15.03.06.47. This vulnerability affects the function formQuickIndex of the file /goform/QuickIndex of the component POST Request Handler. This manipulation of the argument PPPOEPassword causes stack-based buffer overflow. The attack may be initiated remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-4960	A vulnerability was determined in Tenda AC6 15.03.05.16. Affected is the function fromWizardHandle of the file /goform/WizardHandle of the component POST Request Handler. Executing a manipulation of the argument WANT/WANS can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-5130	The Debugger & Troubleshooter plugin for WordPress was vulnerable to Unauthenticated Privilege Escalation in versions up to and including 1.3.2. This was due to the plugin accepting the wp_debug_troubleshoot_simulate_user cookie value directly as a user ID without any cryptographic validation or authorization checks. The cookie value was used to override the determine_current_user filter, which allowed unauthenticated attackers to impersonate any user by simply setting the cookie to their target user ID. This made it possible for unauthenticated attackers to gain administrator-level access and perform any privileged actions including creating new administrator accounts, modifying site content, installing plugins, or taking complete control of the WordPress site. The vulnerability was fixed in version 1.4.0 by implementing a cryptographic token-based validation system where only administrators can initiate user simulation, and the cookie contains a random 64-character token that must be validated against database-stored mappings rather than accepting arbitrary user IDs.	8.8	More Details
CVE-2026-5154	A vulnerability has been found in Tenda CH22 1.0.0.1/1.lf. The impacted element is the function fromSetCfm of the file /goform/setcfm of the component Parameter Handler. The manipulation of the argument funcname leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-5155	A vulnerability was found in Tenda CH22 1.0.0.1. This affects the function fromAdvSetWan of the file /goform/AdvSetWan of the component Parameter Handler. The manipulation of the argument wanmode results in stack-based buffer overflow. The attack can be executed remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-5156	A vulnerability was determined in Tenda CH22 1.0.0.1. This impacts the function formQuickIndex of the file /goform/QuickIndex of the component Parameter Handler. This manipulation of the argument mit_linktype causes stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-4904	A vulnerability has been found in Tenda AC5 15.03.06.47. This issue affects the function formSetCfm of the file /goform/setcfm of the component POST Request Handler. Such manipulation of the argument funcpara1 leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-33755	Group-Office is an enterprise customer relationship management and groupware tool. Prior to versions 6.8.158, 25.0.92, and 26.0.17, an authenticated SQL Injection vulnerability in the JMAP `Contact/query` endpoint allows any authenticated user with basic addressbook access to extract arbitrary data from the database — including active session tokens of other users. This enables full account takeover of any user, including the System Administrator, without knowing their password. Versions 6.8.158, 25.0.92, and 26.0.17 fix the issue.	8.8	More Details
CVE-2026-4946	Ghidra versions prior to 12.0.3 improperly process annotation directives embedded in automatically extracted binary data, resulting in arbitrary command execution when an analyst interacts with the UI. Specifically, the @execute annotation (which is intended for trusted, user-authored comments) is also parsed in comments generated during auto-analysis (such as CFStrings in Mach-O binaries). This allows a crafted binary to present seemingly benign clickable text which, when clicked, executes attacker-controlled commands on the analyst’s machine.	8.8	More Details
CVE-2026-27045	Deserialization of Untrusted Data vulnerability in sbthemes WooCommerce Infinite Scroll sb-woocommerce-infinite-scroll allows Object Injection.This issue affects WooCommerce Infinite Scroll: from n/a through <= 1.6.2.	8.8	More Details
CVE-2026-34005	In Sofia on Xiongmai DVR/NVR (AHB7008T-MH-V2 and NBD7024H-P) 4.03.R11 devices, root OS command injection can occur via shell metacharacters in the HostName value via an authenticated DVRIP protocol (TCP port 34567) request to the NetWork.NetCommon configuration handler, because system() is used.	8.8	More Details
CVE-2026-5046	A flaw has been found in Tenda FH1201 1.2.0.14(408). Affected is the function formWrlExtraSet of the file /goform/WrlExtraSet of the component Parameter Handler. Executing a manipulation of the argument GO can lead to stack-based buffer overflow. The attack may be performed from remote. The exploit has been published and may be used.	8.8	More Details
CVE-2026-5045	A vulnerability was detected in Tenda FH1201 1.2.0.14(408). This impacts the function WrlclientSet of the file /goform/WrlclientSet of the component Parameter Handler. Performing a manipulation of the argument GO results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-4902	A vulnerability was detected in Tenda AC5 15.03.06.47. This affects the function fromAddressNat of the file /goform/addressNat of the component POST Request Handler. The manipulation of the argument page results in stack-based buffer overflow. The attack can be launched remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-34040	Moby is an open source container framework. Prior to version 29.3.1, a security vulnerability has been detected that allows attackers to bypass authorization plugins (AuthZ). This issue has been patched in version 29.3.1.	8.8	More Details
CVE-2026-5044	A security vulnerability has been detected in Belkin F9K1122 1.00.33. This affects the function formSetSystemSettings of the file /goform/formSetSystemSettings of the component Setting Handler. Such manipulation of the argument webpage leads to stack-based buffer overflow. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-27040	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in AA-Team WZone woozone allows Path Traversal.This issue affects WZone: from n/a through <= 14.0.31.	8.8	More Details
CVE-	OpenClaw before 2026.3.11 contains an authorization bypass vulnerability in the gateway agent RPC that allows authenticated operators with		

2026-33573	operator.write permission to override workspace boundaries by supplying attacker-controlled spawnedBy and workspaceDir values. Remote operators can escape the configured workspace boundary and execute arbitrary file and exec operations from any process-accessible directory.	8.8	More Details
CVE-2026-32513	Deserialization of Untrusted Data vulnerability in Miguel Useche JS Archive List jquery-archive-list-widget allows Object Injection.This issue affects JS Archive List: from n/a through <= 6.1.7.	8.8	More Details
CVE-2026-33030	Nginx UI is a web user interface for the Nginx web server. In versions 2.3.3 and prior, Nginx-UI contains an Insecure Direct Object Reference (IDOR) vulnerability that allows any authenticated user to access, modify, and delete resources belonging to other users. The application's base Model struct lacks a user_id field, and all resource endpoints perform queries by ID without verifying user ownership, enabling complete authorization bypass in multi-user environments. At time of publication, there are no publicly available patches.	8.8	More Details
CVE-2026-25360	Deserialization of Untrusted Data vulnerability in rascals Vex vex allows Object Injection.This issue affects Vex: from n/a through < 1.2.9.	8.8	More Details
CVE-2026-4974	A flaw has been found in Tenda AC7 15.03.06.44. Affected by this issue is the function fromSetSysTime of the file /goform/SetSysTimeCfg of the component POST Request Handler. Executing a manipulation of the argument Time can lead to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-4975	A vulnerability has been found in Tenda AC15 15.03.05.19. This affects the function formSetCfm of the file /goform/setcfm of the component POST Request Handler. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-30531	A SQL Injection vulnerability exists in SourceCodester Online Food Ordering System v1.0 in the Actions.php file (specifically the save_category action). The application fails to properly sanitize user input supplied to the "name" parameter. This allows an authenticated attacker to inject malicious SQL commands.	8.8	More Details
CVE-2026-33917	OpenEMR is a free and open source electronic health records and medical practice management application. Versions prior to 8.0.0.3 contais a SQL injection vulnerability in the ajax_save CAMOS form that can be exploited by authenticated attackers. The vulnerability exists due to insufficient input validation in the ajax_save page in the CAMOS form. Version 8.0.0.3 patches the issue.	8.8	More Details
CVE-2026-4862	A security vulnerability has been detected in UTT HiPER 1250GW up to 3.2.7-210907-180535. This issue affects the function strcpy of the file /goform/formConfigDnsFilterGlobal of the component Parameter Handler. Such manipulation of the argument GroupName leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-4861	A weakness has been identified in Wavlink WL-NU516U1 260227. This vulnerability affects the function ftext of the file /cgi-bin/nas.cgi. This manipulation of the argument Content-Length causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-5211	A flaw has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205. This vulnerability affects the function UPnP_AV_Server_Path_Del of the file /cgi-bin/app_mgr.cgi. Executing a manipulation of the argument f_dir can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-5212	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205. This issue affects the function Webdav_Upload_File of the file /cgi-bin/webdav_mgr.cgi. The manipulation of the argument f_file leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-25359	Deserialization of Untrusted Data vulnerability in rascals Pendulum pendulum allows Object Injection.This issue affects Pendulum: from n/a through < 3.1.5.	8.8	More Details
CVE-2026-24359	Authentication Bypass Using an Alternate Path or Channel vulnerability in Dokan, Inc. Dokan dokan-lite allows Authentication Abuse.This issue affects Dokan: from n/a through <= 4.2.4.	8.8	More Details
CVE-2026-25358	Deserialization of Untrusted Data vulnerability in rascals Meloo meloo allows Object Injection.This issue affects Meloo: from n/a through < 2.8.2.	8.8	More Details
CVE-2026-30529	A SQL Injection vulnerability exists in SourceCodester Online Food Ordering System v1.0 in the Actions.php file (specifically the save_user action). The application fails to properly sanitize user input supplied to the "username" parameter. This allows an authenticated attacker to inject malicious SQL commands.	8.8	More Details
CVE-2026-5027	The 'POST /api/v2/files' endpoint does not sanitize the 'filename' parameter from the multipart form data, allowing an attacker to write files to arbitrary locations on the filesystem using path traversal sequences ('../').	8.8	More Details
CVE-2026-24981	Deserialization of Untrusted Data vulnerability in NooTheme Visionary Core noo-visionary-core allows Object Injection.This issue affects Visionary Core: from n/a through <= 1.4.9.	8.8	More Details
CVE-2026-4747	Each RPCSEC_GSS data packet is validated by a routine which checks a signature in the packet. This routine copies a portion of the packet into a stack buffer, but fails to ensure that the buffer is sufficiently large, and a malicious client can trigger a stack overflow. Notably, this does not require the client to authenticate itself first. As kgssapi.ko's RPCSEC_GSS implementation is vulnerable, remote code execution in the kernel is possible by an authenticated user that is able to send packets to the kernel's NFS server while kgssapi.ko is loaded into the kernel. In userspace, applications which have librpcgss_sec loaded and run an RPC server are vulnerable to remote code execution from any client able to send it packets. We are not aware of any such applications in the FreeBSD base system.	8.8	More Details
CVE-2026-4758	The WP Job Portal plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'WPJOBPORTALcustomfields::removeFileCustom' function in all versions up to, and including, 2.4.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	8.8	More Details
CVE-			

2025-70887	An issue in ralphje Signify before v.0.9.2 allows a remote attacker to escalate privileges via the signed_data.py and the context.py components	8.8	More Details
CVE-2026-24978	Deserialization of Untrusted Data vulnerability in NooTheme Jobica Core jobica-core allows Object Injection.This issue affects Jobica Core: from n/a through <= 1.4.1.	8.8	More Details
CVE-2026-32530	Incorrect Privilege Assignment vulnerability in WPFunnels Creator LMS creatorlms allows Privilege Escalation.This issue affects Creator LMS: from n/a through <= 1.1.18.	8.8	More Details
CVE-2026-24974	Deserialization of Untrusted Data vulnerability in NooTheme CitiLights noo-citilights allows Object Injection.This issue affects CitiLights: from n/a through <= 3.7.1.	8.8	More Details
CVE-2026-33713	n8n is an open source workflow automation platform. Prior to versions 2.14.1, 2.13.3, and 1.123.26, an authenticated user with permission to create or modify workflows could exploit a SQL injection vulnerability in the Data Table Get node. On default SQLite DB, single statements can be manipulated and the attack surface is practically limited. On PostgreSQL deployments, multi-statement execution is possible, enabling data modification and deletion. The issue has been fixed in n8n versions 1.123.26, 2.13.3, and 2.14.1. Users should upgrade to one of these versions or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations: Limit workflow creation and editing permissions to fully trusted users only, disable the Data Table node by adding `n8n-nodes-base.dataTable` to the `NODES_EXCLUDE` environment variable, and/or review existing workflows for Data Table Get nodes where `orderByColumn` is set to an expression that incorporates external or user-supplied input. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	8.8	More Details
CVE-2026-33696	n8n is an open source workflow automation platform. Prior to versions 2.14.1, 2.13.3, and 1.123.27, an authenticated user with permission to create or modify workflows could exploit a prototype pollution vulnerability in the XML and the GSuiteAdmin nodes. By supplying a crafted parameters as part of node configuration, an attacker could write attacker-controlled values onto `Object.prototype`. An attacker could use this prototype pollution to achieve remote code execution on the n8n instance. The issue has been fixed in n8n versions 2.14.1, 2.13.3, and 1.123.27. Users should upgrade to one of these versions or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations: Limit workflow creation and editing permissions to fully trusted users only, and/or disable the XML node by adding `n8n-nodes-base.xml` to the `NODES_EXCLUDE` environment variable. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	8.8	More Details
CVE-2026-24068	The VSL privileged helper does utilize NSXPC for IPC. The implementation of the "shouldAcceptNewConnection" function, which is used by the NSXPC framework to validate if a client should be allowed to connect to the XPC listener, does not validate clients at all. This means that any process can connect to this service using the configured protocol. A malicious process is able to call all the functions defined in the corresponding HelperToolProtocol. No validation is performed in the functions "writeReceiptFile" and “runUninstaller” of the HelperToolProtocol. This allows an attacker to write files to any location with any data as well as execute any file with any arguments. Any process can call these functions because of the missing XPC client validation described before. The abuse of the missing endpoint validation leads to privilege escalation.	8.8	More Details
CVE-2026-33660	n8n is an open source workflow automation platform. Prior to versions 2.14.1, 2.13.3, and 1.123.26, an authenticated user with permission to create or modify workflows could use the Merge node's "Combine by SQL" mode to read local files on the n8n host and achieve remote code execution. The AlaSQL sandbox did not sufficiently restrict certain SQL statements, allowing an attacker to access sensitive files on the server or even compromise the instance. The issue has been fixed in n8n versions 2.14.1, 2.13.3, and 1.123.26. Users should upgrade to one of these versions or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations: Limit workflow creation and editing permissions to fully trusted users only, and/or disable the Merge node by adding `n8n-nodes-base.merge` to the `NODES_EXCLUDE` environment variable. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	8.8	More Details
CVE-2026-33506	Ory Polis, formerly known as BoxyHQ Jackson, bridges or proxies a SAML login flow to OAuth 2.0 or OpenID Connect. Versions prior to 26.2.0 contain a DOM-based Cross-Site Scripting (XSS) vulnerability in Ory Polis's login functionality. The application improperly trusts a URL parameter (`callbackUrl`), which is passed to `router.push`. An attacker can craft a malicious link that, when opened by an authenticated user (or an unauthenticated user that later logs in), performs a client-side redirect and executes arbitrary JavaScript in the context of their browser. This could lead to credential theft, internal network pivoting, and unauthorized actions performed on behalf of the victim. Version 26.2.0 contains a patch for the issue.	8.8	More Details
CVE-2026-5213	A vulnerability was determined in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205. The affected element is the function cgi_adduser_to_session of the file /cgi-bin/account_mgr.cgi. This manipulation of the argument read_list causes stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-2931	The Amelia Booking plugin for WordPress is vulnerable to Insecure Direct Object References in versions up to, and including, 9.1.2. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resources. This makes it possible for authenticated attackers with customer-level permissions or above to change user passwords and potentially take over administrator accounts. The vulnerability is in the pro plugin, which has the same slug.	8.8	More Details
CVE-2025-15101	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in the Web management interface of certain ASUS router models. This vulnerability potentially allows actions to be performed with the existing privileges of an authenticated user on the affected device, including the ability to execute system commands through unintended mechanisms. Refer to the 'Security Update for ASUS Router Firmware' section on the ASUS Security Advisory for more information.	8.8	More Details
CVE-2026-20631	A logic issue was addressed with improved checks. This issue is fixed in macOS Tahoe 26.4. A user may be able to elevate privileges.	8.8	More Details
CVE-2026-5214	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205. Impacted is the function cgi_addgroup_get_group_quota_minsize of the file /cgi-bin/account_mgr.cgi. The manipulation of the argument Name results in stack-based buffer overflow. The attack may be performed from remote. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-24164	NVIDIA BioNeMo contains a vulnerability where a user could cause a deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, denial of service, information disclosure, and data tampering.	8.8	More Details

CVE-2025-67030	Directory Traversal vulnerability in the extractFile method of org.codehaus.plexus.util.Expand in plexus-utils before 6d780b3378829318ba5c2d29547e0012d5b29642. This allows an attacker to execute arbitrary code	8.8	More Details
CVE-2026-33991	WeGIA is a web manager for charitable institutions. Prior to version 3.6.7, the file `html/socio/sistema/deletar_tag.php` uses `extract($_REQUEST)` on line 14 and directly concatenates the `$id_tag` variable into SQL queries on lines 16-17 without prepared statements or sanitization. Version 3.6.7 patches the vulnerability.	8.8	More Details
CVE-2026-4840	A security flaw has been discovered in Netcore Power 15AX up to 3.0.0.6938. Affected by this issue is the function setTools of the file /bin/netis.cgi of the component Diagnostic Tool Interface. Performing a manipulation of the argument IpAddr results in os command injection. Remote exploitation of the attack is possible. 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.	8.8	More Details
CVE-2026-24976	Deserialization of Untrusted Data vulnerability in NooTheme Organici Library noo-organici-library allows Object Injection.This issue affects Organici Library: from n/a through <= 2.1.2.	8.8	More Details
CVE-2026-33348	OpenEMR is a free and open source electronic health records and medical practice management application. Users with the `Notes - my encounters` role can fill Eye Exam forms in patient encounters. The answers to the form are displayed on the encounter page and in the visit history for the users with the same role. Versions prior to 8.0.0.3 have a stored cross-site scripting (XSS) vulnerability in the function to display the form answers, allowing any authenticated attacker with the specific role to insert arbitrary JavaScript into the system by entering malicious payloads to the form answers. The JavaScript code is later executed by any user with the form role when viewing the form answers in the patient encounter pages or visit history. Version 8.0.0.3 contains a patch.	8.7	More Details
CVE-2026-28369	A flaw was found in Undertow. When Undertow receives an HTTP request where the first header line starts with one or more spaces, it incorrectly processes the request by stripping these leading spaces. This behavior, which violates HTTP standards, can be exploited by a remote attacker to perform request smuggling. Request smuggling allows an attacker to bypass security mechanisms, access restricted information, or manipulate web caches, potentially leading to unauthorized actions or data exposure.	8.7	More Details
CVE-2026-30587	Multiple Stored XSS vulnerabilities exist in Seafile Server version 13.0.15,13.0.16-pro,12.0.14 and prior and fixed in 13.0.17, 13.0.17-pro, and 12.0.20-pro, via the Seadoc (sdoc) editor. The application fails to properly sanitize WebSocket messages regarding document structure updates. This allows authenticated remote attackers to inject malicious JavaScript payloads via the src attribute of embedded Excalidraw whiteboards or the href attribute of anchor tags	8.7	More Details
CVE-2026-28368	A flaw was found in Undertow. This vulnerability allows a remote attacker to construct specially crafted requests where header names are parsed differently by Undertow compared to upstream proxies. This discrepancy in header interpretation can be exploited to launch request smuggling attacks, potentially bypassing security controls and accessing unauthorized resources.	8.7	More Details
CVE-2025-32957	baserCMS is a website development framework. Prior to version 5.2.3, the application's restore function allows users to upload a .zip file, which is then automatically extracted. A PHP file inside the archive is included using require_once without validating or restricting the filename. An attacker can craft a malicious PHP file within the zip and achieve arbitrary code execution when it is included. This issue has been patched in version 5.2.3.	8.7	More Details
CVE-2025-10551	A Stored Cross-site Scripting (XSS) vulnerability affecting Document Management in ENOVIA Collaborative Industry Innovator from Release 3DEXPERIENCE R2023x through Release 3DEXPERIENCE R2025x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2026-28367	A flaw was found in Undertow. A remote attacker can exploit this vulnerability by sending `\r\r\r` as a header block terminator. This can be used for request smuggling with certain proxy servers, such as older versions of Apache Traffic Server and Google Cloud Classic Application Load Balancer, potentially leading to unauthorized access or manipulation of web requests.	8.7	More Details
CVE-2026-33631	ClearanceKit intercepts file-system access events on macOS and enforces per-process access policies. In versions on the 4.1 branch and earlier, the opfilter Endpoint Security system extension enforced file access policy exclusively by intercepting ES_EVENT_TYPE_AUTH_OPEN events. Seven additional file operation event types were not intercepted, allowing any locally running process to bypass the configured FAA policy without triggering a denial. Commit a3d1733 adds subscriptions for all seven event types and routes them through the existing FAA policy evaluator. AUTH_RENAME and AUTH_UNLINK additionally preserve XProtect change detection: events on the XProtect path are allowed and trigger the existing onXProtectChanged callback rather than being evaluated against user policy. All versions on the 4.2 branch contain the fix. No known workarounds are available.	8.7	More Details
CVE-2025-10553	A Stored Cross-site Scripting (XSS) vulnerability affecting Factory Resource Management in DELMIA Factory Resource Manager from Release 3DEXPERIENCE R2023x through Release 3DEXPERIENCE R2025x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2026-20084	A vulnerability in the DHCP snooping feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause BOOTP packets to be forwarded between VLANs, resulting in a denial of service (DoS) condition. This vulnerability is due to improper handling of BOOTP packets on Cisco Catalyst 9000 Series Switches. An attacker could exploit this vulnerability by sending BOOTP request packets to an affected device. A successful exploit could allow an attacker to forward BOOTP packets from one VLAN to another, resulting in BOOTP VLAN leakage and potentially leading to high CPU utilization. This makes the device unreachable (either through console or remote management) and unable to forward traffic, resulting in a DoS condition. Note: This vulnerability can be exploited with either unicast or broadcast BOOTP packets. There are workarounds that address this vulnerability.	8.6	More Details
CVE-2026-32974	OpenClaw before 2026.3.12 contains an authentication bypass vulnerability in Feishu webhook mode when only verificationToken is configured without encryptKey, allowing acceptance of forged events. Unauthenticated network attackers can inject forged Feishu events and trigger downstream tool execution by reaching the webhook endpoint.	8.6	More Details
CVE-2026-20012	A vulnerability in the Internet Key Exchange version 2 (IKEv2) feature of Cisco IOS Software, Cisco IOS XE Software, Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a memory leak, resulting in a denial of service (DoS) condition on an affected device. This vulnerability is due to improper parsing of IKEv2 packets. An attacker could exploit this vulnerability by sending crafted IKEv2 packets to an affected device. A successful exploit of Cisco IOS Software and IOS XE Software could allow the attacker to cause the affected device to reload, resulting in a DoS condition. A successful exploit of Cisco Secure Firewall ASA Software and Secure FTD Software could allow the attacker to partially exhaust system memory, resulting in system instability, such as the inability to establish new IKEv2 VPN sessions. A manual reboot of the device is required to recover from this condition.	8.6	More Details
CVE-2026-31913	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Whitebox-Studio Scape scape allows Path Traversal.This issue affects Scape: from n/a through < 1.5.16.	8.6	More Details

CVE-2026-32857	Firecrawl version 2.8.0 and prior contain a server-side request forgery (SSRF) protection bypass vulnerability in the Playwright scraping service where network policy validation is applied only to the initial user-supplied URL and not to subsequent redirect destinations. Attackers can supply an externally valid URL that passes validation and returns an HTTP redirect to an internal or restricted resource, allowing the browser to follow the redirect and fetch the final destination without revalidation, thereby gaining access to internal network services and sensitive endpoints. This issue is distinct from CVE-2024-56800, which describes redirect-based SSRF generally. This vulnerability specifically arises from a post-redirect enforcement gap in implemented SSRF protections, where validation is applied only to the initial request and not to the final redirected destination.	8.6	More Details
CVE-2026-33955	Notesnook is a note-taking app. Prior to version 3.3.11 on Web/Desktop, a cross-site scripting vulnerability stored in the note history comparison viewer can escalate to remote code execution in a desktop application. The issue is triggered when an attacker-controlled note header is displayed using `dangerouslySetInnerHTML` without secure handling. When combined with the full backup and restore feature in the desktop application, this becomes remote code execution because Electron is configured with `nodeIntegration: true` and `contextIsolation: false`. Version 3.3.11 patches the issue.	8.6	More Details
CVE-2026-34585	SiYuan is a personal knowledge management system. Prior to version 3.6.2, a vulnerability allows crafted block attribute values to bypass server-side attribute escaping when an HTML entity is mixed with raw special characters. An attacker can embed a malicious IAL value inside a .sy document, package it as a .sy.zip, and have the victim import it through the normal Import -> SiYuan .sy.zip workflow. Once the note is opened, the malicious attribute breaks out of its original HTML context and injects an event handler, resulting in stored XSS. In the Electron desktop client, this XSS reaches remote code execution because injected JavaScript runs with access to Node/Electron APIs. This issue has been patched in version 3.6.2.	8.6	More Details
CVE-2026-22742	Spring AI's spring-ai-bedrock-converse contains a Server-Side Request Forgery (SSRF) vulnerability in BedrockProxyChatModel when processing multimodal messages that include user-supplied media URLs. Insufficient validation of those URLs allows an attacker to induce the server to issue HTTP requests to unintended internal or external destinations. This issue affects Spring AI: from 1.0.0 before 1.0.5, from 1.1.0 before 1.1.4.	8.6	More Details
CVE-2026-33661	Pay is an open-source payment SDK extension package for various Chinese payment services. Prior to version 3.7.20, the `verify_wechat_sign()` function in `src/Functions.php` unconditionally skips all signature verification when the PSR-7 request reports `localhost` as the host. An attacker can exploit this by sending a crafted HTTP request to the WeChat Pay callback endpoint with a `Host: localhost` header, bypassing the RSA signature check entirely. This allows forging fake WeChat Pay payment success notifications, potentially causing applications to mark orders as paid without actual payment. Version 3.7.20 fixes the issue.	8.6	More Details
CVE-2026-33216	NATS-Server is a High-Performance server for NATS.io, a cloud and edge native messaging system. Prior to versions 2.11.15 and 2.12.6, for MQTT deployments using usercodes/passwords: MQTT passwords are incorrectly classified as a non-authenticating identity statement (JWT) and exposed via monitoring endpoints. Versions 2.11.14 and 2.12.6 contain a fix. As a workaround, ensure monitoring end-points are adequately secured. Best practice remains to not expose the monitoring endpoint to the Internet or other untrusted network users.	8.6	More Details
CVE-2026-30976	Sonarr is a PVR for Usenet and BitTorrent users. In versions on the 4.x branch prior to 4.0.17.2950, an unauthenticated remote attacker can potentially read any file readable by the Sonarr process. These include application configuration files (containing API keys and database credentials), Windows system files, and any user-accessible files on the same drive This issue only impacts Windows systems; macOS and Linux are unaffected. Files returned from the API were not limited to the directory on disk they were intended to be served from. This problem has been patched in 4.0.17.2950 in the nightly/develop branch or 4.0.17.2952 for stable/main releases. It's possible to work around the issue by only hosting Sonarr on a secure internal network and accessing it via VPN, Tailscale or similar solution outside that network.	8.6	More Details
CVE-2026-32522	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in vanquish WooCommerce Support Ticket System woocommerce-support-ticket-system allows Path Traversal.This issue affects WooCommerce Support Ticket System: from n/a through < 18.5.	8.6	More Details
CVE-2026-20086	A vulnerability in the processing of Control and Provisioning of Wireless Access Points (CAPWAP) packets of Cisco IOS XE Wireless Controller Software for the Catalyst CW9800 Family could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of a malformed CAPWAP packet. An attacker could exploit this vulnerability by sending a malformed CAPWAP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload unexpectedly, resulting in a DoS condition.	8.6	More Details
CVE-2026-25007	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Element Invader ElementInvader Addons for Elementor elementinvader-addons-for-elementor allows Blind SQL Injection.This issue affects ElementInvader Addons for Elementor: from n/a through <= 1.4.2.	8.5	More Details
CVE-2026-32534	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in JoomSky JS Help Desk js-support-ticket allows Blind SQL Injection.This issue affects JS Help Desk: from n/a through <= 3.0.3.	8.5	More Details
CVE-2026-34352	In TigerVNC before 1.16.2, Image.cxx in x0vncserver allows other users to observe or manipulate the screen contents, or cause an application crash, because of incorrect permissions.	8.5	More Details
CVE-2025-69347	Authorization Bypass Through User-Controlled Key vulnerability in Convers Lab WPSubscription subscription allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPSubscription: from n/a through <= 1.8.10.	8.5	More Details
CVE-2026-27039	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AA-Team WZone woozone allows Blind SQL Injection.This issue affects WZone: from n/a through <= 14.0.31.	8.5	More Details
CVE-2026-33953	LinkAce is a self-hosted archive to collect website links. Versions prior to 2.5.3 block direct requests to private IP literals, but still performs server-side requests to internal-only resources when those resources are referenced through an internal hostname. This allows an authenticated user to trigger server-side requests to internal services reachable by the LinkAce server but not directly reachable by an external user. Version 2.5.3 patches the issue.	8.5	More Details
CVE-2026-24977	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NooTheme Organici Library noo-organici-library allows Blind SQL Injection.This issue affects Organici Library: from n/a through <= 2.1.2.	8.5	More Details
CVE-2026-25001	Improper Control of Generation of Code ('Code Injection') vulnerability in Saad Iqbal Post Snippets post-snippets allows Remote Code Inclusion.This issue affects Post Snippets: from n/a through <= 4.0.12.	8.5	More Details
	LibreChat is a ChatGPT clone with additional features. Prior to version 0.8.3, `isPrivateIP()` in `packages/api/src/auth/domain.ts` fails to detect		

CVE-2026-31943	IPv4-mapped IPv6 addresses in their hex-normalized form, allowing any authenticated user to bypass SSRF protection and make the server issue HTTP requests to internal network resources — including cloud metadata services (e.g., AWS `169.254.169.254`), loopback, and RFC1918 ranges. Version 0.8.3 fixes the issue.	8.5	More Details
CVE-2026-32516	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in kamleshyadav Miraculous Core Plugin miraculouscore allows Blind SQL Injection.This issue affects Miraculous Core Plugin: from n/a through < 2.1.2.	8.5	More Details
CVE-2018-25213	Nsauditor 3.0.28.0 contains a structured exception handling buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying malicious input to the DNS Lookup tool. Attackers can craft a payload with SEH chain overwrite and inject shellcode through the DNS Query field to achieve code execution with application privileges.	8.4	More Details
CVE-2018-25212	Boxoft wav-wma Converter 1.0 contains a local buffer overflow vulnerability in structured exception handling that allows attackers to execute arbitrary code by crafting malicious WAV files. Attackers can create a specially crafted WAV file with excessive data and ROP gadgets to overwrite the SEH chain and achieve code execution on Windows systems.	8.4	More Details
CVE-2016-20040	TiEmu 3.03-nogdb+dfsg-3 contains a buffer overflow vulnerability in the ROM parameter handling that allows local attackers to crash the application or execute arbitrary code. Attackers can supply an oversized ROM parameter to the tiemu command-line interface to overflow the stack buffer and overwrite the instruction pointer with malicious addresses.	8.4	More Details
CVE-2026-33572	OpenClaw before 2026.2.17 creates session transcript JSONL files with overly broad default permissions, allowing local users to read transcript contents. Attackers with local access can read transcript files to extract sensitive information including secrets from tool output.	8.4	More Details
CVE-2016-20037	xwpe 1.5.30a-2.1 and prior contains a stack-based buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying overly long input strings that exceed buffer boundaries. Attackers can craft malicious command-line arguments with 262 bytes of junk data followed by shellcode to overwrite the instruction pointer and achieve code execution or denial of service.	8.4	More Details
CVE-2016-20041	Yasr 0.6.9-5 contains a buffer overflow vulnerability that allows local attackers to crash the application or execute arbitrary code by supplying an oversized argument to the -p parameter. Attackers can invoke yasr with a crafted payload containing junk data, shellcode, and a return address to overwrite the stack and trigger code execution.	8.4	More Details
CVE-2016-20038	yTree 1.94-1.1 contains a stack-based buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying an excessively long argument to the application. Attackers can craft a malicious command-line argument containing shellcode and a return address to overwrite the stack and execute code in the application context.	8.4	More Details
CVE-2016-20042	TRN 3.6-23 contains a stack buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying an oversized argument to the application. Attackers can craft a malicious command-line argument with 156 bytes of padding followed by a return address to overwrite the instruction pointer and execute shellcode with user privileges.	8.4	More Details
CVE-2016-20043	NRSS RSS Reader 0.3.9-1 contains a stack buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying an oversized argument to the -F parameter. Attackers can craft a malicious input with 256 bytes of padding followed by a controlled EIP value to overwrite the return address and achieve code execution.	8.4	More Details
CVE-2016-20045	HNB Organizer 1.9.18-10 contains a local buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying an oversized argument to the -rc command-line parameter. Attackers can craft a malicious input string exceeding 108 bytes containing shellcode and a return address to overwrite the stack and achieve code execution.	8.4	More Details
CVE-2016-20046	zFTP Client 20061220+dfsg3-4.1 contains a buffer overflow vulnerability in the NAME parameter handling of FTP connections that allows local attackers to crash the application or execute arbitrary code. Attackers can supply an oversized NAME value exceeding the 80-byte buffer allocated in strcpy_chk to overwrite the instruction pointer and execute shellcode with user privileges.	8.4	More Details
CVE-2016-20047	EKG Gadu 1.9~pre+r2855-3+b1 contains a local buffer overflow vulnerability in the username handling that allows local attackers to execute arbitrary code by supplying an oversized username string. Attackers can trigger the overflow in the strlcpy function by passing a crafted buffer exceeding 258 bytes to overwrite the instruction pointer and execute shellcode with user privileges.	8.4	More Details
CVE-2016-20048	iSelect 1.4.0-2+b1 contains a local buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying an oversized value to the -k/--key parameter. Attackers can craft a malicious argument containing a NOP sled, shellcode, and return address to overflow a 1024-byte stack buffer and gain code execution with user privileges.	8.4	More Details
CVE-2026-32918	OpenClaw before 2026.3.11 contains a session sandbox escape vulnerability in the session_status tool that allows sandboxed subagents to access parent or sibling session state. Attackers can supply arbitrary sessionKey values to read or modify session data outside their sandbox scope, including persisted model overrides.	8.4	More Details
CVE-2017-20226	Mapscrn 2.0.3 contains a stack-based buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying an oversized input buffer. Attackers can craft a malicious buffer with junk data, return address, NOP instructions, and shellcode to overflow the stack and achieve code execution or denial of service.	8.4	More Details
CVE-2018-25217	PDF Explorer 1.5.66.2 contains a structured exception handler (SEH) overflow vulnerability that allows local attackers to execute arbitrary code by overwriting SEH records with malicious data. Attackers can craft a payload with buffer overflow, NSEH jump, and ROP gadget chains that execute when the Custom fields settings dialog processes the malicious input in the Label field.	8.4	More Details
CVE-2018-25222	SC v7.16 contains a stack-based buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying oversized input that exceeds buffer boundaries. Attackers can craft malicious input strings exceeding 1052 bytes to overwrite the instruction pointer and execute shellcode in the application context.	8.4	More Details
CVE-2018-25224	PMS 0.42 contains a stack-based buffer overflow vulnerability that allows local unauthenticated attackers to execute arbitrary code by supplying malicious values in the configuration file. Attackers can craft configuration files with oversized input that overflows the stack buffer and execute shell commands via return-oriented programming gadgets.	8.4	More Details
CVE-2018-25225	SIPP 3.3 contains a stack-based buffer overflow vulnerability that allows local unauthenticated attackers to execute arbitrary code by supplying malicious input in the configuration file. Attackers can craft a configuration file with oversized values that overflow a stack buffer, overwriting the return address and executing arbitrary code through return-oriented programming gadgets.	8.4	More Details
CVE-2026-33747	BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. Prior to version 0.28.1, when using a custom BuildKit frontend, the frontend can craft an API message that causes files to be written outside of the BuildKit state directory for the execution context. The issue has been fixed in v0.28.1. The vulnerability requires using an untrusted BuildKit frontend set with `#syntax` or `--build-arg BUILDKIT_SYNTAX`. Using these options with a well-known frontend image like `docker/dockerfile` is not affected.	8.4	More Details

CVE-2016-20039	Multi Emulator Super System 0.154-3.1 contains a buffer overflow vulnerability in the gamma parameter handling that allows local attackers to crash the application or execute arbitrary code. Attackers can supply an oversized gamma parameter value to overflow the stack buffer and overwrite the instruction pointer with a controlled address to achieve code execution.	8.4	More Details
CVE-2017-20228	Flat Assembler 1.71.21 contains a stack-based buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying oversized input to the application. Attackers can craft malicious assembly input exceeding 5895 bytes to overwrite the instruction pointer and execute return-oriented programming chains for shell command execution.	8.4	More Details
CVE-2016-20044	PInfo 0.6.9-5.1 contains a local buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying an oversized argument to the -m parameter. Attackers can craft a malicious input string with 564 bytes of padding followed by a return address to overwrite the instruction pointer and execute shellcode with user privileges.	8.4	More Details
CVE-2026-32920	OpenClaw before 2026.3.12 automatically discovers and loads plugins from .OpenClaw/extensions/ without explicit trust verification, allowing arbitrary code execution. Attackers can execute malicious code by including crafted workspace plugins in cloned repositories that execute when users run OpenClaw from the directory.	8.4	More Details
CVE-2018-25219	PassFab Excel Password Recovery 8.3.1 contains a structured exception handling buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious payload in the registration code field. Attackers can craft a buffer overflow payload with a pop-pop-ret gadget and shellcode that triggers code execution when pasted into the Licensed E-mail and Registration Code field during the registration process.	8.4	More Details
CVE-2026-23995	EVerest is an EV charging software stack. Prior to version 2026.02.0, stack-based buffer overflow in CAN interface initialization: passing an interface name longer than IFNAMSIZ (16) to CAN open routines overflows `ifreq.ifr_name`, corrupting adjacent stack data and enabling potential code execution. A malicious or misconfigured interface name can trigger this before any privilege checks. Version 2026.02.0 contains a patch.	8.4	More Details
CVE-2026-22593	EVerest is an EV charging software stack. Prior to version 2026.02.0, an off-by-one check in IsoMux certificate filename handling causes a stack-based buffer overflow when a filename length equals `MAX_FILE_NAME_LENGTH` (100). A crafted filename in the certificate directory can overflow `file_names[idx]`, corrupting stack state and enabling potential code execution. Version 2026.02.0 contains a patch.	8.4	More Details
CVE-2018-25218	PassFab RAR Password Recovery 9.3.2 contains a structured exception handler (SEH) buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious payload. Attackers can craft a payload with a buffer overflow, NSEH jump, and shellcode, then paste it into the 'Licensed E-mail and Registration Code' field during registration to trigger code execution.	8.4	More Details
CVE-2026-28832	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to disclose kernel memory.	8.4	More Details
CVE-2026-28821	A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to gain elevated privileges.	8.4	More Details
CVE-2019-25650	River Past CamDo 3.7.6 contains a structured exception handler (SEH) buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious string in the Lame_enc.dll name field. Attackers can craft a payload with a 280-byte buffer, NSEH jump instruction, and SEH handler address pointing to a pop-pop-ret gadget to trigger code execution and establish a bind shell on port 3110.	8.4	More Details
CVE-2026-32725	SciTokens C++ is a minimal library for creating and using SciTokens from C or C++. Prior to version 1.4.1, scitokens-cpp is vulnerable to an authorization bypass when processing path-based scopes in tokens. The library normalizes the scope path from the token before authorization and collapses ".." path components instead of rejecting them. As a result, an attacker can use parent-directory traversal in the scope claim to broaden the effective authorization beyond the intended directory. This issue has been patched in version 1.4.1.	8.3	More Details
CVE-2019-25651	Ubiquiti UniFi Network Controller prior to 5.10.12 (excluding 5.6.42), UAP FW prior to 4.0.6, UAP-AC, UAP-AC v2, and UAP-AC Outdoor FW prior to 3.8.17, USW FW prior to 4.0.6, USG FW prior to 4.4.34 uses AES-CBC encryption for device-to-controller communication, which contains cryptographic weaknesses that allow attackers to recover encryption keys from captured traffic. Attackers with adjacent network access can capture sufficient encrypted traffic and exploit AES-CBC mode vulnerabilities to derive the encryption keys, enabling unauthorized control and management of network devices.	8.3	More Details
CVE-2026-0562	A critical security vulnerability in parisneo/lollms versions up to 2.2.0 allows any authenticated user to accept or reject friend requests belonging to other users. The `respond_request()` function in `backend/routers/friends.py` does not implement proper authorization checks, enabling Insecure Direct Object Reference (IDOR) attacks. Specifically, the `/api/friends/requests/{friendship_id}` endpoint fails to verify whether the authenticated user is part of the friendship or the intended recipient of the request. This vulnerability can lead to unauthorized access, privacy violations, and potential social engineering attacks. The issue has been addressed in version 2.2.0.	8.3	More Details
CVE-2025-55262	HCL Aftermarket DPC is affected by SQL Injection which allows attacker to exploit this vulnerability to retrieve sensitive information from the database.	8.3	More Details
CVE-2026-33980	Azure Data Explorer MCP Server is a Model Context Protocol (MCP) server that enables AI assistants to execute KQL queries and explore Azure Data Explorer (ADX/Kusto) databases through standardized interfaces. Versions up to and including 0.1.1 contain KQL (Kusto Query Language) injection vulnerabilities in three MCP tool handlers: `get_table_schema`, `sample_table_data`, and `get_table_details`. The `table_name` parameter is interpolated directly into KQL queries via f-strings without any validation or sanitization, allowing an attacker (or a prompt-injected AI agent) to execute arbitrary KQL queries against the Azure Data Explorer cluster. Commit 0abe0ee55279e111281076393e5e966335fffd30 patches the issue.	8.3	More Details
CVE-2026-30534	A SQL Injection vulnerability exists in SourceCodester Online Food Ordering System v1.0 in admin/manage_category.php via the "id" parameter.	8.3	More Details
CVE-2026-24148	NVIDIA Jetson for JetPack contains a vulnerability in the system initialization logic, where an unprivileged attacker could cause the initialization of a resource with an insecure default. A successful exploit of this vulnerability might lead to information disclosure of encrypted data, data tampering, and partial denial of service across devices sharing the same machine ID.	8.3	More Details
CVE-2026-34504	OpenClaw before 2026.3.28 contains a server-side request forgery vulnerability in the fal provider image-generation-provider.ts component that allows attackers to fetch internal URLs. A malicious or compromised fal relay can exploit unguarded image download fetches to expose internal service metadata and responses through the image pipeline.	8.3	More Details
CVE-	Botan is a C++ cryptography library. From version 2.3.0 to before version 3.11.0, during SM2 decryption, the code that checked the		

2026-32877	authentication code value (C3) failed to check that the encoded value was of the expected length prior to comparison. An invalid ciphertext can cause a heap over-read of up to 31 bytes, resulting in a crash or potentially other undefined behavior. This issue has been patched in version 3.11.0.	8.2	More Details
CVE-2026-33941	Handlebars provides the power necessary to let users build semantic templates. In versions 4.0.0 through 4.7.8, the Handlebars CLI precompiler (`bin/handlebars` / `lib/precompiler.js`) concatenates user-controlled strings — template file names and several CLI options — directly into the JavaScript it emits, without any escaping or sanitization. An attacker who can influence template filenames or CLI arguments can inject arbitrary JavaScript that executes when the generated bundle is loaded in Node.js or a browser. Version 4.7.9 fixes the issue. Some workarounds are available. First, validate all CLI inputs before invoking the precompiler. Reject filenames and option values that contain characters with JavaScript string-escaping significance (`"`, `'`, `;`, etc.). Second, use a fixed, trusted namespace string passed via a configuration file rather than command-line arguments in automated pipelines. Third, run the precompiler in a sandboxed environment (container with no write access to sensitive paths) to limit the impact of successful exploitation. Fourth, audit template filenames in any repository or package that is consumed by an automated build pipeline.	8.2	More Details
CVE-2026-33009	EVerest is an EV charging software stack. Versions prior to 2026.02.0 have a data race leading to C++ UB (potential memory corruption). This is triggered by an MQTT `everest_external/nodered/{connector}/cmd/switch_three_phases_while_charging` message and results in `Charger::shared_context` / `internal_context` accessed concurrently without lock. Version 2026.02.0 contains a patch.	8.2	More Details
CVE-2026-31921	Missing Authorization vulnerability in Devteam HaywoodTech Product Rearrange for WooCommerce products-rearrange-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Product Rearrange for WooCommerce: from n/a through <= 1.2.2.	8.2	More Details
CVE-2024-58341	OpenCart Core 4.0.2.3 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'search' parameter. Attackers can send GET requests to the product search endpoint with malicious 'search' values to extract sensitive database information using boolean-based blind or time-based blind SQL injection techniques.	8.2	More Details
CVE-2018-25183	Shipping System CMS 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to bypass authentication by injecting SQL code through the username parameter. Attackers can submit malicious SQL payloads using boolean-based blind techniques in POST requests to the admin login endpoint to authenticate without valid credentials.	8.2	More Details
CVE-2026-2072	Cross-Site Scripting vulnerability in Hitachi Infrastructure Analytics Advisor (Analytics probe component), Hitachi Ops Center Analyzer.This issue affects Hitachi Infrastructure Analytics Advisor:; Hitachi Ops Center Analyzer: from 10.0.0-00 before 11.0.5-00.	8.2	More Details
CVE-2018-25185	Wecodex Restaurant CMS 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the username parameter. Attackers can send POST requests to the login endpoint with malicious SQL payloads using boolean-based blind or time-based blind techniques to extract sensitive database information.	8.2	More Details
CVE-2018-25195	Wecodex Hotel CMS 1.0 contains an SQL injection vulnerability in the admin login functionality that allows unauthenticated attackers to bypass authentication by injecting SQL code. Attackers can submit malicious SQL payloads through the username parameter in POST requests to index.php with action=processlogin to extract sensitive database information or gain unauthorized administrative access.	8.2	More Details
CVE-2026-34042	act is a project which allows for local running of github actions. Prior to version 0.2.86, act's built in actions/cache server listens to connections on all interfaces and allows anyone who can connect to it including someone anywhere on the internet to create caches with arbitrary keys and retrieve all existing caches. If they can predict which cache keys will be used by local actions, they can create malicious caches containing whatever files they please most likely allowing arbitrary remote code execution within the docker container. This issue has been patched in version 0.2.86.	8.2	More Details
CVE-2026-34375	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the YPTWallet Stripe payment confirmation page directly echoes the `$_REQUEST['plugin']` parameter into a JavaScript block without any encoding or sanitization. The `plugin` parameter is not included in any of the framework's input filter lists defined in `security.php`, so it passes through completely raw. An attacker can inject arbitrary JavaScript by crafting a malicious URL and sending it to a victim user. The same script block also outputs the current user's username and password hash via `User::getUserName()` and `User::getUserPass()`, meaning a successful XSS exploitation can immediately exfiltrate these credentials. Commit fa0bc102493a15d79fe03f86c07ab7ca1b5b63e2 fixes the issue.	8.2	More Details
CVE-2018-25209	OpenBiz Cubi Lite 3.0.8 contains a SQL injection vulnerability in the login form that allows unauthenticated attackers to manipulate database queries through the username parameter. Attackers can submit POST requests to /bin/controller.php with malicious SQL code in the username field to extract sensitive database information or bypass authentication.	8.2	More Details
CVE-2018-25202	SAT CFDI 3.3 contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the 'id' parameter in the signIn endpoint. Attackers can submit POST requests with boolean-based blind, stacked queries, or time-based blind SQL injection payloads to extract sensitive data or compromise the application.	8.2	More Details
CVE-2018-25210	WebOfisi E-Ticaret 4.0 contains an SQL injection vulnerability in the 'urun' GET parameter of the endpoint that allows unauthenticated attackers to manipulate database queries. Attackers can inject SQL payloads through the 'urun' parameter to execute boolean-based blind, error-based, time-based blind, and stacked query attacks against the backend database.	8.2	More Details
CVE-2026-4984	The Twilio integration webhook handler accepts any POST request without validating Twilio's 'X-Twilio-Signature'. When processing media messages, it fetches user-controlled URLs ('MediaUrlN' parameters) using HTTP requests that include the integration's Twilio credentials in the 'Authorization' header. An attacker can forge a webhook payload pointing to their own server and receive the victim's 'accountSID' and 'authToken' in plaintext (base64-encoded Basic Auth), leading to full compromise of the Twilio account.	8.2	More Details
CVE-2026-29872	A cross-session information disclosure vulnerability exists in the awesome-llm-apps project in commit e46690f99c3f08be80a9877fab52acacf7ab8251 (2026-01-19). The affected Streamlit-based GitHub MCP Agent stores user-supplied API tokens in process-wide environment variables using os.environ without proper session isolation. Because Streamlit serves multiple concurrent users from a single Python process, credentials provided by one user remain accessible to subsequent unauthenticated users. An attacker can exploit this issue to retrieve sensitive information such as GitHub Personal Access Tokens or LLM API keys, potentially leading to unauthorized access to private resources and financial abuse.	8.2	More Details
CVE-2018-25204	Library CMS 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to bypass authentication by injecting SQL code through the username parameter. Attackers can send POST requests to the admin login endpoint with boolean-based blind SQL injection payloads in the username field to manipulate database queries and gain unauthorized access.	8.2	More Details
CVE-2018-25208	qdPM 9.1 contains an SQL injection vulnerability that allows unauthenticated attackers to extract database information by injecting SQL code through filter_by parameters. Attackers can submit malicious POST requests to the timeReport endpoint with crafted filter_by[CommentCreatedFrom] and filter_by[CommentCreatedTo] parameters to execute arbitrary SQL queries and retrieve sensitive data.	8.2	More Details
CVE-	KomSeo Cart 1.3 contains an SQL injection vulnerability that allows attackers to inject SQL commands through the 'my_item_search' parameter		More

2018-25206	in edit.php. Attackers can submit POST requests with malicious SQL payloads to extract sensitive database information using boolean-based blind or error-based injection techniques.	8.2	Details
CVE-2018-25203	Online Store System CMS 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the email parameter. Attackers can send POST requests to index.php with the action=clientaccess parameter using boolean-based blind or time-based blind SQL injection payloads in the email field to extract sensitive database information.	8.2	More Details
CVE-2026-33979	Express XSS Sanitizer is Express 4.x and 5.x middleware which sanitizes user input data (in req.body, req.query, req.headers and req.params) to prevent Cross Site Scripting (XSS) attack. A vulnerability has been identified in versions prior to 2.0.2 where restrictive sanitization configurations are silently ignored. In version 2.0.2, the validation logic has been updated to respect explicitly provided empty configurations. Now, if allowedTags or allowedAttributes are provided (even if empty), they are passed directly to sanitize-html without being overridden.	8.2	More Details
CVE-2018-25205	ASP.NET jVideo Kit 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to inject SQL commands through the 'query' parameter in the search functionality. Attackers can submit malicious SQL payloads via GET or POST requests to the /search endpoint to extract sensitive database information using boolean-based blind or error-based techniques.	8.2	More Details
CVE-2025-41368	Problem in the Small HTTP Server v3.06.36 service. An authenticated path traversal vulnerability in '/' allows remote users to bypass the intended restrictions of SecurityManager and display any file if they have the appropriate permissions outside the document root configured on the server.	8.1	More Details
CVE-2026-22495	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Greenville greenville allows PHP Local File Inclusion.This issue affects Greenville: from n/a through <= 1.3.2.	8.1	More Details
CVE-2026-22494	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Good Homes good-homes allows PHP Local File Inclusion.This issue affects Good Homes: from n/a through <= 1.3.13.	8.1	More Details
CVE-2026-22493	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Gaspard gaspard allows PHP Local File Inclusion.This issue affects Gaspard: from n/a through <= 1.3.	8.1	More Details
CVE-2026-33468	Kysely is a type-safe TypeScript SQL query builder. Prior to version 0.28.14, Kysely's `DefaultQueryCompiler.sanitizeStringLiteral()` only escapes single quotes by doubling them (`'` → `''`) but does not escape backslashes. When used with the MySQL dialect (where `NO_BACKSLASH_ESCAPES` is OFF by default), an attacker can use a backslash to escape the trailing quote of a string literal, breaking out of the string context and injecting arbitrary SQL. This affects any code path that uses `ImmediateValueTransformer` to inline values — specifically `CreateIndexBuilder.where()` and `CreateViewBuilder.as()`. Version 0.28.14 contains a fix.	8.1	More Details
CVE-2026-25382	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in jwsthemes IdealAuto idealauto allows PHP Local File Inclusion.This issue affects IdealAuto: from n/a through < 3.8.6.	8.1	More Details
CVE-2026-34503	OpenClaw before 2026.3.28 fails to disconnect active WebSocket sessions when devices are removed or tokens are revoked. Attackers with revoked credentials can maintain unauthorized access through existing live sessions until forced reconnection.	8.1	More Details
CVE-2026-25379	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in jwsthemes StreamVid streamvid allows PHP Local File Inclusion.This issue affects StreamVid: from n/a through < 6.8.6.	8.1	More Details
CVE-2026-33989	Mobile Next is an MCP server for mobile development and automation. Prior to version 0.0.49, the `@mobilenext/mobile-mcp` server contains a Path Traversal vulnerability in the `mobile_save_screenshot` and `mobile_start_screen_recording` tools. The `saveTo` and `output` parameters were passed directly to filesystem operations without validation, allowing an attacker to write files outside the intended workspace. Version 0.0.49 fixes the issue.	8.1	More Details
CVE-2026-25380	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in jwsthemes Feedy feedy allows PHP Local File Inclusion.This issue affects Feedy: from n/a through < 2.1.5.	8.1	More Details
CVE-2026-22496	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Hypnotherapy hypnotherapy allows PHP Local File Inclusion.This issue affects Hypnotherapy: from n/a through <= 1.2.10.	8.1	More Details
CVE-2026-33442	Kysely is a type-safe TypeScript SQL query builder. In versions 0.28.12 and 0.28.13, the `sanitizeStringLiteral` method in Kysely's query compiler escapes single quotes (`'` → `''`) but does not escape backslashes. On MySQL with the default `BACKSLASH_ESCAPES` SQL mode, an attacker can inject a backslash before a single quote to neutralize the escaping, breaking out of the JSON path string literal and injecting arbitrary SQL. Version 0.28.14 fixes the issue.	8.1	More Details
CVE-2026-25381	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in jwsthemes LoveDate lovedate allows PHP Local File Inclusion.This issue affects LoveDate: from n/a through < 3.8.6.	8.1	More Details
CVE-2026-22505	Deserialization of Untrusted Data vulnerability in AncoraThemes Morning Records morning-records allows Object Injection.This issue affects Morning Records: from n/a through <= 1.2.	8.1	More Details
CVE-2026-22498	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Laurent laurent allows PHP Local File Inclusion.This issue affects Laurent: from n/a through <= 3.1.	8.1	More Details
CVE-2026-22499	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Lella lella allows PHP Local File Inclusion.This issue affects Lella: from n/a through <= 1.2.	8.1	More Details
CVE-2026-25017	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in stmcan NaturaLife Extensions naturalife-extensions allows PHP Local File Inclusion.This issue affects NaturaLife Extensions: from n/a through <= 2.1.	8.1	More Details

CVE-2026-33149	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. Versions up to and including 2.5.3 set ALLOWED_HOSTS = '*' by default, which causes Django to accept any value in the HTTP Host header without validation. The application uses request.build_absolute_uri() to generate absolute URLs in multiple contexts, including invite link emails, API pagination, and OpenAPI schema generation. An attacker who can send requests to the application with a crafted Host header can manipulate all server-generated absolute URLs. The most critical impact is invite link poisoning: when an admin creates an invite and the application sends the invite email, the link points to the attacker's server instead of the real application. When the victim clicks the link, the invite token is sent to the attacker, who can then use it at the real application. As of time of publication, it is unknown if a patched version is available.	8.1	More Details
CVE-2026-3857	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.10 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1 that could have allowed an unauthenticated user to execute arbitrary GraphQL mutations on behalf of authenticated users due to insufficient CSRF protection.	8.1	More Details
CVE-2026-25334	Incorrect Privilege Assignment vulnerability in wordpresschef Salon Booking System Pro salon-booking-plugin-pro allows Privilege Escalation.This issue affects Salon Booking System Pro: from n/a through < 10.30.12.	8.1	More Details
CVE-2026-33496	ORY Oathkeeper is an Identity & Access Proxy (IAP) and Access Control Decision API that authorizes HTTP requests based on sets of Access Rules. Versions prior to 26.2.0 are vulnerable to authentication bypass due to cache key confusion. The `oauth2_introspection` authenticator cache does not distinguish tokens that were validated with different introspection URLs. An attacker can therefore legitimately use a token to prime the cache, and subsequently use the same token for rules that use a different introspection server. Ory Oathkeeper has to be configured with multiple `oauth2_introspection` authenticator servers, each accepting different tokens. The authenticators also must be configured to use caching. An attacker has to have a way to gain a valid token for one of the configured introspection servers. Starting in version 26.2.0, Ory Oathkeeper includes the introspection server URL in the cache key, preventing confusion of tokens. Update to the patched version of Ory Oathkeeper. If that is not immediately possible, disable caching for `oauth2_introspection` authenticators.	8.1	More Details
CVE-2026-32531	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in gavias Kunco kunco allows PHP Local File Inclusion.This issue affects Kunco: from n/a through < 1.4.5.	8.1	More Details
CVE-2026-34055	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, the legacy patient notes functions in `library/pnotes.inc.php` perform updates and deletes using `WHERE id = ?` without verifying that the note belongs to a patient the user is authorized to access. Multiple web UI callers pass user-controlled note IDs directly to these functions. This is the same class of vulnerability as CVE-2026-25745 (REST API IDOR), but affects the web UI code paths. Version 8.0.0.3 patches the issue.	8.1	More Details
CVE-2026-34394	WWBN AVideo is an open source video platform. In versions 26.0 and prior, AVideo's admin plugin configuration endpoint (admin/save.json.php) lacks any CSRF token validation. There is no call to isGlobalTokenValid() or verifyToken() before processing the request. Combined with the application's explicit SameSite=None cookie policy, an attacker can forge cross-origin POST requests from a malicious page to overwrite arbitrary plugin settings on a victim administrator's session. Because the plugins table is included in the ignoreTableSecurityCheck() array in objects/Object.php, standard table-level access controls are also bypassed. This allows a complete takeover of platform functionality by reconfiguring payment processors, authentication providers, cloud storage credentials, and more. At time of publication, there are no publicly available patches.	8.1	More Details
CVE-2026-24373	Incorrect Privilege Assignment vulnerability in Metagauss RegistrationMagic custom-registration-form-builder-with-submission-manager allows Privilege Escalation.This issue affects RegistrationMagic: from n/a through <= 6.0.7.1.	8.1	More Details
CVE-2026-25357	Authentication Bypass Using an Alternate Path or Channel vulnerability in azzaroco Ultimate Membership Pro indeed-membership-pro allows Authentication Abuse.This issue affects Ultimate Membership Pro: from n/a through <= 13.7.	8.1	More Details
CVE-2026-28817	A race condition was addressed with improved state handling. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. A sandboxed process may be able to circumvent sandbox restrictions.	8.1	More Details
CVE-2026-4800	Impact: The fix for CVE-2021-23337 (https://github.com/advisories/GHSA-35jh-r3h4-6jhm) added validation for the variable option in _.template but did not apply the same validation to options.imports key names. Both paths flow into the same Function() constructor sink. When an application passes untrusted input as options.imports key names, an attacker can inject default-parameter expressions that execute arbitrary code at template compilation time. Additionally, _.template uses assignInWith to merge imports, which enumerates inherited properties via for..in. If Object.prototype has been polluted by any other vector, the polluted keys are copied into the imports object and passed to Function(). Patches: Users should upgrade to version 4.18.0. Workarounds: Do not pass untrusted input as key names in options.imports. Only use developer-controlled, static key names.	8.1	More Details
CVE-2026-32726	SciTokens C++ is a minimal library for creating and using SciTokens from C or C++. Prior to version 1.4.1, scitokens-cpp is vulnerable to an authorization bypass in path-based scope validation. The enforcer used a simple string-prefix comparison when checking whether a requested resource path was covered by a token's authorized scope path. Because the check did not require a path-segment boundary, a token scoped to one path could incorrectly authorize access to sibling paths that merely started with the same prefix. This issue has been patched in version 1.4.1.	8.1	More Details
CVE-2026-22516	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Wizor's wizors-investments allows PHP Local File Inclusion.This issue affects Wizor's: from n/a through <= 2.12.	8.1	More Details
CVE-2026-22515	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes VegaDays vegadays allows PHP Local File Inclusion.This issue affects VegaDays: from n/a through <= 1.2.0.	8.1	More Details
CVE-2026-22514	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Unica unica allows PHP Local File Inclusion.This issue affects Unica: from n/a through <= 1.4.1.	8.1	More Details
CVE-2026-22513	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Triompher triompher allows PHP Local File Inclusion.This issue affects Triompher: from n/a through <= 1.1.0.	8.1	More Details
CVE-2026-22512	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Roisin roisin allows PHP Local File Inclusion.This issue affects Roisin: from n/a through <= 1.2.1.	8.1	More Details

CVE-2026-22511	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes NeoBeat neobeat allows PHP Local File Inclusion.This issue affects NeoBeat: from n/a through <= 1.2.	8.1	More Details
CVE-2026-22510	Deserialization of Untrusted Data vulnerability in AncoraThemes Melody melodyschool allows Object Injection.This issue affects Melody: from n/a through <= 1.6.3.	8.1	More Details
CVE-2026-22509	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Gioia gioia allows PHP Local File Inclusion.This issue affects Gioia: from n/a through <= 1.4.	8.1	More Details
CVE-2026-22508	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Dentalux dentalux allows PHP Local File Inclusion.This issue affects Dentalux: from n/a through <= 3.3.	8.1	More Details
CVE-2026-22506	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Amoli amoli allows PHP Local File Inclusion.This issue affects Amoli: from n/a through <= 1.0.	8.1	More Details
CVE-2026-32504	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CreativeWS VintWood vintwood allows PHP Local File Inclusion.This issue affects VintWood: from n/a through <= 1.1.8.	8.1	More Details
CVE-2026-22504	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX ProLingua prolingua allows PHP Local File Inclusion.This issue affects ProLingua: from n/a through <= 1.1.12.	8.1	More Details
CVE-2026-22503	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Nelson nelson allows PHP Local File Inclusion.This issue affects Nelson: from n/a through <= 1.2.0.	8.1	More Details
CVE-2026-22502	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Mr. Cobbler mr-cobbler allows PHP Local File Inclusion.This issue affects Mr. Cobbler: from n/a through <= 1.1.9.	8.1	More Details
CVE-2026-32505	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CreativeWS Kiddy kiddy allows PHP Local File Inclusion.This issue affects Kiddy: from n/a through <= 2.0.8.	8.1	More Details
CVE-2026-27079	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Amfissa amfissa allows PHP Local File Inclusion.This issue affects Amfissa: from n/a through <= 1.1.	8.1	More Details
CVE-2026-33579	OpenClaw before 2026.3.28 contains a privilege escalation vulnerability in the /pair approve command path that fails to forward caller scopes into the core approval check. A caller with pairing privileges but without admin privileges can approve pending device requests asking for broader scopes including admin access by exploiting the missing scope validation in extensions/device-pair/index.ts and src/infra/device-pairing.ts.	8.1	More Details
CVE-2026-25458	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Moments moments allows PHP Local File Inclusion.This issue affects Moments: from n/a through <= 2.2.	8.1	More Details
CVE-2026-27048	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes The Aisle Core theaisle-core allows PHP Local File Inclusion.This issue affects The Aisle Core: from n/a through <= 2.0.5.	8.1	More Details
CVE-2026-27047	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Curly Core curly-core allows PHP Local File Inclusion.This issue affects Curly Core: from n/a through <= 2.1.6.	8.1	More Details
CVE-2025-12805	A flaw was found in Red Hat OpenShift AI (RHOAI) llama-stack-operator. This vulnerability allows unauthorized access to Llama Stack services deployed in other namespaces via direct network requests, because no NetworkPolicy restricts access to the llama-stack service endpoint. As a result, a user in one namespace can access another user's Llama Stack instance and potentially view or manipulate sensitive data.	8.1	More Details
CVE-2026-29187	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, a Blind SQL Injection vulnerability exists in the Patient Search functionality (/interface/new/new_search_popup.php). The vulnerability allows an authenticated attacker to execute arbitrary SQL commands by manipulating the HTTP parameter keys rather than the values. Version 8.0.0.3 contains a patch.	8.1	More Details
CVE-2026-33938	Handlebars provides the power necessary to let users build semantic templates. In versions 4.0.0 through 4.7.8, the `@partial-block` special variable is stored in the template data context and is reachable and mutable from within a template via helpers that accept arbitrary objects. When a helper overwrites `@partial-block` with a crafted Handlebars AST, a subsequent invocation of `{{> @partial-block}}` compiles and executes that AST, enabling arbitrary JavaScript execution on the server. Version 4.7.9 fixes the issue. Some workarounds are available. First, use the runtime-only build (`require('handlebars/runtime')`). The `compile()` method is absent, eliminating the vulnerable fallback path. Second, audit registered helpers for any that write arbitrary values to context objects. Helpers should treat context data as read-only. Third, avoid registering helpers from third-party packages (such as `handlebars-helpers`) in contexts where templates or context data can be influenced by untrusted input.	8.1	More Details
CVE-2025-55261	HCL Aftermarket DPC is affected by Missing Functional Level Access Control which will allow attacker to escalate his privileges and may compromise the application and may steal and manipulate the data.	8.1	More Details
CVE-2026-30975	Sonarr is a PVR for Usenet and BitTorrent users. Versions prior to 4.0.16.2942 have an authentication bypass that affected users that had disabled authentication for local addresses (Authentication Required set to: `Disabled for Local Addresses`) without a reverse proxy running in front of Sonarr that didn't not pass through the invalid header. Patches are available in version 4.0.16.2942 in the nightly/develop branch and version 4.0.16.2944 for stable/main releases. Some workarounds are available. Make sure Sonarr's Authentication Required setting is set to	8.1	More Details

	`Enabled`, run Sonarr behind a reverse proxy, and/or do not expose Sonarr directly to the internet and instead rely on accessing it through a VPN, Tailscale or a similar solution.		
CVE-2026-25457	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Mixtape mixtape allows PHP Local File Inclusion.This issue affects Mixtape: from n/a through <= 2.1.	8.1	More Details
CVE-2026-2370	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 14.3 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1 affecting Jira Connect installations that could have allowed an authenticated user with minimal workspace permissions to obtain installation credentials and impersonate the GitLab app due to improper authorization checks.	8.1	More Details
CVE-2026-27081	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Rosebud rosebud allows PHP Local File Inclusion.This issue affects Rosebud: from n/a through <= 1.4.	8.1	More Details
CVE-2026-33940	Handlebars provides the power necessary to let users build semantic templates. In versions 4.0.0 through 4.7.8, a crafted object placed in the template context can bypass all conditional guards in `resolvePartial()` and cause `invokePartial()` to return `undefined`. The Handlebars runtime then treats the unresolved partial as a source that needs to be compiled, passing the crafted object to `env.compile()`. Because the object is a valid Handlebars AST containing injected code, the generated JavaScript executes arbitrary commands on the server. The attack requires the adversary to control a value that can be returned by a dynamic partial lookup. Version 4.7.9 fixes the issue. Some workarounds are available. First, use the runtime-only build (`require('handlebars/runtime')`). Without `compile()`, the fallback compilation path in `invokePartial` is unreachable. Second, sanitize context data before rendering: Ensure no value in the context is a non-primitive object that could be passed to a dynamic partial. Third, avoid dynamic partial lookups (`{{> (lookup ...)}}`) when context data is user-controlled.	8.1	More Details
CVE-2026-32488	Incorrect Privilege Assignment vulnerability in wpeverest User Registration user-registration allows Privilege Escalation.This issue affects User Registration: from n/a through <= 4.4.9.	8.1	More Details
CVE-2026-32716	SciTokens is a reference library for generating and using SciTokens. Prior to version 1.9.6, the Enforcer incorrectly validates scope paths by using a simple prefix match (startswith). This allows a token with access to a specific path (e.g., /john) to also access sibling paths that start with the same prefix (e.g., /johnathan, /johnny), which is an Authorization Bypass. This issue has been patched in version 1.9.6.	8.1	More Details
CVE-2026-32727	SciTokens is a reference library for generating and using SciTokens. Prior to version 1.9.7, the Enforcer is vulnerable to a path traversal attack where an attacker can use dot-dot (..) in the scope claim of a token to escape the intended directory restriction. This occurs because the library normalizes both the authorized path (from the token) and the requested path (from the application) before comparing them using startswith. This issue has been patched in version 1.9.7.	8.1	More Details
CVE-2026-25464	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in TieLabs Jannah jannah allows PHP Local File Inclusion.This issue affects Jannah: from n/a through <= 7.6.3.	8.1	More Details
CVE-2024-14031	Sereal::Encoder versions from 4.000 through 4.009_002 for Perl is vulnerable to a buffer overwrite flaw in the Zstandard library. Sereal::Encoder embeds a version of the Zstandard (zstd) library that is vulnerable to CVE-2019-11922. This is a race condition in the one-pass compression functions of Zstandard prior to version 1.3.8 could allow an attacker to write bytes out of bounds if an output buffer smaller than the recommended size was used.	8.1	More Details
CVE-2024-14030	Sereal::Decoder versions from 4.000 through 4.009_002 for Perl is vulnerable to a buffer overwrite flaw in the Zstandard library. Sereal::Decoder embeds a version of the Zstandard (zstd) library that is vulnerable to CVE-2019-11922. This is a race condition in the one-pass compression functions of Zstandard prior to version 1.3.8 could allow an attacker to write bytes out of bounds if an output buffer smaller than the recommended size was used.	8.1	More Details
CVE-2026-32503	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CreativeWS Trendustry trendustry allows PHP Local File Inclusion.This issue affects Trendustry: from n/a through <= 1.1.4.	8.1	More Details
CVE-2026-4415	Gigabyte Control Center developed by GIGABYTE has an Arbitrary File Write vulnerability. When the pairing feature is enabled, unauthenticated remote attackers can write arbitrary files to any location on the underlying operating system, leading to arbitrary code execution or privilege escalation.	8.1	More Details
CVE-2026-28891	A race condition was addressed with additional validation. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to break out of its sandbox.	8.1	More Details
CVE-2026-27077	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes MultiOffice multioffice allows PHP Local File Inclusion.This issue affects MultiOffice: from n/a through <= 1.2.	8.1	More Details
CVE-2026-33577	OpenClaw before 2026.3.28 contains an insufficient scope validation vulnerability in the node pairing approval path that allows low-privilege operators to approve nodes with broader scopes. Attackers can exploit missing callerScopes validation in node-pairing.ts to extend privileges onto paired nodes beyond their authorization level.	8.1	More Details
CVE-2026-27075	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Belfort belfort allows PHP Local File Inclusion.This issue affects Belfort: from n/a through <= 1.0.	8.1	More Details
CVE-2026-32500	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CreativeWS MetaMax metamax allows PHP Local File Inclusion.This issue affects MetaMax: from n/a through <= 1.1.4.	8.1	More Details
CVE-2026-27076	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes LuxeDrive luxedrive allows PHP Local File Inclusion.This issue affects LuxeDrive: from n/a through <= 1.0.	8.1	More Details
CVE-2026-27078	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Emaurri emaurri allows PHP Local File Inclusion.This issue affects Emaurri: from n/a through <= 1.0.1.	8.1	More Details
CVE-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes		More

2026-27080	Deston deston allows PHP Local File Inclusion.This issue affects Deston: from n/a through <= 1.0.	8.1	Details
CVE-2026-3108	Mattermost versions 11.2.x <= 11.2.2, 10.11.x <= 10.11.10, 11.4.x <= 11.4.0, 11.3.x <= 11.3.1 fail to sanitize user-controlled post content in the mmctl commands terminal output which allows attackers to manipulate administrator terminals via crafted messages containing ANSI and OSC escape sequences that enable screen manipulation, fake prompts, and clipboard hijacking.. Mattermost Advisory ID: MMSA-2026-00599	8.0	More Details
CVE-2026-1961	A flaw was found in Foreman. A remote attacker could exploit a command injection vulnerability in Foreman's WebSocket proxy implementation. This vulnerability arises from the system's use of unsanitized hostname values from compute resource providers when constructing shell commands. By operating a malicious compute resource server, an attacker could achieve remote code execution on the Foreman server when a user accesses VM VNC console functionality. This could lead to the compromise of sensitive credentials and the entire managed infrastructure.	8.0	More Details
CVE-2026-4248	The Ultimate Member plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.11.2. This is due to the '{usermeta:password_reset_link}' template tag being processed within post content via the '[um_loggedin]' shortcode, which generates a valid password reset token for the currently logged-in user viewing the page. This makes it possible for authenticated attackers, with Contributor-level access and above, to craft a malicious pending post that, when previewed by an Administrator, generates a password reset token for the Administrator and exfiltrates it to an attacker-controlled server, leading to full account takeover.	8.0	More Details
CVE-2026-32978	OpenClaw before 2026.3.11 contains an approval integrity vulnerability where system.run approvals fail to bind mutable file operands for certain script runners like tsx and jiti. Attackers can obtain approval for benign script commands, rewrite referenced scripts on disk, and execute modified code under the approved run context.	8.0	More Details
CVE-2026-3502	TrueConf Client downloads application update code and applies it without performing verification. An attacker who is able to influence the update delivery path can substitute a tampered update payload. If the payload is executed or installed by the updater, this may result in arbitrary code execution in the context of the updating process or user.	7.8	More Details
CVE-2026-34054	vcpkg is a free and open-source C/C++ package manager. Prior to version 3.6.1#3, vcpkg's Windows builds of OpenSSL set openssldir to a path on the build machine, making that path be attackable later on customer machines. This issue has been patched in version 3.6.1#3.	7.8	More Details
CVE-2026-27309	Substance3D - Stager versions 3.1.7 and earlier are affected by a Use After Free 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-2026-33744	BentoML is a Python library for building online serving systems optimized for AI apps and model inference. Prior to 1.4.37, the `docker.system_packages` field in `bentofile.yaml` accepts arbitrary strings that are interpolated directly into Dockerfile `RUN` commands without sanitization. Since `system_packages` is semantically a list of OS package names (data), users do not expect values to be interpreted as shell commands. A malicious `bentofile.yaml` achieves arbitrary command execution during `bentoml containerize` / `docker build`. Version 1.4.37 fixes the issue.	7.8	More Details
CVE-2026-33491	Zen C is a systems programming language that compiles to human-readable GNU C/C11. Prior to version 0.4.4, a stack-based buffer overflow vulnerability in the Zen C compiler allows attackers to cause a compiler crash or potentially execute arbitrary code by providing a specially crafted Zen C source file (`.zc`) with excessively long struct, function, or trait identifiers. Users are advised to update to Zen C version v0.4.4 or later to receive a patch.	7.8	More Details
CVE-2025-41359	Vulnerability related to an unquoted service path in Small HTTP Server 3.06.36, specifically affecting the executable located at 'C:\Program Files (x86)\shttps_mg\http.exe service'. This misconfiguration allows a local attacker to place a malicious executable with the same name in a higher priority directory, causing the service to execute the malicious file instead of the legitimate one. Exploiting this flaw could allow arbitrary code execution, unauthorized access to the system, or service disruption. To mitigate the risk, the service path must be properly quoted, and systems must be kept up to date with security patches, while restricting physical and network access.	7.8	More Details
CVE-2026-4416	The Performance Library component of Gigabyte Control Center has an Insecure Deserialization vulnerability. Authenticated local attackers can send a malicious serialized payload to the EasyTune Engine service, resulting in privilege escalation.	7.8	More Details
CVE-2026-33874	Gematik Authenticator securely authenticates users for login to digital health applications. Starting in version 4.12.0 and prior to version 4.16.0, the Mac OS version of the Authenticator is vulnerable to remote code execution, triggered when victims open a malicious file. Update the gematik Authenticator to version 4.16.0 or greater to receive a patch. There are no known workarounds.	7.8	More Details
CVE-2026-3991	Symantec Data Loss Prevention Windows Endpoint, prior to 25.1 MP1, 16.1 MP2, 16.0 RU2 HF9, 16.0 RU1 MP1 HF12, and 16.0 MP2 HF15, may be susceptible to a Elevation of Privilege vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	7.8	More Details
CVE-2026-20698	The issue was addressed with improved memory handling. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An app may be able to cause unexpected system termination or corrupt kernel memory.	7.8	More Details
CVE-2018-25211	Allok Video Splitter 3.1.1217 contains a buffer overflow vulnerability that allows local attackers to cause a denial of service or execute arbitrary code by supplying an oversized string in the License Name field. Attackers can craft a malicious payload exceeding 780 bytes, paste it into the License Name registration field, and trigger the overflow when the Register button is clicked.	7.8	More Details
CVE-2026-24165	NVIDIA BioNeMo contains a vulnerability where a user could cause a deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2026-30309	InfCode's terminal auto-execution module contains a critical command filtering vulnerability that renders its blacklist security mechanism completely ineffective. The predefined blocklist fails to cover native high-risk commands in Windows PowerShell (such as powershell), and the matching algorithm lacks dynamic semantic parsing unable to recognize string concatenation, variable assignment, or double-quote interpolation in Shell syntax. Malicious commands can bypass interception through simple syntax obfuscation. An attacker can construct a file containing malicious instructions for remote code injection. When a user imports and views such a file in the IDE, the Agent executes dangerous PowerShell commands outside the blacklist without user confirmation, resulting in arbitrary command execution or sensitive data leakage.	7.8	More Details
CVE-2026-33711	Incus is a system container and virtual machine manager. Incus provides an API to retrieve VM screenshots. That API relies on the use of a temporary file for QEMU to write the screenshot to which is then picked up and sent to the user prior to deletion. As versions prior to 6.23.0 use predictable paths under /tmp for this, an attacker with local access to the system can abuse this mechanism by creating their own symlinks ahead of time. On the vast majority of Linux systems, this will result in a "Permission denied" error when requesting a screenshot. That's because the Linux kernel has a security feature designed to block such attacks, `protected_symlinks`. On the rare systems with this	7.8	More Details

	purposefully disabled, it's then possible to trick Incus intro truncating and altering the mode and permissions of arbitrary files on the filesystem, leading to a potential denial of service or possible local privilege escalation. Version 6.23.0 fixes the issue.		
CVE-2026-24970	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in designingmedia Energox energox allows Path Traversal.This issue affects Energox: from n/a through <= 1.2.	7.7	More Details
CVE-2026-24969	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in designingmedia Instant VA instantva allows Path Traversal.This issue affects Instant VA: from n/a through <= 1.0.1.	7.7	More Details
CVE-2026-30463	Daylight Studio FuelCMS v1.5.2 was discovered to contain a SQL injection vulnerability via the /controllers/Login.php component.	7.7	More Details
CVE-2026-34056	OpenEMR is a free and open source electronic health records and medical practice management application. A Broken Access Control vulnerability in OpenEMR up to and including version 8.0.0.3 allows low-privilege users to view and download Ensora eRx error logs without proper authorization checks. This flaw compromises system confidentiality by exposing sensitive information, potentially leading to unauthorized data disclosure and misuse. As of time of publication, no known patches versions are available.	7.7	More Details
CVE-2026-29925	Invoice Ninja v5.12.46 and v5.12.48 is vulnerable to Server-Side Request Forgery (SSRF) in CheckDatabaseRequest.php.	7.7	More Details
CVE-2026-33530	InvenTree is an Open Source Inventory Management System. Prior to version 1.2.6, certain API endpoints associated with bulk data operations can be hijacked to exfiltrate sensitive information from the database. The bulk operation API endpoints (e.g. `/api/part/`, `/api/stock/`, `/api/order/so/allocation/`, and others) accept a filters parameter that is passed directly to Django's ORM queryset.filter(**filters) without any field allowlisting. This enables any authenticated user to traverse model relationships using Django's __ lookup syntax and perform blind boolean-based data extraction. This issue is patched in version 1.2.6, and 1.3.0 (or above). Users should update to the patched versions. No known workarounds are available.	7.7	More Details
CVE-2026-24031	Dovecot SQL based authentication can be bypassed when auth_username_chars is cleared by admin. This vulnerability allows bypassing authentication for any user and user enumeration. Do not clear auth_username_chars. If this is not possible, install latest fixed version. No publicly available exploits are known.	7.7	More Details
CVE-2026-2995	GitLab has remediated an issue in GitLab EE affecting all versions from 15.4 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1 that could have allowed an authenticated user to add email addresses to targeted user accounts due to improper sanitization of HTML content.	7.7	More Details
CVE-2026-32441	Missing Authorization vulnerability in WebToffee Comments Import & Export comments-import-export-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Comments Import & Export: from n/a through <= 2.4.9.	7.7	More Details
CVE-2026-34163	FastGPT is an AI Agent building platform. Prior to version 4.14.9.5, FastGPT's MCP (Model Context Protocol) tools endpoints (/api/core/app/mcpTools/getTools and /api/core/app/mcpTools/runTool) accept a user-supplied URL parameter and make server-side HTTP requests to it without validating whether the URL points to an internal/private network address. Although the application has a dedicated isInternalAddress() function for SSRF protection (used in other endpoints like the HTTP workflow node), the MCP tools endpoints do not call this function. An authenticated attacker can use these endpoints to scan internal networks, access cloud metadata services, and interact with internal services such as MongoDB and Redis. This issue has been patched in version 4.14.9.5.	7.7	More Details
CVE-2024-51346	An issue in Eufy Homebase 2 version 3.3.4.1h allows a local attacker to obtain sensitive information via the cryptographic scheme.	7.7	More Details
CVE-2026-20125	A vulnerability in the HTTP Server feature of Cisco IOS Software and Cisco IOS XE Software Release 3E could allow an authenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending malformed HTTP requests to an affected device. A successful exploit could allow the attacker to cause a watchdog timer to expire and the device to reload, resulting in a DoS condition. To exploit this vulnerability, the attacker must have a valid user account.	7.7	More Details
CVE-2026-31945	LibreChat is a ChatGPT clone with additional features. Versions 0.8.2-rc2 through 0.8.2 are vulnerable to a server-side request forgery (SSRF) attack when using agent actions or MCP. Although a previous SSRF vulnerability (https://github.com/danny-avila/LibreChat/security/advisories/GHSA-rgjq-4q58-m3q8) was reported and patched, the fix only introduced hostname validation. It does not verify whether DNS resolution results in a private IP address. As a result, an attacker can still bypass the protection and gain access to internal resources, such as an internal RAG API or cloud instance metadata endpoints. Version 0.8.3-rc1 contains a patch.	7.7	More Details
CVE-2026-34214	Trino is a distributed SQL query engine for big data analytics. From version 439 to before version 480, Iceberg connector REST catalog static credentials (access key) or vended credentials (temporary access key) are accessible to users that have write privilege on SQL level. This issue has been patched in version 480.	7.7	More Details
CVE-2026-33913	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, an authenticated user with access to the Carecoordination module can upload a crafted CCDA document containing `<xi:include href="file:///etc/passwd" parse="text"/>` to read arbitrary files from the server. Version 8.0.0.3 patches the issue.	7.7	More Details
CVE-2026-33636	LIBPNG is a reference library for use in applications that read, create, and manipulate PNG (Portable Network Graphics) raster image files. In versions 1.6.36 through 1.6.55, an out-of-bounds read and write exists in libpng's ARM/AArch64 Neon-optimized palette expansion path. When expanding 8-bit paletted rows to RGB or RGBA, the Neon loop processes a final partial chunk without verifying that enough input pixels remain. Because the implementation works backward from the end of the row, the final iteration dereferences pointers before the start of the row buffer (OOB read) and writes expanded pixel data to the same underflowed positions (OOB write). This is reachable via normal decoding of attacker-controlled PNG input if Neon is enabled. Version 1.6.56 fixes the issue.	7.6	More Details
CVE-2026-34365	InvoiceShelf is an open-source web & mobile app that helps track expenses, payments and create professional invoices and estimates. Prior to version 2.2.0, a Server-Side Request Forgery (SSRF) vulnerability exists in the Estimate PDF generation module. User-supplied HTML in the estimate Notes field is passed unsanitised to the Dompdf rendering library, which will fetch any remote resources referenced in the markup. The vulnerability is exploitable directly via the PDF preview and customer view endpoints regardless of whether automated email attachments are enabled. This issue has been patched in version 2.2.0.	7.6	More Details
CVE-	NVIDIA Jetson Linux has vulnerability in initrd, where an unprivileged attacker with physical access coul inject incorrect command line		

2026-24154	arguments. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, data tampering, and information disclosure.	7.6	More Details
CVE-2026-34367	InvoiceShelf is an open-source web & mobile app that helps track expenses, payments and create professional invoices and estimates. Prior to version 2.2.0, a Server-Side Request Forgery (SSRF) vulnerability exists in the Invoice PDF generation module. User-supplied HTML in the invoice Notes field is passed unsanitised to the Dompdf rendering library, which will fetch any remote resources referenced in the markup. This can be triggered via the PDF preview and email delivery endpoints. This issue has been patched in version 2.2.0.	7.6	More Details
CVE-2026-34366	InvoiceShelf is an open-source web & mobile app that helps track expenses, payments and create professional invoices and estimates. Prior to version 2.2.0, a Server-Side Request Forgery (SSRF) vulnerability exists in the Payment receipt PDF generation module. User-supplied HTML in the payment Notes field is passed unsanitised to the Dompdf rendering library, which will fetch any remote resources referenced in the markup. The vulnerability is exploitable directly via the PDF receipt endpoint, regardless of whether automated email attachments are enabled. This issue has been patched in version 2.2.0.	7.6	More Details
CVE-2026-33932	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, a stored cross-site scripting vulnerability in the CCDA document preview allows an attacker who can upload or send a CCDA document to execute arbitrary JavaScript in a clinician's browser session when the document is previewed. The XSL stylesheet sanitizes attributes for all other narrative elements but not for `linkHtml`, allowing `href="javascript:..."` and event handler attributes to pass through unchanged. Version 8.0.0.3 patches the issue.	7.6	More Details
CVE-2026-24750	Kiteworks is a private data network (PDN). In Kiteworks Secure Data Forms prior to version 9.2.1, an authenticated attacker could exploit an Improper Neutralization of Input During Web Page Generation as Stored XSS when modifying forms. Upgrade Kiteworks to version 9.2.1 or later to receive a patch.	7.6	More Details
CVE-2026-29954	In KubePlus 4.1.4, the mutating webhook and kubeconfiggenerator components have an SSRF vulnerability when processing the chartURL field of ResourceComposition resources. The field is only URL-encoded without validating the target address. More critically, when kubeconfiggenerator uses wget to download charts, the chartURL is directly concatenated into the command, allowing attackers to inject wget's `--header` option to achieve arbitrary HTTP header injection.	7.6	More Details
CVE-2026-29870	A directory traversal vulnerability in the agentic-context-engine project versions up to 0.7.1 allows arbitrary file writes via the checkpoint_dir parameter in OfflineACE.run. The save_to_file method in ace/skillbook.py fails to normalize or validate filesystem paths, allowing traversal sequences to escape the intended checkpoint directory. This vulnerability allows attackers to overwrite arbitrary files accessible to the application process, potentially leading to application corruption, privilege escalation, or code execution depending on the deployment context.	7.6	More Details
CVE-2026-33918	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, the billing file-download endpoint `interface/billing/get_claim_file.php` only verifies that the caller has a valid session and CSRF token, but does not check any ACL permissions. This allows any authenticated OpenEMR user — regardless of whether they have billing privileges — to download and permanently delete electronic claim batch files containing protected health information (PHI). Version 8.0.0.3 patches the issue.	7.6	More Details
CVE-2026-29924	Grav CMS v1.7.x and before is vulnerable to XML External Entity (XXE) through the SVG file upload functionality in the admin panel and File Manager plugin.	7.6	More Details
CVE-2026-33718	OpenHands is software for AI-driven development. Starting in version 1.5.0, a Command Injection vulnerability exists in the `get_git_diff()` method at `openhands/runtime/utils/git_handler.py:134`. The `path` parameter from the `/api/conversations/{conversation_id}/git/diff` API endpoint is passed unsanitized to a shell command, allowing authenticated attackers to execute arbitrary commands in the agent sandbox. The user is already allowed to instruct the agent to execute commands, but this bypasses the normal channels. Version 1.5.0 fixes the issue.	7.6	More Details
CVE-2026-33673	PrestaShop is an open source e-commerce web application. Versions prior to 8.2.5 and 9.1.0 are vulnerable to stored Cross-Site Scripting (stored XSS) vulnerabilities in the BO. An attacker who can inject data into the database, via limited back-office access or a previously existing vulnerability, can exploit unprotected variables in back-office templates. Versions 8.2.5 and 9.1.0 contain a fix. No known workarounds are available.	7.6	More Details
CVE-2026-32537	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in nK Visual Portfolio, Photo Gallery & Post Grid visual-portfolio allows PHP Local File Inclusion.This issue affects Visual Portfolio, Photo Gallery & Post Grid: from n/a through <= 3.5.1.	7.5	More Details
CVE-2026-33665	n8n is an open source workflow automation platform. Prior to versions 2.4.0 and 1.121.0, when LDAP authentication is enabled, n8n automatically linked an LDAP identity to an existing local account if the LDAP email attribute matched the local account's email. An authenticated LDAP user who could control their own LDAP email attribute could set it to match another user's email — including an administrator's — and upon login gain full access to that account. The account linkage persisted even if the LDAP email was later reverted, resulting in a permanent account takeover. LDAP authentication must be configured and active (non-default). The issue has been fixed in n8n versions 2.4.0 and 1.121.0. Users should upgrade to one of these versions or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations: Disable LDAP authentication until the instance can be upgraded, restrict LDAP directory permissions so that users cannot modify their own email attributes, and/or audit existing LDAP-linked accounts for unexpected account associations. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	7.5	More Details
CVE-2026-33182	Saloon is a PHP library that gives users tools to build API integrations and SDKs. Prior to version 4.0.0, when building the request URL, Saloon combined the connector's base URL with the request endpoint. If the endpoint was a valid absolute URL, the code used that URL as-is and ignored the base URL. The request—and any authentication headers, cookies, or tokens attached by the connector—was then sent to the attacker-controlled host. If the endpoint could be influenced by user input or configuration (e.g. redirect_uri, callback URL), this allowed server-side request forgery (SSRF) and/or credential leakage to a third-party host. The fix in version 4.0.0 is to reject absolute URLs in the endpoint: URLHelper::join() throws InvalidArgumentException when the endpoint is a valid absolute URL, unless explicitly allowed, requiring callers to opt-in to the functionality on a per-connector or per-request basis.	7.5	More Details
CVE-2026-33870	Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.132.Final and 4.2.10.Final, Netty incorrectly parses quoted strings in HTTP/1.1 chunked transfer encoding extension values, enabling request smuggling attacks. Versions 4.1.132.Final and 4.2.10.Final fix the issue.	7.5	More Details
CVE-2026-26061	Fleet is open source device management software. Prior to 4.81.0, Fleet contained multiple unauthenticated HTTP endpoints that read request bodies without enforcing a size limit. An unauthenticated attacker could exploit this behavior by sending large or repeated HTTP payloads, causing excessive memory allocation and resulting in a denial-of-service (DoS) condition. Version 4.81.0 patches the issue.	7.5	More Details
CVE-2026-	Insertion of Sensitive Information Into Sent Data vulnerability in Noor Alam SMTP Mailer smtp-mailer allows Retrieve Embedded Sensitive Data.This issue affects SMTP Mailer: from n/a through <= 1.1.24.	7.5	More Details

32538			
CVE-2026-33285	LiquidJS is a Shopify / GitHub Pages compatible template engine in pure JavaScript. Prior to version 10.25.1, LiquidJS's `memoryLimit` security mechanism can be completely bypassed by using reverse range expressions (e.g., `(100000000..1)`), allowing an attacker to allocate unlimited memory. Combined with a string flattening operation (e.g., `replace` filter), this causes a V8 Fatal error that crashes the Node.js process, resulting in complete denial of service from a single HTTP request. Version 10.25.1 patches the issue.	7.5	More Details
CVE-2026-33287	LiquidJS is a Shopify / GitHub Pages compatible template engine in pure JavaScript. Prior to version 10.25.1, the `replace_first` filter in LiquidJS uses JavaScript's `String.prototype.replace()` which interprets `$&` as a back reference to the matched substring. The filter only charges `memoryLimit` for the input string length, not the amplified output. An attacker can achieve exponential memory amplification (up to 625,000:1) while staying within the `memoryLimit` budget, leading to denial of service. Version 10.25.1 patches the issue.	7.5	More Details
CVE-2026-33526	Squid is a caching proxy for the Web. Prior to version 7.5, due to heap Use-After-Free, Squid is vulnerable to Denial of Service when handling ICP traffic. This problem allows a remote attacker to perform a reliable and repeatable Denial of Service attack against the Squid service using ICP protocol. This attack is limited to Squid deployments that explicitly enable ICP support (i.e. configure non-zero `icp_port`). This problem _cannot_ be mitigated by denying ICP queries using `icp_access` rules. Version 7.5 contains a patch.	7.5	More Details
CVE-2026-3988	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.5 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1 that could have allowed an unauthenticated user to cause a denial of service by making the GitLab instance unresponsive due to improper input validation in GraphQL request processing.	7.5	More Details
CVE-2026-27889	NATS-Server is a High-Performance server for NATS.io, a cloud and edge native messaging system. Starting in version 2.2.0 and prior to versions 2.11.14 and 2.12.5, a missing sanity check on a WebSockets frame could trigger a server panic in the nats-server. This happens before authentication, and so is exposed to anyone who can connect to the websockets port. Versions 2.11.14 and 2.12.5 contains a fix. A workaround is available. The vulnerability only affects deployments which use WebSockets and which expose the network port to untrusted end-points. If one is able to do so, a defense in depth of restricting either of these will mitigate the attack.	7.5	More Details
CVE-2026-25401	Missing Authorization vulnerability in Arni Cinco WPCargo Track & Trace wpcargo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPCargo Track & Trace: from n/a through <= 8.0.2.	7.5	More Details
CVE-2026-25317	Missing Authorization vulnerability in tychesoftwares Print Invoice & Delivery Notes for WooCommerce woocommerce-delivery-notes allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Print Invoice & Delivery Notes for WooCommerce: from n/a through <= 5.9.0.	7.5	More Details
CVE-2026-29785	NATS-Server is a High-Performance server for NATS.io, a cloud and edge native messaging system. Prior to versions 2.11.14 and 2.12.5, if the nats-server has the "leafnode" configuration enabled (not default), then anyone who can connect can crash the nats-server by triggering a panic. This happens pre-authentication and requires that compression be enabled (which it is, by default, when leafnodes are used). Versions 2.11.14 and 2.12.5 contain a fix. As a workaround, disable compression on the leafnode port.	7.5	More Details
CVE-2026-32748	Squid is a caching proxy for the Web. Prior to version 7.5, due to premature release of resource during expected lifetime and heap Use-After-Free bugs, Squid is vulnerable to Denial of Service when handling ICP traffic. This problem allows a remote attacker to perform a reliable and repeatable Denial of Service attack against the Squid service using ICP protocol. This attack is limited to Squid deployments that explicitly enable ICP support (i.e. configure non-zero `icp_port`). This problem _cannot_ be mitigated by denying ICP queries using `icp_access` rules. This bug is fixed in Squid version 7.5.	7.5	More Details
CVE-2025-70952	pf4j before 20c2f80 has a path traversal vulnerability in the extract() function of Unzip.java, where improper handling of zip entry names can allow directory traversal or Zip Slip attacks, due to a lack of proper path normalization and validation.	7.5	More Details
CVE-2026-33895	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. Prior to version 1.4.0, Ed25519 signature verification accepts forged non-canonical signatures where the scalar S is not reduced modulo the group order (`S >= L`). A valid signature and its `S + L` variant both verify in forge, while Node.js `crypto.verify` (OpenSSL-backed) rejects the `S + L` variant, as defined by the specification. This class of signature malleability has been exploited in practice to bypass authentication and authorization logic (see CVE-2026-25793, CVE-2022-35961). Applications relying on signature uniqueness (i.e., dedup by signature bytes, replay tracking, signed-object canonicalization checks) may be bypassed. Version 1.4.0 patches the issue.	7.5	More Details
CVE-2026-25397	Path Traversal: '.../...//' vulnerability in Snowray Software File Uploader for WooCommerce file-uploader-for-woocommerce allows Path Traversal.This issue affects File Uploader for WooCommerce: from n/a through <= 1.0.4.	7.5	More Details
CVE-2026-33867	WWBN AVideo is an open source video platform. In versions up to and including 26.0, AVideo allows content owners to password-protect individual videos. The video password is stored in the database in plaintext — no hashing, salting, or encryption is applied. If an attacker gains read access to the database (via SQL injection, a database backup, or misconfigured access controls), they obtain all video passwords in cleartext. Commit f2d68d2adbf73588ea61be2b781d93120a819e36 contains a patch.	7.5	More Details
CVE-2026-33939	Handlebars provides the power necessary to let users build semantic templates. In versions 4.0.0 through 4.7.8, when a Handlebars template contains decorator syntax referencing an unregistered decorator (e.g. `{{*n}}`), the compiled template calls `lookupProperty(decorators, "n")`, which returns `undefined`. The runtime then immediately invokes the result as a function, causing an unhandled `TypeError: ... is not a function` that crashes the Node.js process. Any application that compiles user-supplied templates without wrapping the call in a `try/catch` is vulnerable to a single-request Denial of Service. Version 4.7.9 fixes the issue. Some workarounds are available. Wrap compilation and rendering in `try/catch`. Validate template input before passing it to `compile()`; reject templates containing decorator syntax (`{{*...}}`) if decorators are not used in your application. Use the pre-compilation workflow; compile templates at build time and serve only pre-compiled templates; do not call `compile()` at request time.	7.5	More Details
CVE-2026-32485	Missing Authorization vulnerability in weDevs WP User Frontend wp-user-frontend allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP User Frontend: from n/a through <= 4.2.8.	7.5	More Details
CVE-2026-30576	A Business Logic vulnerability exists in SourceCodester Pharmacy Product Management System 1.0 in the add-stock.php file. The application fails to validate the "txtprice" and "txttotalcost" parameters during stock entry, allowing negative financial values to be submitted. This leads to corruption of financial records, allowing attackers to manipulate inventory asset values and procurement costs.	7.5	More Details
CVE-2026-30575	A Business Logic vulnerability exists in SourceCodester Pharmacy Product Management System 1.0 in the add-stock.php file. The application fails to validate the "txtqty" parameter during stock entry, allowing negative values to be processed. This causes the system to decrease the inventory level instead of increasing it, leading to inventory corruption and potential Denial of Service by depleting stock records.	7.5	More Details
CVE-	Missing Authorization vulnerability in Aarsiv Groups Automated FedEx live/manual rates with shipping labels a2z-fedex-shipping allows		More

2026-25456	Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Automated FedEx live/manual rates with shipping labels: from n/a through <= 5.1.8.	7.5	Details
CVE-2026-30574	A Business Logic vulnerability exists in SourceCodester Pharmacy Product Management System 1.0 in the add-sales.php file. The application fails to verify if the requested sales quantity (txtqty) exceeds the available stock level. An attacker can manipulate the request to purchase a quantity that is significantly higher than the actual available stock.	7.5	More Details
CVE-2026-32495	Missing Authorization vulnerability in Link Software LLC WP Terms Popup wp-terms-popup allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Terms Popup: from n/a through <= 2.10.0.	7.5	More Details
CVE-2026-32515	Missing Authorization vulnerability in kamleshyadav Miraculous miraculous allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Miraculous: from n/a through < 2.1.2.	7.5	More Details
CVE-2026-25396	Missing Authorization vulnerability in CoderPress Commerce Coinbase For WooCommerce commerce-coinbase-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Commerce Coinbase For WooCommerce: from n/a through <= 1.6.6.	7.5	More Details
CVE-2026-32241	Flannel is a network fabric for containers, designed for Kubernetes. The Flannel project includes an experimental Extension backend that allows users to easily prototype new backend types. In versions of Flannel prior to 0.28.2, this Extension backend is vulnerable to a command injection that allows an attacker who can set Kubernetes Node annotations to achieve root-level arbitrary command execution on every flannel node in the cluster. The Extension backend's SubnetAddCommand and SubnetRemoveCommand receive attacker-controlled data via stdin (from the `flannel.alpha.coreos.com/backend-data` Node annotation). The content of this annotation is unmarshalled and piped directly to a shell command without checks. Kubernetes clusters using Flannel with the Extension backend are affected by this vulnerability. Other backends such as vxlan and wireguard are unaffected. The vulnerability is fixed in version v0.28.2. As a workaround, use Flannel with another backend such as vxlan or wireguard.	7.5	More Details
CVE-2026-33218	NATS-Server is a High-Performance server for NATS.io, a cloud and edge native messaging system. Prior to versions 2.11.15 and 2.12.6, a client which can connect to the leafnode port can crash the nats-server with a certain malformed message pre-authentication. Versions 2.11.15 and 2.12.6 contain a fix. As a workaround, disable leafnode support if not needed or restrict network connections to the leafnode port, if plausible without compromising the service offered.	7.5	More Details
CVE-2019-25652	UniFi Network Controller before version 5.10.22 and 5.11.x before 5.11.18 contains an improper certificate verification vulnerability that allows adjacent network attackers to conduct man-in-the-middle attacks by presenting a false SSL certificate during SMTP connections. Attackers can intercept SMTP traffic and obtain credentials by exploiting the insecure SSL host verification mechanism in the SMTP certificate validation process.	7.5	More Details
CVE-2026-27073	Use of Hard-coded Credentials vulnerability in Addi Addi – Cuotas que se adaptan a ti buy-now-pay-later-addi allows Password Recovery Exploitation.This issue affects Addi – Cuotas que se adaptan a ti: from n/a through <= 2.0.4.	7.5	More Details
CVE-2026-33871	Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.132.Final and 4.2.10.Final, a remote user can trigger a Denial of Service (DoS) against a Netty HTTP/2 server by sending a flood of `CONTINUATION` frames. The server's lack of a limit on the number of `CONTINUATION` frames, combined with a bypass of existing size-based mitigations using zero-byte frames, allows an user to cause excessive CPU consumption with minimal bandwidth, rendering the server unresponsive. Versions 4.1.132.Final and 4.2.10.Final fix the issue.	7.5	More Details
CVE-2026-33894	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. Prior to version 1.4.0, RSASSA PKCS#1 v1.5 signature verification accepts forged signatures for low public exponent keys (e=3). Attackers can forge signatures by stuffing “garbage” bytes within the ASN structure in order to construct a signature that passes verification, enabling Bleichenbacher style forgery. This issue is similar to CVE-2022-24771, but adds bytes in an addition field within the ASN structure, rather than outside of it. Additionally, forge does not validate that signatures include a minimum of 8 bytes of padding as defined by the specification, providing attackers additional space to construct Bleichenbacher forgeries. Version 1.4.0 patches the issue.	7.5	More Details
CVE-2026-32498	Missing Authorization vulnerability in Metagauss RegistrationMagic custom-registration-form-builder-with-submission-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects RegistrationMagic: from n/a through <= 6.0.7.6.	7.5	More Details
CVE-2026-25309	Missing Authorization vulnerability in PublishPress PublishPress Authors publishpress-authors allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PublishPress Authors: from n/a through <= 4.10.1.	7.5	More Details
CVE-2026-32546	Missing Authorization vulnerability in StellarWP Restrict Content restrict-content allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Restrict Content: from n/a through <= 3.2.22.	7.5	More Details
CVE-2026-28842	The issue was addressed with improved bounds checks. This issue is fixed in macOS Tahoe 26.4. A buffer overflow may result in memory corruption and unexpected app termination.	7.5	More Details
CVE-2026-28876	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, visionOS 26.4. An app may be able to access sensitive user data.	7.5	More Details
CVE-2026-3124	The Download Monitor plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.1.7 via the executePayment() function due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to complete arbitrary pending orders by exploiting a mismatch between the PayPal transaction token and the local order, allowing theft of paid digital goods by paying a minimal amount for a low-cost item and using that payment token to finalize a high-value order.	7.5	More Details
CVE-2026-0560	A Server-Side Request Forgery (SSRF) vulnerability exists in parisneo/lollms versions prior to 2.2.0, specifically in the `/api/files/export-content` endpoint. The `_download_image_to_temp()` function in `backend/routers/files.py` fails to validate user-controlled URLs, allowing attackers to make arbitrary HTTP requests to internal services and cloud metadata endpoints. This vulnerability can lead to internal network access, cloud metadata access, information disclosure, port scanning, and potentially remote code execution.	7.5	More Details
CVE-2026-33575	OpenClaw before 2026.3.12 embeds long-lived shared gateway credentials directly in pairing setup codes generated by /pair endpoint and OpenClaw qr command. Attackers with access to leaked setup codes from chat history, logs, or screenshots can recover and reuse the shared gateway credential outside the intended one-time pairing flow.	7.5	More Details

CVE-2026-32980	OpenClaw before 2026.3.13 reads and buffers Telegram webhook request bodies before validating the x-telegram-bot-api-secret-token header, allowing unauthenticated attackers to exhaust server resources. Attackers can send POST requests to the webhook endpoint to force memory consumption, socket time, and JSON parsing work before authentication validation occurs.	7.5	More Details
CVE-2026-3622	The vulnerability exists in the UPnP component of TL-WR841N v14, where improper input validation leads to an out-of-bounds read, potentially causing a crash of the UPnP service. Successful exploitation can cause the UPnP service to crash, resulting in a Denial-of-Service condition. This vulnerability affects TL-WR841N v14 < EN_0.9.1 4.19 Build 260303 Rel.42399n (V14_260303) and < US_0.9.1.4.19 Build 260312 Rel. 49108n (V14_0304).	7.5	More Details
CVE-2026-3573	Incorrect Authorization vulnerability in Drupal AI (Artificial Intelligence) allows Resource Injection.This issue affects AI (Artificial Intelligence): from 0.0.0 before 1.1.11, from 1.2.0 before 1.2.12.	7.5	More Details
CVE-2026-27828	EVerest is an EV charging software stack. Prior to version 2026.02.0, ISO15118_chargerImpl::handle_session_setup uses v2g_ctx after it has been freed when ISO15118 initialization fails (e.g., no IPv6 link-local address). The EVSE process can be crashed remotely by an attacker with MQTT access who issues a session_setup command while v2g_ctx has been released. Version 2026.02.0 contains a patch.	7.5	More Details
CVE-2026-32846	OpenClaw through 2026.3.23 (fixed in commit 4797bbc) contains a path traversal vulnerability in media parsing that allows attackers to read arbitrary files by bypassing path validation in the isLikelyLocalPath() and isValidMedia() functions. Attackers can exploit incomplete validation and the allowBareFilename bypass to reference files outside the intended application sandbox, resulting in disclosure of sensitive information including system files, environment files, and SSH keys.	7.5	More Details
CVE-2026-28875	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 26.4 and iPadOS 26.4. A remote attacker may be able to cause a denial-of-service.	7.5	More Details
CVE-2026-1519	If a BIND resolver is performing DNSSEC validation and encounters a maliciously crafted zone, the resolver may consume excessive CPU. Authoritative-only servers are generally unaffected, although there are circumstances where authoritative servers may make recursive queries (see: https://kb.isc.org/docs/why-does-my-authoritative-server-make-recursive-queries). This issue affects BIND 9 versions 9.11.0 through 9.16.50, 9.18.0 through 9.18.46, 9.20.0 through 9.20.20, 9.21.0 through 9.21.19, 9.11.3-S1 through 9.16.50-S1, 9.18.11-S1 through 9.18.46-S1, and 9.20.9-S1 through 9.20.20-S1.	7.5	More Details
CVE-2026-28874	The issue was addressed with improved checks. This issue is fixed in iOS 26.4 and iPadOS 26.4. A remote attacker may cause an unexpected app termination.	7.5	More Details
CVE-2026-34209	mppx is a TypeScript interface for machine payments protocol. Prior to version 0.4.11, the tempo/session cooperative close handler validated the close voucher amount using "<" instead of "<=" against the on-chain settled amount. An attacker could submit a close voucher exactly equal to the settled amount, which would be accepted without committing any new funds, effectively closing or griefing the channel for free. This issue has been patched in version 0.4.11.	7.5	More Details
CVE-2026-28865	An authentication issue was addressed with improved state management. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An attacker in a privileged network position may be able to intercept network traffic.	7.5	More Details
CVE-2026-33416	LIBPNG is a reference library for use in applications that read, create, and manipulate PNG (Portable Network Graphics) raster image files. In versions 1.2.1 through 1.6.55, `png_set_tRNS` and `png_set_PLTE` each alias a heap-allocated buffer between `png_struct` and `png_info`, sharing a single allocation across two structs with independent lifetimes. The `trans_alpha` aliasing has been present since at least libpng 1.0, and the `palette` aliasing since at least 1.2.1. Both affect all prior release lines `png_set_tRNS` sets `png_ptr->trans_alpha = info_ptr->trans_alpha` (256-byte buffer) and `png_set_PLTE` sets `info_ptr->palette = png_ptr->palette` (768-byte buffer). In both cases, calling `png_free_data` (with `PNG_FREE_TRNS` or `PNG_FREE_PLTE`) frees the buffer through `info_ptr` while the corresponding `png_ptr` pointer remains dangling. Subsequent row-transform functions dereference and, in some code paths, write to the freed memory. A second call to `png_set_tRNS` or `png_set_PLTE` has the same effect, because both functions call `png_free_data` internally before reallocating the `info_ptr` buffer. Version 1.6.56 fixes the issue.	7.5	More Details
CVE-2026-34240	JOSE is a Javascript Object Signing and Encryption (JOSE) library. Prior to version 0.3.5+1, a vulnerability in jose could allow an unauthenticated, remote attacker to forge valid JWS/JWT tokens by using a key embedded in the JOSE header (jwk). The vulnerability exists because key selection could treat header-provided jwk as a verification candidate even when that key was not present in the trusted key store. Since JOSE headers are untrusted input, an attacker could exploit this by creating a token payload, embedding an attacker-controlled public key in the header, and signing with the matching private key. Applications using affected versions for token verification are impacted. This issue has been patched in version 0.3.5+1. A workaround for this issue involves rejecting tokens where header jwk is present unless that jwk matches a key already present in the application's trusted key store.	7.5	More Details
CVE-2026-28855	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 26.3 and iPadOS 26.3, macOS Tahoe 26.3. An app may be able to access protected user data.	7.5	More Details
CVE-2026-27664	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.10), SICORE Base system (All versions < V26.10.0). The affected application contains an out-of-bounds write vulnerability while parsing specially crafted XML inputs. This could allow an unauthenticated attacker to exploit this issue by sending a malicious XML request, which may cause the service to crash, resulting in a denial-of-service condition.	7.5	More Details
CVE-2026-28837	A logic issue was addressed with improved checks. This issue is fixed in macOS Tahoe 26.4. An app may be able to access sensitive user data.	7.5	More Details
CVE-2026-2328	An unauthenticated remote attacker can exploit insufficient input validation to access backend components beyond their intended scope via path traversal, resulting in exposure of sensitive information.	7.5	More Details
CVE-2026-3945	An integer overflow vulnerability in the HTTP chunked transfer encoding parser in tinyproxy up to and including version 1.11.3 allows an unauthenticated remote attacker to cause a denial of service (DoS). The issue occurs because chunk size values are parsed using strtol() without properly validating overflow conditions (e.g., errno == ERANGE). A crafted chunk size such as 0x7fffffffffffffff (LONG_MAX) bypasses the existing validation check (chunklen < 0), leading to a signed integer overflow during arithmetic operations (chunklen + 2). This results in incorrect size calculations, causing the proxy to attempt reading an extremely large amount of request-body data and holding worker connections open indefinitely. An attacker can exploit this behavior to exhaust all available worker slots, preventing new connections from being accepted and causing complete service unavailability. Upstream addressed this issue in commit bb7edc4; however, the latest stable	7.5	More Details

	release (1.11.3) remains affected at the time of publication.		
CVE-2019-25654	Core FTP/SFTP Server 1.2 contains a buffer overflow vulnerability that allows attackers to crash the service by supplying an excessively long string in the User domain field. Attackers can paste a malicious payload containing 7000 bytes of data into the domain configuration to trigger an application crash and deny service.	7.5	More Details
CVE-2026-25026	Missing Authorization vulnerability in RadiusTheme Team tlp-team allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Team: from n/a through <= 5.0.11.	7.5	More Details
CVE-2026-26008	EVerest is an EV charging software stack. Versions prior to 2026.02.0 have an out-of-bounds access (std::vector) that leads to possible remote crash/memory corruption. This is because the CSMS sends UpdateAllowedEnergyTransferModes over the network. Version 2026.2.0 contains a patch.	7.5	More Details
CVE-2026-5201	A flaw was found in the gdk-pixbuf library. This heap-based buffer overflow vulnerability occurs in the JPEG image loader due to improper validation of color component counts when processing a specially crafted JPEG image. A remote attacker can exploit this flaw without user interaction, for example, via thumbnail generation. Successful exploitation leads to application crashes and denial of service (DoS) conditions.	7.5	More Details
CVE-2026-33671	Picomatch is a glob matcher written JavaScript. Versions prior to 4.0.4, 3.0.2, and 2.3.2 are vulnerable to Regular Expression Denial of Service (ReDoS) when processing crafted extglob patterns. Certain patterns using extglob quantifiers such as `+()` and `*()`, especially when combined with overlapping alternatives or nested extglobs, are compiled into regular expressions that can exhibit catastrophic backtracking on non-matching input. Applications are impacted when they allow untrusted users to supply glob patterns that are passed to `picomatch` for compilation or matching. In those cases, an attacker can cause excessive CPU consumption and block the Node.js event loop, resulting in a denial of service. Applications that only use trusted, developer-controlled glob patterns are much less likely to be exposed in a security-relevant way. This issue is fixed in picomatch 4.0.4, 3.0.2 and 2.3.2. Users should upgrade to one of these versions or later, depending on their supported release line. If upgrading is not immediately possible, avoid passing untrusted glob patterns to `picomatch`. Possible mitigations include disabling extglob support for untrusted patterns by using `noextglob: true`, rejecting or sanitizing patterns containing nested extglobs or extglob quantifiers such as `+()` and `*()`, enforcing strict allowlists for accepted pattern syntax, running matching in an isolated worker or separate process with time and resource limits, and applying application-level request throttling and input validation for any endpoint that accepts glob patterns.	7.5	More Details
CVE-2026-3650	A memory leak exists in the Grassroots DICOM library (GDCM). The bug occurs when parsing malformed DICOM files with non-standard VR types in file meta information. The vulnerability leads to vast memory allocations and resource depletion, triggering a denial-of-service condition. A maliciously crafted file can fill the heap in a single read operation without properly releasing it.	7.5	More Details
CVE-2026-32982	OpenClaw before 2026.3.13 contains an information disclosure vulnerability in the fetchRemoteMedia function that exposes Telegram bot tokens in error messages. When media downloads fail, the original Telegram file URLs containing bot tokens are embedded in MediaFetchError strings and leaked to logs and error surfaces.	7.5	More Details
CVE-2026-2511	The JS Help Desk – AI-Powered Support & Ticketing System plugin for WordPress is vulnerable to SQL Injection via the `multiformid` parameter in the `storeTickets()` function in all versions up to, and including, 3.0.4. This is due to the user-supplied `multiformid` value being passed to `esc_sql()` without enclosing the result in quotes in the SQL query, rendering the escaping ineffective against payloads that do not contain quote characters. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-32988	OpenClaw before 2026.3.11 contains a sandbox boundary bypass vulnerability in fs-bridge staged writes where temporary file creation and population are not pinned to a verified parent directory. Attackers can exploit a race condition in parent-path alias changes to write attacker-controlled bytes outside the intended validated path before the final guarded replace step executes.	7.5	More Details
CVE-2026-34070	LangChain is a framework for building agents and LLM-powered applications. Prior to version 1.2.22, multiple functions in langchain_core.prompts.loading read files from paths embedded in deserialized config dicts without validating against directory traversal or absolute path injection. When an application passes user-influenced prompt configurations to load_prompt() or load_prompt_from_config(), an attacker can read arbitrary files on the host filesystem, constrained only by file-extension checks (.txt for templates, .json/.yaml for examples). This issue has been patched in version 1.2.22.	7.5	More Details
CVE-2026-28894	A denial-of-service issue was addressed with improved input validation. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. A remote attacker may be able to cause a denial-of-service.	7.5	More Details
CVE-2026-4020	The Gravity SMTP plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.1.4. This is due to a REST API endpoint registered at /wp-json/gravitysmtp/v1/tests/mock-data with a permission_callback that unconditionally returns true, allowing any unauthenticated visitor to access it. When the ?page=gravitysmtp-settings query parameter is appended, the plugin's register_connector_data() method populates internal connector data, causing the endpoint to return approximately 365 KB of JSON containing the full System Report. This makes it possible for unauthenticated attackers to retrieve detailed system configuration data including PHP version, loaded extensions, web server version, document root path, database server type and version, WordPress version, all active plugins with versions, active theme, WordPress configuration details, database table names, and any API keys/tokens configured in the plugin.	7.5	More Details
CVE-2026-28377	A vulnerability in Grafana Tempo exposes the S3 SSE-C encryption key in plaintext through the /status/config endpoint, potentially allowing unauthorized users to obtain the key used to encrypt trace data stored in S3. Thanks to william_goodfellow for reporting this vulnerability.	7.5	More Details
CVE-2026-33986	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.24.2, in yuv_ensure_buffer() in libfreerdp/codec/h264.c, h264->width and h264->height are updated before the reallocation loop. If any winpr_aligned_recalloc() call fails, the function returns FALSE but width/height are already inflated. This issue has been patched in version 3.24.2.	7.5	More Details
CVE-2026-33984	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.24.2, in resize_vbar_entry() in libfreerdp/codec/clear.c, vBarEntry->size is updated to vBarEntry->count before the winpr_aligned_recalloc() call. If realloc fails, size is inflated while pixels still points to the old, smaller buffer. On a subsequent call where count <= size (the inflated value), realloc is skipped. The caller then writes count * bpp bytes of attacker-controlled pixel data into the undersized buffer, causing a heap buffer overflow. This issue has been patched in version 3.24.2.	7.5	More Details
CVE-2026-4933	Incorrect Authorization vulnerability in Drupal Unpublished Node Permissions allows Forceful Browsing.This issue affects Unpublished Node Permissions: from 0.0.0 before 1.7.0.	7.5	More Details
CVE-2026-4046	The iconv() function in the GNU C Library versions 2.43 and earlier may crash due to an assertion failure when converting inputs from the IBM1390 or IBM1399 character sets, which may be used to remotely crash an application. This vulnerability can be trivially mitigated by removing the IBM1390 and IBM1399 character sets from systems that do not need them.	7.5	More Details

CVE-2026-30077	OpenAirInterface V2.2.0 AMF crashes when it fails to decode the message. Not all decode failures result in a crash. But the crash is consistent for particular inputs. An example input in hex stream is 80 00 00 0E 00 00 01 00 0F 80 02 02 40 00 58 00 01 88.	7.5	More Details
CVE-2026-33697	Cocos AI is a confidential computing system for AI. The current implementation of attested TLS (aTLS) in CoCoS is vulnerable to a relay attack affecting all versions from v0.4.0 through v0.8.2. This vulnerability is present in both the AMD SEV-SNP and Intel TDX deployment targets supported by CoCoS. In the affected design, an attacker may be able to extract the ephemeral TLS private key used during the intra-handshake attestation. Because the attestation evidence is bound to the ephemeral key but not to the TLS channel, possession of that key is sufficient to relay or divert the attested TLS session. A client will accept the connection under false assumptions about the endpoint it is communicating with — the attestation report cannot distinguish the genuine attested service from the attacker's relay. This undermines the intended authentication guarantees of attested TLS. A successful attack may allow an attacker to impersonate an attested CoCoS service and access data or operations that the client intended to send only to the genuine attested endpoint. Exploitation requires the attacker to first extract the ephemeral TLS private key, which is possible through physical access to the server hardware, transient execution attacks, or side-channel attacks. Note that the aTLS implementation was fully redesigned in v0.7.0, but the redesign does not address this vulnerability. The relay attack weakness is architectural and affects all releases in the v0.4.0–v0.8.2 range. This vulnerability class was formally analyzed and demonstrated across multiple attested TLS implementations, including CoCoS, by researchers whose findings were disclosed to the IETF TLS Working Group. Formal verification was conducted using ProVerif. As of time of publication, there is no patch available. No complete workaround is available. The following hardening measures reduce but do not eliminate the risk: Keep TEE firmware and microcode up to date to reduce the key-extraction surface; define strict attestation policies that validate all available report fields, including firmware versions, TCB levels, and platform configuration registers; and/or enable mutual aTLS with CA-signed certificates where deployment architecture permits.	7.5	More Details
CVE-2025-27260	Ericsson Indoor Connect 8855 versions prior to 2025.Q3 contains an Improper Filtering of Special Elements vulnerability which, if exploited, can lead to unauthorized modification of certain information	7.5	More Details
CVE-2026-3608	Sending a maliciously crafted message to the kea-ctrl-agent, kea-dhcp-ddns, kea-dhcp4, or kea-dhcp6 daemons over any configured API socket or HA listener can cause the receiving daemon to exit with a stack overflow error. This issue affects Kea versions 2.6.0 through 2.6.4 and 3.0.0 through 3.0.2.	7.5	More Details
CVE-2026-3104	A specially crafted domain can be used to cause a memory leak in a BIND resolver simply by querying this domain. This issue affects BIND 9 versions 9.20.0 through 9.20.20, 9.21.0 through 9.21.19, and 9.20.9-S1 through 9.20.20-S1. BIND 9 versions 9.18.0 through 9.18.46 and 9.18.11-S1 through 9.18.46-S1 are NOT affected.	7.5	More Details
CVE-2026-24363	Missing Authorization vulnerability in loopus WP Cost Estimation & Payment Forms Builder WP_Estimation_Form allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Cost Estimation & Payment Forms Builder: from n/a through < 10.3.0.	7.5	More Details
CVE-2026-32286	The DataRow.Decode function fails to properly validate field lengths. A malicious or compromised PostgreSQL server can send a DataRow message with a negative field length, causing a slice bounds out of range panic.	7.5	More Details
CVE-2026-24372	Authentication Bypass by Spoofing vulnerability in WP Swings Subscriptions for WooCommerce subscriptions-for-woocommerce allows Input Data Manipulation.This issue affects Subscriptions for WooCommerce: from n/a through <= 1.8.10.	7.5	More Details
CVE-2026-24382	Missing Authorization vulnerability in wproyal News Magazine X news-magazine-x allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects News Magazine X: from n/a through <= 1.2.50.	7.5	More Details
CVE-2026-4652	On a system exposing an NVMe/TCP target, a remote client can trigger a kernel panic by sending a CONNECT command for an I/O queue with a bogus or stale CNTLID. An attacker with network access to the NVMe/TCP target can trigger an unauthenticated Denial of Service condition on the affected machine.	7.5	More Details
CVE-2026-4247	When a challenge ACK is to be sent tcp_respond() constructs and sends the challenge ACK and consumes the mbuf that is passed in. When no challenge ACK should be sent the function returns and leaks the mbuf. If an attacker is either on path with an established TCP connection, or can themselves establish a TCP connection, to an affected FreeBSD machine, they can easily craft and send packets which meet the challenge ACK criteria and cause the FreeBSD host to leak an mbuf for each crafted packet in excess of the configured rate limit settings i.e. with default settings, crafted packets in excess of the first 5 sent within a 1s period will leak an mbuf. Technically, off-path attackers can also exploit this problem by guessing the IP addresses, TCP port numbers and in some cases the sequence numbers of established connections and spoofing packets towards a FreeBSD machine, but this is harder to do effectively.	7.5	More Details
CVE-2026-27880	The OpenFeature feature toggle evaluation endpoint reads unbounded values into memory, which can cause out-of-memory crashes.	7.5	More Details
CVE-2026-29871	A path traversal vulnerability exists in the awesome-llm-apps project in commit e46690f99c3f08be80a9877fab52acacf7ab8251 (2026-01-19) in the Beifong AI News and Podcast Agent backend in FastAPI backend, stream-audio endpoint, in file routers/podcast_router.py, in function stream_audio. The stream-audio endpoint accepts a user-controlled path parameter that is concatenated into a filesystem path without proper validation or restriction. An unauthenticated remote attacker can exploit this vulnerability to read arbitrary files from the server filesystem, potentially disclosing sensitive information such as configuration files and credentials.	7.5	More Details
CVE-2026-30637	Server-Side Request Forgery (SSRF) vulnerability exists in the AnnounContent of the /admin/read.php in OTCMS V7.66 and before. The vulnerability allows remote attackers to craft HTTP requests, without authentication, containing a URL pointing to internal services or any remote server	7.5	More Details
CVE-2026-32285	The Delete function fails to properly validate offsets when processing malformed JSON input. This can lead to a negative slice index and a runtime panic, allowing a denial of service attack.	7.5	More Details
CVE-2026-34731	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the AVideo on_publish_done.php endpoint in the Live plugin allows unauthenticated users to terminate any active live stream. The endpoint processes RTMP callback events to mark streams as finished in the database, but performs no authentication or authorization checks before doing so. An attacker can enumerate active stream keys from the unauthenticated stats.json.php endpoint, then send crafted POST requests to on_publish_done.php to terminate any live broadcast. This enables denial-of-service against all live streaming functionality on the platform. At time of publication, there are no publicly available patches.	7.5	More Details
CVE-2026-	goxmlsig provides XML Digital Signatures implemented in Go. Prior to version 1.6.0, the `validateSignature` function in `validate.go` goes through the references in the `SignedInfo` block to find one that matches the signed element's ID. In Go versions before 1.22, or when `go.mod` uses an older version, there is a loop variable capture issue. The code takes the address of the loop variable `_ref` instead of its	7.5	More

33487	value. As a result, if more than one reference matches the ID or if the loop logic is incorrect, the `ref` pointer will always end up pointing to the last element in the `SignedInfo.References` slice after the loop. goxmlsig version 1.6.0 contains a patch.		Details
CVE-2026-32284	The msgpack decoder fails to properly validate the input buffer length when processing truncated fixext data (format codes 0xd4-0xd8). This can lead to an out-of-bounds read and a runtime panic, allowing a denial of service attack.	7.5	More Details
CVE-2026-25002	Authentication Bypass Using an Alternate Path or Channel vulnerability in ThimPress LearnPress – Sepay Payment learnpress-sepay-payment allows Authentication Abuse.This issue affects LearnPress – Sepay Payment: from n/a through <= 4.0.0.	7.5	More Details
CVE-2023-7338	Ruckus Unleashed contains a remote code execution vulnerability in the web-based management interface that allows authenticated remote attackers to execute arbitrary code on the system when gateway mode is enabled. Attackers can exploit this vulnerability by sending specially crafted requests through the management interface to achieve arbitrary code execution on affected systems.	7.5	More Details
CVE-2026-30689	A blog.admin v.8.0 and before system's getinfobytoken API interface contains an improper access control which leads to sensitive data exposure. Unauthorized parties can obtain sensitive administrator account information via a valid token, threatening system security.	7.5	More Details
CVE-2026-4926	Impact: A bad regular expression is generated any time you have multiple sequential optional groups (curly brace syntax), such as `{a}{b}{c}:z`. The generated regex grows exponentially with the number of groups, causing denial of service. Patches: Fixed in version 8.4.0. Workarounds: Limit the number of sequential optional groups in route patterns. Avoid passing user-controlled input as route patterns.	7.5	More Details
CVE-2026-20639	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.3. Processing a maliciously crafted string may lead to heap corruption.	7.5	More Details
CVE-2026-34453	SiYuan is a personal knowledge management system. Prior to version 3.6.2, the publish service exposes bookmarked blocks from password-protected documents to unauthenticated visitors. In publish/read-only mode, /api/bookmark/getBookmark filters bookmark results by calling FilterBlocksByPublishAccess(nil, ...). Because the filter treats a nil context as authorized, it skips the publish password check and returns bookmarked blocks from documents configured as Protected. As a result, anyone who can access the publish service can retrieve content from protected documents without providing the required password, as long as at least one block in the document is bookmarked. This issue has been patched in version 3.6.2.	7.5	More Details
CVE-2026-20622	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sequoia 15.7.4, macOS Tahoe 26.3. An app may be able to capture a user's screen.	7.5	More Details
CVE-2026-4867	Impact: A bad regular expression is generated any time you have three or more parameters within a single segment, separated by something that is not a period (.). For example, /:a-:b-:c or /:a-:b-:c-:d. The backtrack protection added in path-to-regexp@0.1.12 only prevents ambiguity for two parameters. With three or more, the generated lookahead does not block single separator characters, so capture groups overlap and cause catastrophic backtracking. Patches: Upgrade to path-to-regexp@0.1.13 Custom regex patterns in route definitions (e.g., /:a-:b([^-/]+)-:c([^-/]+)) are not affected because they override the default capture group. Workarounds: All versions can be patched by providing a custom regular expression for parameters after the first in a single segment. As long as the custom regular expression does not match the text before the parameter, you will be safe. For example, change /:a-:b-:c to /:a-:b([^-/]+)-:c([^-/]+). If paths cannot be rewritten and versions cannot be upgraded, another alternative is to limit the URL length.	7.5	More Details
CVE-2026-27858	Attacker can send a specifically crafted message before authentication that causes managesieve to allocate large amount of memory. Attacker can force managesieve-login to be unavailable by repeatedly crashing the process. Protect access to managesieve protocol, or install fixed version. No publicly available exploits are known.	7.5	More Details
CVE-2025-69358	Missing Authorization vulnerability in Metagauss EventPrime eventprime-event-calendar-management allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects EventPrime: from n/a through <= 4.2.6.0.	7.5	More Details
CVE-2026-33891	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. Prior to version 1.4.0, a Denial of Service (DoS) vulnerability exists in the node-forge library due to an infinite loop in the BigInteger.modInverse() function (inherited from the bundled jsbn library). When modInverse() is called with a zero value as input, the internal Extended Euclidean Algorithm enters an unreachable exit condition, causing the process to hang indefinitely and consume 100% CPU. Version 1.4.0 patches the issue.	7.5	More Details
CVE-2026-5190	Out-of-bounds write in the streaming decoder component in aws-c-event-stream before 0.6.0 might allow a third party operating a server to cause memory corruption leading to arbitrary code execution on a client application that processes crafted event-stream messages. To remediate this issue, users should upgrade to version 0.6.0 or later.	7.5	More Details
CVE-2026-32287	Boolean XPath expressions that evaluate to true can cause an infinite loop in logicalQuery.Select, leading to 100% CPU usage. This can be triggered by top-level selectors such as "1=1" or "true()".	7.5	More Details
CVE-2026-34226	Happy DOM is a JavaScript implementation of a web browser without its graphical user interface. Versions prior to 20.8.9 may attach cookies from the current page origin (`window.location`) instead of the request target URL when `fetch(..., { credentials: "include" })` is used. This can leak cookies from origin A to destination B. Version 20.8.9 fixes the issue.	7.5	More Details
CVE-2026-22448	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in flexcubed PitchPrint pitchprint allows Path Traversal.This issue affects PitchPrint: from n/a through <= 11.1.2.	7.5	More Details
CVE-2026-4987	The SureForms – Contact Form, Payment Form & Other Custom Form Builder plugin for WordPress is vulnerable to Payment Amount Bypass in all versions up to, and including, 2.5.2. This is due to the create_payment_intent() function performing a payment validation solely based on the value of a user-controlled parameter. This makes it possible for unauthenticated attackers to bypass configured form payment-amount validation and create underpriced payment/subscription intents by setting form_id to 0.	7.5	More Details
CVE-2026-22743	Spring AI's spring-ai-neo4j-store contains a Cypher injection vulnerability in Neo4jVectorFilterExpressionConverter. When a user-controlled string is passed as a filter expression key in Neo4jVectorFilterExpressionConverter of spring-ai-neo4j-store, doKey() embeds the key into a backtick-delimited Cypher property accessor (node.`metadata.`) after stripping only double quotes, without escaping embedded backticks.This issue affects Spring AI: from 1.0.0 before 1.0.5, from 1.1.0 before 1.1.4.	7.5	More Details
CVE-	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5,		More

2026-20701	macOS Tahoe 26.4. An app may be able to connect to a network share without user consent.	7.5	Details
CVE-2026-22744	In RedisFilterExpressionConverter of spring-ai-redis-store, when a user-controlled string is passed as a filter value for a TAG field, stringValue() inserts the value directly into the @field:{VALUE} RediSearch TAG block without escaping characters.This issue affects Spring AI: from 1.0.0 before 1.0.5, from 1.1.0 before 1.1.4.	7.5	More Details
CVE-2025-59032	ManageSieve AUTHENTICATE command crashes when using literal as SASL initial response. This can be used to crash ManageSieve service repeatedly, making it unavailable for other users. Control access to ManageSieve port, or disable the service if it's not needed. Alternatively upgrade to a fixed version. No publicly available exploits are known.	7.5	More Details
CVE-2026-23806	Missing Authorization vulnerability in BlueGlass Interactive AG Jobs for WordPress job-postings allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Jobs for WordPress: from n/a through <= 2.8.	7.5	More Details
CVE-2026-23977	Missing Authorization vulnerability in WPFactory Helpdesk Support Ticket System for WooCommerce support-ticket-system-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Helpdesk Support Ticket System for WooCommerce: from n/a through <= 2.1.2.	7.5	More Details
CVE-2026-34381	Admidio is an open-source user management solution. From version 5.0.0 to before version 5.0.8, Admidio relies on adm_my_files/.htaccess to deny direct HTTP access to uploaded documents. The Docker image ships with AllowOverride None in the Apache configuration, which causes Apache to silently ignore all .htaccess files. As a result, any file uploaded to the documents module regardless of the role-based permissions configured in the UI, is directly accessible over HTTP without authentication by anyone who knows the file path. The file path is disclosed in the upload response JSON. This issue has been patched in version 5.0.8.	7.5	More Details
CVE-2026-33896	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. Prior to version 1.4.0, `pki.verifyCertificateChain()` does not enforce RFC 5280 basicConstraints requirements when an intermediate certificate lacks both the `basicConstraints` and `keyUsage` extensions. This allows any leaf certificate (without these extensions) to act as a CA and sign other certificates, which node-forge will accept as valid. Version 1.4.0 patches the issue.	7.4	More Details
CVE-2026-34359	HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. Prior to version 6.9.4, ManagedWebAccessUtils.getServer() uses String.startsWith() to match request URLs against configured server URLs for authentication credential dispatch. Because configured server URLs (e.g., http://tx.fhir.org) lack a trailing slash or host boundary check, an attacker-controlled domain like http://tx.fhir.org.attacker.com matches the prefix and receives Bearer tokens, Basic auth credentials, or API keys when the HTTP client follows a redirect to that domain. This issue has been patched in version 6.9.4.	7.4	More Details
CVE-2026-20004	A vulnerability in the TLS library of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to exhaust the available memory of an affected device. This vulnerability is due to improper management of memory resources during TLS connection setup. An attacker could exploit this vulnerability by repeatedly triggering the conditions that cause the memory increase. This could be done in a variety of ways, such as by repeatedly attempting Extensible Authentication Protocol (EAP) authentication when local EAP is enabled on an affected device or by using a machine-in-the-middle attack and resetting TLS connections between the affected device and other devices. A successful exploit could allow the attacker to exhaust the available memory on an affected device, resulting in an unexpected reload and a denial of service (DoS) condition.	7.4	More Details
CVE-2026-27856	Doveadm credentials are verified using direct comparison which is susceptible to timing oracle attack. An attacker can use this to determine the configured credentials. Figuring out the credential will lead into full access to the affected component. Limit access to the doveadm http service port, install fixed version. No publicly available exploits are known.	7.4	More Details
CVE-2026-33247	NATS-Server is a High-Performance server for NATS.io, a cloud and edge native messaging system. Prior to versions 2.11.15 and 2.12.6, if a nats-server is run with static credentials for all clients provided via argv (the command-line), then those credentials are visible to any user who can see the monitoring port, if that too is enabled. The `/debug/vars` end-point contains an unredacted copy of argv. Versions 2.11.15 and 2.12.6 contain a fix. As a workaround, configure credentials inside a configuration file instead of via argv, and do not enable the monitoring port if using secrets in argv. Best practice remains to not expose the monitoring port to the Internet, or to untrusted network sources.	7.4	More Details
CVE-2026-33745	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.39.0, the cpp-httplib HTTP client forwards stored Basic Auth, Bearer Token, and Digest Auth credentials to arbitrary hosts when following cross-origin HTTP redirects (301/302/307/308). A malicious or compromised server can redirect the client to an attacker-controlled host, which then receives the plaintext credentials in the `Authorization` header. Version 0.39.0 fixes the issue.	7.4	More Details
CVE-2026-29953	SQL Injection vulnerability in SchemaHero 0.23.0 via the column parameter to the columnAsInsert function in file plugins/postgres/lib/column.go.	7.4	More Details
CVE-2026-33724	n8n is an open source workflow automation platform. Prior to version 2.5.0, when the Source Control feature is configured to use SSH, the SSH command used for git operations explicitly disabled host key verification. A network attacker positioned between the n8n instance and the remote Git server could intercept the connection and present a fraudulent host key, potentially injecting malicious content into workflows or intercepting repository data. This issue only affects instances where the Source Control feature has been explicitly enabled and configured to use SSH (non-default). The issue has been fixed in n8n version 2.5.0. Users should upgrade to this version or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations: Disable the Source Control feature if it is not actively required, and/or restrict network access to ensure the n8n instance communicates with the Git server only over trusted, controlled network paths. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	7.4	More Details
CVE-2026-33643	SQL Injection vulnerability in SchemaHero 0.23.0 via the column parameter to the mysqlColumnAsInsert function in file plugins/mysql/lib/column.go.	7.4	More Details
CVE-2026-5210	A vulnerability was detected in SourceCodester Leave Application System 1.0. This affects an unknown part. Performing a manipulation of the argument page results in file inclusion. Remote exploitation of the attack is possible. The exploit is now public and may be used.	7.3	More Details
CVE-2026-33430	Briefcase is a tool for converting a Python project into a standalone native application. Starting in version 0.3.0 and prior to version 0.3.26, if a developer uses Briefcase to produce an Windows MSI installer for a project, and that project is installed for All Users (i.e., per-machine scope), the installation process creates an directory that inherits all the permissions of the parent directory. Depending on the location chosen by the installing user, this may allow a low privilege but authenticated user to replace or modify the binaries installed by the application. If an administrator then runs the altered binary, the binary will run with elevated privileges. The problem is caused by the template used to generate the WXS file for Windows projects. It was fixed in the templates used in Briefcase 0.3.26, 0.4.0, and 0.4.1. Re-running `briefcase create` on your	7.3	More Details

	Briefcase project will result in the updated templates being used. As a workaround, the patch can be added to any existing Briefcase .wxs file generated by Briefcase 0.3.24 or later.		
CVE-2026-4784	A vulnerability was found in code-projects Simple Laundry System 1.0. This affects an unknown function of the file /checkcheckout.php of the component Parameter Handler. The manipulation of the argument serviceId results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-33664	Kestra is an open-source, event-driven orchestration platform Versions up to and including 1.3.3 render user-supplied flow YAML metadata fields — description, inputs[].displayName, inputs[].description — through the Markdown.vue component instantiated with html: true. The resulting HTML is injected into the DOM via Vue's v-html without any sanitization. This allows a flow author to embed arbitrary JavaScript that executes in the browser of any user who views or interacts with the flow. This is distinct from GHSA-r36c-83hm-pc8j / CVE-2026-29082, which covers only FilePreview.vue rendering .md files from execution outputs. The present finding affects different components, different data sources, and requires significantly less user interaction (zero-click for input.displayName). As of time of publication, it is unclear if a patch is available.	7.3	More Details
CVE-2026-5198	A vulnerability was determined in code-projects Student Membership System 1.0. The impacted element is an unknown function of the file /admin/index.php of the component Admin Login. This manipulation of the argument username/password causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-4838	A flaw has been found in SourceCodester Malawi Online Market 1.0. The impacted element is an unknown function of the file /display.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-5195	A flaw has been found in code-projects Student Membership System 1.0. This issue affects some unknown processing of the component User Registration Handler. Executing a manipulation can lead to sql injection. The attack can be launched remotely.	7.3	More Details
CVE-2026-5002	A vulnerability has been found in PromtEngineer localGPT up to 4d41c7d1713b16b216d8e062e51a5dd88b20b054. The impacted element is the function _route_using_overviews of the file backend/server.py of the component LLM Prompt Handler. Such manipulation leads to injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-5000	A vulnerability was detected in PromtEngineer localGPT up to 4d41c7d1713b16b216d8e062e51a5dd88b20b054. Impacted is the function LocalGPTHandler of the file backend/server.py of the component API Endpoint. The manipulation of the argument BaseHTTPRequestHandler results in missing authentication. The attack can be executed remotely. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-4998	A weakness has been identified in Sinaptik AI PandasAI up to 3.0.0. This vulnerability affects the function CodeExecutor.execute of the file pandasai/core/code_execution/code_executor.py of the component Chat Message Handler. Executing a manipulation can lead to code injection. 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.	7.3	More Details
CVE-2026-5182	A vulnerability was found in SourceCodester Teacher Record System 1.0. Impacted is an unknown function of the file Teacher Record System of the component Parameter Handler. Performing a manipulation of the argument searchteacher results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-4908	A security flaw has been discovered in code-projects Simple Laundry System 1.0. This affects an unknown function of the file /modstaffinfo.php of the component Parameter Handler. The manipulation of the argument userid results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-4910	A security vulnerability has been detected in Shenzhen Ruiming Technology Streamax Crocus up to 1.3.44. Affected is an unknown function of the file /RemoteFormat.do of the component Endpoint. Such manipulation of the argument State leads to sql 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 but did not respond in any way.	7.3	More Details
CVE-2026-4959	A vulnerability was found in OpenBMB XAgent 1.0.0. This impacts the function check_user of the file XAgentServer/application/websockets/share.py of the component ShareServer WebSocket Endpoint. Performing a manipulation of the argument interaction_id results in missing authentication. 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 but did not respond in any way.	7.3	More Details
CVE-2026-1679	The eswifi socket offload driver copies user-provided payloads into a fixed buffer without checking available space; oversized sends overflow `eswifi->buf`, corrupting kernel memory (CWE-120). Exploit requires local code that can call the socket send API; no remote attacker can reach it directly.	7.3	More Details
CVE-2026-4990	A security vulnerability has been detected in chatwoot up to 4.11.1. The affected element is an unknown function of the file /app/login of the component Signup Endpoint. Such manipulation of the argument signupEnabled with the input true leads to improper authorization. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-4860	A security flaw has been discovered in 648540858 wvp-GB28181-pro up to 2.7.4. This affects the function GenericFastJsonRedisSerializer of the file src/main/java/com/genersoft/iot/vmp/conf/redis/RedisTemplateConfig.java of the component API Endpoint. The manipulation results in deserialization. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-4850	A security flaw has been discovered in code-projects Simple Laundry System 1.0. Affected is an unknown function of the file /checkregisitem.php of the component Parameter Handler. The manipulation of the argument Long-arm-shirtVol results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-4844	A vulnerability was detected in code-projects Online Food Ordering System 1.0. This issue affects some unknown processing of the file /admin.php of the component Admin Login Module. The manipulation of the argument Username results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	7.3	More Details
CVE-2026-4842	A security vulnerability has been detected in itsourcecode Online Enrollment System 1.0. This vulnerability affects unknown code of the file /sms/grades/index.php?view=edit&id=1 of the component Parameter Handler. The manipulation of the argument deptid leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details

CVE-2026-4841	A weakness has been identified in code-projects Online Food Ordering System 1.0. This affects an unknown part of the file form/cart.php of the component Shopping Cart Module. Executing a manipulation of the argument del can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-4956	A vulnerability was detected in Shenzhen Ruiming Technology Streamax Crocus 1.3.44. The affected element is an unknown function of the file /DevicePrint.do?Action=ReadTask of the component Parameter Handler. The manipulation of the argument State results in sql injection. 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.	7.3	More Details
CVE-2026-4955	A vulnerability was found in Shenzhen Ruiming Technology Streamax Crocus 1.3.44. This impacts an unknown function of the file /OperateStatistic.do. The manipulation of the argument VehicleID results in sql injection. 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.	7.3	More Details
CVE-2026-4839	A vulnerability has been found in SourceCodester Food Ordering System 1.0. This affects an unknown function of the file /purchase.php of the component Parameter Handler. The manipulation of the argument custom leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-4953	A weakness has been identified in mingSoft MCMS up to 5.5.0. This issue affects the function catchImage of the file net/mingsoft/cms/action/BaseAction.java of the component Editor Endpoint. Executing a manipulation of the argument catchimage can lead to server-side request forgery. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-5001	A flaw has been found in PromtEngineer localGPT up to 4d41c7d1713b16b216d8e062e51a5dd88b20b054. The affected element is the function do_POST of the file backend/server.py. This manipulation causes unrestricted upload. The attack is possible to be carried out remotely. The exploit has been published and may be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-4996	A vulnerability was identified in Sinaptik AI PandasAI up to 0.1.4. Affected by this issue is the function delete_question_and_answers/delete_docs/update_question_answer/update_docs/get_relevant_question_answers_by_id/get_relevant_docs_by_id of the file extensions/ee/vectorstores/lancedb/pandasai_lancedb/lancedb.py of the component pandasai-lancedb Extension. Such manipulation leads to sql injection. 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.	7.3	More Details
CVE-2026-5012	A flaw has been found in elecV2 elecV2P up to 3.8.3. This issue affects the function pm2run of the file /rpc. Executing a manipulation can lead to os command injection. The attack can be executed remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-32979	OpenClaw before 2026.3.11 contains an approval integrity vulnerability allowing attackers to execute rewritten local code by modifying scripts between approval and execution when exact file binding cannot occur. Remote attackers can change approved local scripts before execution to achieve unintended code execution as the OpenClaw runtime user.	7.3	More Details
CVE-2026-5180	A flaw has been found in SourceCodester Simple Doctors Appointment System 1.0. This vulnerability affects unknown code of the file /admin/ajax.php?action=login2. This manipulation of the argument email causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-5179	A vulnerability was detected in SourceCodester Simple Doctors Appointment System 1.0. This affects an unknown part of the file /admin/login.php. The manipulation of the argument Username results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-55263	HCL Aftermarket DPC is affected by Hardcoded Sensitive Data which allows attacker to gain access to the source code or if it is stored in insecure repositories, they can easily retrieve these hardcoded secrets.	7.3	More Details
CVE-2026-5176	A security flaw has been discovered in Totolink A3300R 17.0.0cu.557_b20221024. Affected is the function setSyslogCfg of the file /cgi-bin/cstecgi.cgi. Performing a manipulation of the argument provided results in command injection. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-4965	A vulnerability was detected in letta-ai letta 0.16.4. This issue affects the function resolve_type of the file letta/functions/ast_parsers.py of the component Incomplete Fix CVE-2025-6101. Performing a manipulation results in improper neutralization of directives in dynamically evaluated code. The attack can be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-5150	A security vulnerability has been detected in code-projects Accounting System 1.0. This issue affects some unknown processing of the file /viewin_costumer.php of the component Parameter Handler. Such manipulation of the argument cos_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-5016	A vulnerability was identified in elecV2 elecV2P up to 3.8.3. This affects the function eAxios of the file /mock of the component URL Handler. Such manipulation of the argument req leads to server-side request forgery. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-5147	A security flaw has been discovered in YunaiV yudao-cloud up to 2026.01. This affects an unknown part of the file /admin-api/system/tenant/get-by-website. The manipulation of the argument Website results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-5237	A security flaw has been discovered in itsourcecode Payroll Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /manage_user.php of the component Parameter Handler. Performing a manipulation of the argument ID results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-5035	A vulnerability has been found in code-projects Accounting System 1.0. This affects an unknown part of the file /view_work.php of the component Parameter Handler. Such manipulation of the argument en_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-5017	A security flaw has been discovered in code-projects Simple Food Order System 1.0. This impacts an unknown function of the file /all-tickets.php of the component Parameter Handler. Performing a manipulation of the argument Status results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details

CVE-2026-5034	A flaw has been found in code-projects Accounting System 1.0. Affected by this issue is some unknown functionality of the file /edit_costumer.php of the component Parameter Handler. This manipulation of the argument cos_id causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-5033	A vulnerability was detected in code-projects Accounting System 1.0. Affected by this vulnerability is an unknown functionality of the file /view_costumer.php of the component Parameter Handler. The manipulation of the argument cos_id results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	7.3	More Details
CVE-2026-5019	A security vulnerability has been detected in code-projects Simple Food Order System 1.0. Affected by this vulnerability is an unknown functionality of the file all-orders.php of the component Parameter Handler. The manipulation of the argument Status leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-5018	A weakness has been identified in code-projects Simple Food Order System 1.0. Affected is an unknown function of the file register-router.php of the component Parameter Handler. Executing a manipulation of the argument Name can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-2231	The Fluent Booking plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters in all versions up to, and including, 2.0.01 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-2026-3328	The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to PHP Object Injection via deserialization of the 'post_content' of admin_form posts in all versions up to, and including, 3.28.31. This is due to the use of WordPress's `maybe_unserialize()` function without class restrictions on user-controllable content stored in admin_form post content. This makes it possible for authenticated attackers, with Editor-level access and above, to inject a PHP Object. The additional presence of a POP chain allows attackers to achieve remote code execution.	7.2	More Details
CVE-2026-4329	The Blackhole for Bad Bots plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the User-Agent HTTP header in all versions up to and including 3.8. This is due to insufficient input sanitization and output escaping. The plugin uses sanitize_text_field() when capturing bot data (which strips HTML tags but does not escape HTML entities like double quotes), then stores the data via update_option(). When an administrator views the Bad Bots log page, the stored data is output directly into HTML input value attributes (lines 75-83) without esc_attr() and into HTML span content without esc_html(). This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute when an administrator views the Blackhole Bad Bots admin page.	7.2	More Details
CVE-2026-27602	Modoboa is a mail hosting and management platform. Prior to version 2.7.1, `exec_cmd()` in `modoboa/lib/sysutils.py` always runs subprocess calls with `shell=True`. Since domain names flow directly into shell command strings without any sanitization, a Reseller or SuperAdmin can include shell metacharacters in a domain name to run arbitrary OS commands on the server. Version 2.7.1 patches the issue.	7.2	More Details
CVE-2026-33504	Ory Hydra is an OAuth 2.0 Server and OpenID Connect Provider. Prior to version 26.2.0, the listOAuth2Clients, listOAuth2ConsentSessions, and listTrustedOAuth2JwtGrantIssuers Admin APIs in Ory Hydra are vulnerable to SQL injection due to flaws in its pagination implementation. Pagination tokens are encrypted using the secret configured in `secrets.pagination`. If this value is not set, Hydra falls back to using `secrets.system`. An attacker who knows this secret can craft their own tokens, including malicious tokens that lead to SQL injection. This issue can be exploited when one or more admin APIs listed above are directly or indirectly accessible to the attacker; the attacker can pass a raw pagination token to the affected API; and the configuration value `secrets.pagination` is set and known to the attacker, or `secrets.pagination` is not set and `secrets.system` is known to the attacker. An attacker can execute arbitrary SQL queries through forged pagination tokens. As a first line of defense, immediately configure a custom value for `secrets.pagination` by generating a cryptographically secure random secret. Next, upgrade Hydra to the fixed version, 26.2.0 as soon as possible.	7.2	More Details
CVE-2026-33503	Ory Kratos is an identity, user management and authentication system for cloud services. Prior to version 26.2.0, the ListCourierMessages Admin API in Ory Kratos is vulnerable to SQL injection due to flaws in its pagination implementation. Pagination tokens are encrypted using the secret configured in `secrets.pagination`. An attacker who knows this secret can craft their own tokens, including malicious tokens that lead to SQL injection. If this configuration value is not set, Kratos falls back to a default pagination encryption secret. Because this default value is publicly known, attackers can generate valid and malicious pagination tokens manually for installations where this secret is not set. As a first line of defense, immediately configure a custom value for `secrets.pagination` by generating a cryptographically secure random secret. Next, upgrade Kratos** to a fixed version, 26.2.0 or later, as soon as possible.	7.2	More Details
CVE-2026-33914	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, the PostCalendar module contains a blind SQL injection vulnerability in the `categoriesUpdate` administrative function. The `dels` POST parameter is read via `pnVarCleanFromInput()`, which only strips HTML tags and performs no SQL escaping. The value is then interpolated directly into a raw SQL `DELETE` statement that is executed unsanitized via Doctrine DBAL's `executeStatement()`. Version 8.0.0.3 patches the issue.	7.2	More Details
CVE-2025-69986	A buffer overflow vulnerability exists in the ONVIF GetStreamUri function of LSC Indoor Camera V7.6.32. The application fails to validate the length of the Protocol parameter inside the Transport element. By sending a specially crafted SOAP request containing an oversized protocol string, an attacker can overflow the stack buffer, overwriting the return instruction pointer (RIP). This vulnerability allows for Denial of Service (DoS) via device crash or Remote Code Execution (RCE) in the context of the ONVIF service.	7.2	More Details
CVE-2026-33725	Metabase is an open source business intelligence and embedded analytics tool. In Metabase Enterprise prior to versions 1.54.22, 1.55.22, 1.56.22, 1.57.16, 1.58.10, and 1.59.4, authenticated admins on Metabase Enterprise Edition can achieve Remote Code Execution (RCE) and Arbitrary File Read via the `POST /api/ee/serialization/import` endpoint. A crafted serialization archive injects an `INIT` property into the H2 JDBC spec, which can execute arbitrary SQL during a database sync. We confirmed this was possible on Metabase Cloud. This only affects Metabase Enterprise. Metabase OSS lacks the affected codepaths. All versions of Metabase Enterprise that have serialization, which dates back to at least version 1.47, are affected. Metabase Enterprise versions 1.54.22, 1.55.22, 1.56.22, 1.57.16, 1.58.10, and 1.59.4 patch the issue. As a workaround, disable the serialization import endpoint in their Metabase instance to prevent access to the vulnerable codepaths.	7.2	More Details
CVE-2026-33910	OpenEMR is a free and open source electronic health records and medical practice management application. Versions up to and including 8.0.0.2 contain a SQL injection vulnerability in the patient selection feature that can be exploited by authenticated attackers. The vulnerability exists due to insufficient input validation in the patient selection feature. Version 8.0.0.3 contains a patch.	7.2	More Details
CVE-2026-33505	Ory Keto is am open source authorization server for managing permissions at scale. Prior to version 26.2.0, the GetRelationships API in Ory Keto is vulnerable to SQL injection due to flaws in its pagination implementation. Pagination tokens are encrypted using the secret configured in `secrets.pagination`. An attacker who knows this secret can craft their own tokens, including malicious tokens that lead to SQL injection. If this configuration value is not set, Keto falls back to a hard-coded default pagination encryption secret. Because this default value is publicly known, attackers can generate valid and malicious pagination tokens manually for installations where this secret is not set. This issue can be exploited when GetRelationships API is directly or indirectly accessible to the attacker, the attacker can pass a raw pagination token to the affected API, and the configuration value `secrets.pagination` is not set or known to the attacker. An attacker can execute arbitrary SQL queries through forged pagination tokens. As a first line of defense, immediately configure a custom value for `secrets.pagination` by generating a cryptographically secure random secret. Next, upgrade Keto to a fixed version, 26.2.0 or later, as soon as possible.	7.2	More Details

CVE-2025-12886	The Oxygen Theme theme for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 6.0.8 via the laborator_calc_route AJAX action. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	7.2	More Details
CVE-2026-33906	Ella Core is a 5G core designed for private networks. Prior to version 1.7.0, the NetworkManager role was granted backup and restore permission. The restore endpoint accepted any valid SQLite file without verifying its contents. A NetworkManager could replace the production database with a tampered copy to escalate to Admin, gaining access to user management, audit logs, debug endpoints, and operator identity configuration that the role was explicitly denied. In version 1.7.0, backup and restore permissions have been removed from the NetworkManager role.	7.2	More Details
CVE-2026-22480	Deserialization of Untrusted Data vulnerability in WebToffee Product Feed for WooCommerce webtoffee-product-feed allows Object Injection.This issue affects Product Feed for WooCommerce: from n/a through <= 2.3.3.	7.2	More Details
CVE-2024-51347	A buffer overflow vulnerability in the dgiot binary in LSC Smart Indoor IP Camera V7.6.32. The flaw exists in the handling of the Time Zone (TZ) parameter within the ONVIF configuration interface. The time zone (TZ) parameter does not have its length properly validated before being copied into a fixed-size buffer using the insecure strcpy function.	7.2	More Details
CVE-2026-30940	baserCMS is a website development framework. Prior to version 5.2.3, a path traversal vulnerability exists in the theme file management API (/baser/api/admin/bc-theme-file/theme_files/add.json) that allows arbitrary file write. An authenticated administrator can include ../ sequences in the path parameter to create a PHP file in an arbitrary directory outside the theme directory, which may result in remote code execution (RCE). This issue has been patched in version 5.2.3.	7.2	More Details
CVE-2026-4267	The Query Monitor – The developer tools panel for WordPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the '$_SERVER['REQUEST_URI']' parameter in all versions up to, and including, 3.20.3 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.	7.2	More Details
CVE-2026-25025	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikRestaurants vikrestaurants allows Reflected XSS.This issue affects VikRestaurants: from n/a through <= 1.5.2.	7.1	More Details
CVE-2026-25033	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uixthemes Motta Addons motta-addons allows Reflected XSS.This issue affects Motta Addons: from n/a through < 1.6.1.	7.1	More Details
CVE-2026-25304	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Jaroti jaroti allows Reflected XSS.This issue affects Jaroti: from n/a through < 1.4.8.	7.1	More Details
CVE-2026-25349	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Loobek loobek allows Reflected XSS.This issue affects Loobek: from n/a through < 1.5.2.	7.1	More Details
CVE-2026-25306	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 8theme XStore Core et-core-plugin allows Reflected XSS.This issue affects XStore Core: from n/a through <= 5.6.4.	7.1	More Details
CVE-2026-25341	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RSJoomla! RSFirewall! rsfirewall allows Stored XSS.This issue affects RSFirewall!: from n/a through <= 1.1.45.	7.1	More Details
CVE-2026-25342	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kutethemes Boutique kute-boutique allows Reflected XSS.This issue affects Boutique: from n/a through < 2.4.6.	7.1	More Details
CVE-2026-25346	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro FAQ Builder AYS faq-builder-ays allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects FAQ Builder AYS: from n/a through <= 1.8.2.	7.1	More Details
CVE-2026-25018	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in stmcan NaturaLife Extensions naturalife-extensions allows Reflected XSS.This issue affects NaturaLife Extensions: from n/a through <= 2.1.	7.1	More Details
CVE-2026-25013	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WHMCSdes Phox Hosting phox-host allows Reflected XSS.This issue affects Phox Hosting: from n/a through <= 2.0.8.	7.1	More Details
CVE-2026-25347	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Acato WP REST Cache wp-rest-cache allows Stored XSS.This issue affects WP REST Cache: from n/a through <= 2026.1.0.	7.1	More Details
CVE-2026-23979	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Softwebmedia Gyan Elements gyan-elements allows Reflected XSS.This issue affects Gyan Elements: from n/a through <= 2.2.1.	7.1	More Details
CVE-2026-25350	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Miti miti allows Reflected XSS.This issue affects Miti: from n/a through < 1.5.3.	7.1	More Details
CVE-2026-24980	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme Visionary Core noo-visionary-core allows Reflected XSS.This issue affects Visionary Core: from n/a through <= 1.4.9.	7.1	More Details
CVE-2026-25351	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup MyMedi mymedi allows Reflected XSS.This issue affects MyMedi: from n/a through < 1.7.7.	7.1	More Details

CVE-2026-25352	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup MyDecor mydecor allows Reflected XSS.This issue affects MyDecor: from n/a through < 1.5.9.	7.1	More Details
CVE-2026-34053	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, missing authorization in the AJAX deletion endpoint `interface/forms/procedure_order/handle_deletions.php` allows any authenticated user, regardless of role, to irreversibly delete procedure orders, answers, and specimens belonging to any patient in the system. Version 8.0.0.3 patches the issue.	7.1	More Details
CVE-2026-25353	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Nooni nooni allows Reflected XSS.This issue affects Nooni: from n/a through < 1.5.1.	7.1	More Details
CVE-2026-25354	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Reebox reebox allows Reflected XSS.This issue affects Reebox: from n/a through < 1.4.8.	7.1	More Details
CVE-2026-25356	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Yobazar yobazar allows Reflected XSS.This issue affects Yobazar: from n/a through < 1.6.7.	7.1	More Details
CVE-2026-25361	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in magepeopleteam WpEvently mage-eventpress allows Reflected XSS.This issue affects WpEvently: from n/a through <= 5.1.4.	7.1	More Details
CVE-2026-25373	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ProgressionStudios Vayvo vayvo-progression allows Reflected XSS.This issue affects Vayvo: from n/a through < 6.8.	7.1	More Details
CVE-2026-25376	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eyecix Addon Jobsearch Chat addon-jobsearch-chat allows Reflected XSS.This issue affects Addon Jobsearch Chat: from n/a through <= 3.0.	7.1	More Details
CVE-2026-25435	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdevart Booking calendar, Appointment Booking System booking-calendar allows Stored XSS.This issue affects Booking calendar, Appointment Booking System: from n/a through <= 3.2.36.	7.1	More Details
CVE-2026-24983	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UpSolution UpSolution Core us-core allows Reflected XSS.This issue affects UpSolution Core: from n/a through <= 8.41.	7.1	More Details
CVE-2026-24391	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeMakers Car Dealer cardealer allows Reflected XSS.This issue affects Car Dealer: from n/a through <= 1.6.7.	7.1	More Details
CVE-2026-24979	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme Jobica Core jobica-core allows Reflected XSS.This issue affects Jobica Core: from n/a through <= 1.4.1.	7.1	More Details
CVE-2018-25207	Online Quiz Maker 1.0 contains SQL injection vulnerabilities in the catid and usern parameters that allow authenticated attackers to execute arbitrary SQL commands. Attackers can submit malicious POST requests to quiz-system.php or add-category.php with crafted SQL payloads in POST parameters to extract sensitive database information or bypass authentication.	7.1	More Details
CVE-2026-20687	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Tahoe 26.4, tvOS 26.4, watchOS 26.4. An app may be able to cause unexpected system termination or write kernel memory.	7.1	More Details
CVE-2026-33645	Fireshare facilitates self-hosted media and link sharing. In version 1.5.1, an authenticated path traversal vulnerability in Fireshare's chunked upload endpoint allows an attacker to write arbitrary files outside the intended upload directory. The `checkSum` multipart field is used directly in filesystem path construction without sanitization or containment checks. This enables unauthorized file writes to attacker-chosen paths writable by the Fireshare process (e.g., container `/tmp`), violating integrity and potentially enabling follow-on attacks depending on deployment. Version 1.5.2 fixes the issue.	7.1	More Details
CVE-2026-32971	OpenClaw before 2026.3.11 contains an approval-integrity vulnerability in node-host system.run approvals that displays extracted shell payloads instead of the executed argv. Attackers can place wrapper binaries and induce wrapper-shaped commands to execute local code after operators approve misleading command text.	7.1	More Details
CVE-2025-10559	A Path Traversal vulnerability affecting Factory Resource Management in DELMIA Factory Resource Manager from Release 3DEXPERIENCE R2023x through Release 3DEXPERIENCE R2025x allows an attacker to read or write files in specific directories on the server.	7.1	More Details
CVE-2026-32734	baserCMS is a website development framework. Prior to version 5.2.3, baserCMS has DOM-based cross-site scripting in tag creation. This issue has been patched in version 5.2.3.	7.1	More Details
CVE-2026-33987	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.24.2, in persistent_cache_read_entry_v3() in libfreerdp/cache/persistent.c, persistent->bmpSize is updated before winpr_aligned_recalloc(). If realloc fails, bmpSize is inflated while bmpData points to the old buffer. This issue has been patched in version 3.24.2.	7.1	More Details
CVE-2026-33982	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.24.2, there is a heap-buffer-overflow READ vulnerability at 24 bytes before the allocation, in winpr_aligned_offset_recalloc(). This issue has been patched in version 3.24.2.	7.1	More Details
CVE-2026-28788	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to version 0.8.6, any authenticated user can overwrite any file's content by ID through the `POST /api/v1/retrieval/process/files/batch` endpoint. The endpoint performs no ownership check, so a regular user with read access to a shared knowledge base can obtain file UUIDs via `GET /api/v1/knowledge/{id}/files` and then overwrite those files, escalating from read to write. The overwritten content is served to the LLM via RAG, meaning the attacker controls what the model tells other users. Version 0.8.6 patches the issue.	7.1	More Details

CVE-2026-34472	Unauthenticated credential disclosure in the wizard interface in ZTE ZXHN H188A V6.0.10P2_TE and V6.0.10P3N3_TE allows unauthenticated attackers on the local network to retrieve sensitive credentials from the router's web management interface, including the default administrator password, WLAN PSK, and PPPoE credentials. In some observed cases, configuration changes may also be performed without authentication.	7.1	More Details
CVE-2026-32972	OpenClaw before 2026.3.11 contains an authorization bypass vulnerability allowing authenticated operators with only operator.write permission to access admin-only browser profile management routes through browser.request. Attackers can create or modify browser profiles and persist attacker-controlled remote CDP endpoints to disk without holding operator.admin privileges.	7.1	More Details
CVE-2025-69096	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in G5Theme Zorka zorka allows Reflected XSS.This issue affects Zorka: from n/a through <= 1.5.7.	7.1	More Details
CVE-2026-24975	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme Organici Library noo-organici-library allows Reflected XSS.This issue affects Organici Library: from n/a through <= 2.1.2.	7.1	More Details
CVE-2018-25201	School Management System CMS 1.0 contains an SQL injection vulnerability in the admin login functionality that allows attackers to bypass authentication by injecting SQL code through the username parameter. Attackers can submit malicious payloads using boolean-based blind SQL injection techniques to the processlogin endpoint to authenticate as administrator without valid credentials.	7.1	More Details
CVE-2026-22491	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wphocus My auctions allegro my-auctions-allegro-free-edition allows Reflected XSS.This issue affects My auctions allegro: from n/a through <= 3.6.35.	7.1	More Details
CVE-2026-22520	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in G5Theme Handmade Framework handmade-framework allows Reflected XSS.This issue affects Handmade Framework: from n/a through <= 3.9.	7.1	More Details
CVE-2026-22523	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themepassion Ultra WordPress Admin ultra-admin allows Reflected XSS.This issue affects Ultra WordPress Admin: from n/a through <= 11.7.	7.1	More Details
CVE-2026-22524	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themepassion Legacy Admin legacy-admin allows Reflected XSS.This issue affects Legacy Admin: from n/a through <= 9.5.	7.1	More Details
CVE-2026-23807	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Socio WP Telegram Widget and Join Link wptelegram-widget allows Reflected XSS.This issue affects WP Telegram Widget and Join Link: from n/a through <= 2.2.13.	7.1	More Details
CVE-2026-23973	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uxper Golo golo allows Reflected XSS.This issue affects Golo: from n/a through < 1.7.5.	7.1	More Details
CVE-2026-24369	Missing Authorization vulnerability in Theme-one The Grid the-grid allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Grid: from n/a through < 2.8.0.	7.1	More Details
CVE-2026-25461	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in purethemes Listeo Core listeo-core allows Reflected XSS.This issue affects Listeo Core: from n/a through <= 2.0.21.	7.1	More Details
CVE-2026-24973	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme CitiLights noo-citilights allows Reflected XSS.This issue affects CitiLights: from n/a through <= 3.7.1.	7.1	More Details
CVE-2026-25452	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPDO Remoji remoji allows Stored XSS.This issue affects Remoji: from n/a through <= 2.2.	7.1	More Details
CVE-2026-25383	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Iqonic Design KiviCare kivicare-clinic-management-system allows Reflected XSS.This issue affects KiviCare: from n/a through <= 3.6.16.	7.1	More Details
CVE-2026-32528	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in don-themes Riode riode allows Reflected XSS.This issue affects Riode: from n/a through < 1.6.29.	7.1	More Details
CVE-2026-32540	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bookly Bookly bookly-responsive-appointment-booking-tool allows Reflected XSS.This issue affects Bookly: from n/a through <= 26.7.	7.1	More Details
CVE-2026-27088	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in G5Theme Darna Framework darna-framework allows Reflected XSS.This issue affects Darna Framework: from n/a through <= 2.9.	7.1	More Details
CVE-2026-32494	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Image Slider by Ays ays-slider allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Image Slider by Ays: from n/a through <= 2.7.1.	7.1	More Details
CVE-2026-33217	NATS-Server is a High-Performance server for NATS.io, a cloud and edge native messaging system. Prior to versions 2.11.15 and 2.12.6, when using ACLs on message subjects, these ACLs were not applied in the `$MQTT.>` namespace, allowing MQTT clients to bypass ACL checks for MQTT subjects. Versions 2.11.15 and 2.12.6 contain a fix. No known workarounds are available.	7.1	More Details
CVE-2026-32501	Missing Authorization vulnerability in wp-configurator WP Configurator Pro wp-configurator-pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Configurator Pro: from n/a through <= 3.7.9.	7.1	More Details
CVE-			

2026-27087	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in G5Theme Wolverine Framework wolverine-framework allows Reflected XSS.This issue affects Wolverine Framework: from n/a through <= 1.9.	7.1	More Details
CVE-2026-32517	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kleor Contact Manager contact-manager allows Reflected XSS.This issue affects Contact Manager: from n/a through <= 9.1.	7.1	More Details
CVE-2026-27054	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Soledad Data Migrator penci-data-migrator allows Reflected XSS.This issue affects Penci Soledad Data Migrator: from n/a through <= 1.3.1.	7.1	More Details
CVE-2026-32518	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in imithemes Gaea gaea allows Reflected XSS.This issue affects Gaea: from n/a through < 3.8.	7.1	More Details
CVE-2026-32526	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VillaTheme Abandoned Cart Recovery for WooCommerce woo-abandoned-cart-recovery allows Stored XSS.This issue affects Abandoned Cart Recovery for WooCommerce: from n/a through <= 1.1.10.	7.1	More Details
CVE-2026-32529	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in don-themes Molla molla allows Reflected XSS.This issue affects Molla: from n/a through < 1.5.19.	7.1	More Details
CVE-2026-32532	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeHunk Contact Form & Lead Form Elementor Builder lead-form-builder allows Stored XSS.This issue affects Contact Form & Lead Form Elementor Builder: from n/a through <= 2.0.1.	7.1	More Details
CVE-2025-36258	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 product stores user credentials and other sensitive information in plain text which can be read by a local user.	7.1	More Details
CVE-2026-32544	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OOPSpam Team OOPSpam Anti-Spam oopspam-anti-spam allows Stored XSS.This issue affects OOPSpam Anti-Spam: from n/a through <= 1.2.62.	7.1	More Details
CVE-2026-32545	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Taboola Taboola Pixel taboola-pixel allows Reflected XSS.This issue affects Taboola Pixel: from n/a through <= 1.1.4.	7.1	More Details
CVE-2026-32542	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeFusion Fusion Builder fusion-builder allows Reflected XSS.This issue affects Fusion Builder: from n/a through < 3.15.0.	7.1	More Details
CVE-2026-4962	A security flaw has been discovered in UltraVNC up to 1.6.4.0. Affected by this issue is some unknown functionality in the library version.dll of the component Service. The manipulation results in uncontrolled search path. The attack needs to be approached locally. This attack is characterized by high complexity. The exploitation is known to be difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.0	More Details
CVE-2026-4824	A vulnerability has been found in Enter Software Iperius Backup up to 8.7.3. Affected by this issue is some unknown functionality of the component Backup Job Configuration File Handler. The manipulation leads to improper privilege management. The attack must be carried out locally. The attack is considered to have high complexity. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. Upgrading to version 8.7.4 can resolve this issue. 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.	7.0	More Details
CVE-2026-4822	A vulnerability was detected in Enter Software Iperius Backup up to 8.7.3. Affected is an unknown function of the file C:\ProgramData\IperiusBackup\Jobs\ of the component Backup Service. Performing a manipulation results in creation of temporary file with insecure permissions. The attack is only possible with local access. A high degree of complexity is needed for the attack. The exploitability is told to be difficult. The exploit is now public and may be used. Upgrading to version 8.7.4 is able to address this issue. It is recommended 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.	7.0	More Details
CVE-2026-26074	EVerest is an EV charging software stack. Versions prior to 2026.02.0 have a data race leading to possible `std::map<std::queue>` corruption. The trigger is CSMS GetLog/UpdateFirmware request (network) with an EVSE fault event (physical). This results in TSAN reports concurrent access (data race) to `event_queue`. Version 2026.2.0 contains a patch.	7.0	More Details
CVE-2026-1724	GitLab has remediated an issue in GitLab EE affecting all versions from 18.5 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1 that could have allowed an unauthenticated user to access API tokens of self-hosted AI models due to improper access control.	6.8	More Details
CVE-2026-4818	In Search Guard FLX versions from 3.0.0 up to 4.0.1, there exists an issue which allows users without the necessary privileges to execute some management operations against data streams.	6.8	More Details
CVE-2026-3112	Mattermost versions 11.4.x <= 11.4.0, 11.3.x <= 11.3.1, 11.2.x <= 11.2.3, 10.11.x <= 10.11.11 fail to validate Advanced Logging file target paths which allows system administrators to read arbitrary host files via malicious AdvancedLoggingJSON configuration in support packet generation. Mattermost Advisory ID: MMSA-2025-00562	6.8	More Details
CVE-2026-4346	The vulnerability affecting TL-WR850N v3 allows cleartext storage of administrative and Wi-Fi credentials in a region of the device’s flash memory while the serial interface remains enabled and protected by weak authentication. An attacker with physical access and the ability to connect to the serial port can recover sensitive information, including the router’s management password and wireless network key. Successful exploitation can lead to full administrative control of the device and unauthorized access to the associated wireless network.	6.8	More Details
CVE-2026-33486	Roadiz is a polymorphic content management system based on a node system that can handle many types of services. A vulnerability in roadiz/documents prior to versions 2.7.9, 2.6.28, 2.5.44, and 2.3.42 allows an authenticated attacker to read any file on the server's local file system that the web server process has access to, including highly sensitive environment variables, database credentials, and internal configuration files. Versions 2.7.9, 2.6.28, 2.5.44, and 2.3.42 contain a patch.	6.8	More Details

CVE-2026-27855	Dovecot OTP authentication is vulnerable to replay attack under specific conditions. If auth cache is enabled, and username is altered in passdb, then OTP credentials can be cached so that same OTP reply is valid. An attacker able to observe an OTP exchange is able to log in as the user. If authentication happens over unsecure connection, switch to SCRAM protocol. Alternatively ensure the communcations are secured, and if possible switch to OAUTH2 or SCRAM. No publicly available exploits are known.	6.8	More Details
CVE-2025-15433	The Shared Files WordPress plugin before 1.7.58 allows users with a role as low as Contributor to download any file on the web server (such as wp-config.php) via a path traversal vector	6.8	More Details
CVE-2026-25328	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in add-ons.org Product File Upload for WooCommerce products-file-upload-for-woocommerce allows Path Traversal.This issue affects Product File Upload for WooCommerce: from n/a through <= 2.2.4.	6.8	More Details
CVE-2025-43534	A path handling issue was addressed with improved validation. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.2 and iPadOS 26.2. A user with physical access to an iOS device may be able to bypass Activation Lock.	6.8	More Details
CVE-2026-31951	LibreChat is a ChatGPT clone with additional features. In versions 0.8.2-rc1 through 0.8.3-rc1, user-created MCP (Model Context Protocol) servers can include arbitrary HTTP headers that undergo credential placeholder substitution. An attacker can create a malicious MCP server with headers containing `{{LIBRECHAT_OPENID_ACCESS_TOKEN}}` (and others), causing victims who call tools on that server to have their OAuth tokens exfiltrated. Version 0.8.3-rc2 fixes the issue.	6.8	More Details
CVE-2026-33997	Moby is an open source container framework. Prior to version 29.3.1, a security vulnerability has been detected that allows plugins privilege validation to be bypassed during docker plugin install. Due to an error in the daemon's privilege comparison logic, the daemon may incorrectly accept a privilege set that differs from the one approved by the user. Plugins that request exactly one privilege are also affected, because no comparison is performed at all. This issue has been patched in version 29.3.1.	6.8	More Details
CVE-2026-32567	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in icopydoc YML for Yandex Market yml-for-yandex-market allows Path Traversal.This issue affects YML for Yandex Market: from n/a through < 5.3.0.	6.8	More Details
CVE-2026-2745	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 7.11 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1 that could have allowed an unauthenticated user to bypass WebAuthn two-factor authentication and gain unauthorized access to user accounts due to inconsistent input validation in the authentication process.	6.8	More Details
CVE-2026-33623	PinchTab is a standalone HTTP server that gives AI agents direct control over a Chrome browser. PinchTab `v0.8.4` contains a Windows-only command injection issue in the orphaned Chrome cleanup path. When an instance is stopped, the Windows cleanup routine builds a PowerShell `-Command` string using a `needle` derived from the profile path. In `v0.8.4`, that string interpolation escapes backslashes but does not safely neutralize other PowerShell metacharacters. If an attacker can launch an instance using a crafted profile name and then trigger the cleanup path, they may be able to execute arbitrary PowerShell commands on the Windows host in the security context of the PinchTab process user. This is not an unauthenticated internet RCE. It requires authenticated, administrative-equivalent API access to instance lifecycle endpoints, and the resulting command execution inherits the permissions of the PinchTab OS user rather than bypassing host privilege boundaries. Version 0.8.5 contains a patch for the issue.	6.7	More Details
CVE-2025-15616	Wazuh wazuh-agent and wazuh-manager versions 2.1.0 before 4.8.0 contain multiple shell injection and untrusted search path vulnerabilities that allow attackers to execute arbitrary commands through various components including logcollector configuration, maild SMTP server tags, and Kaspersky AR script parameters. Attackers can exploit these vulnerabilities by injecting malicious commands through configuration files, SMTP server settings, and custom flags to achieve remote code execution on affected systems.	6.7	More Details
CVE-2025-14917	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.3 IBM WebSphere Application Server Liberty could provide weaker than expected security when administering security settings.	6.7	More Details
CVE-2026-5165	A flaw was found in virtio-win, specifically within the VirtIO Block (BLK) device. When the device undergoes a reset, it fails to properly manage memory, resulting in a use-after-free vulnerability. This issue could allow a local attacker to corrupt system memory, potentially leading to system instability or unexpected behavior.	6.7	More Details
CVE-2026-32496	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in NYSL Spam Protect for Contact Form 7 wp-contact-form-7-spam-blocker allows Path Traversal.This issue affects Spam Protect for Contact Form 7: from n/a through <= 1.2.9.	6.7	More Details
CVE-2026-5164	A flaw was found in virtio-win. The `RhelDoUnMap()` function does not properly validate the number of descriptors provided by a user during an unmap request. A local user could exploit this input validation vulnerability by supplying an excessive number of descriptors, leading to a buffer overrun. This can cause a system crash, resulting in a Denial of Service (DoS).	6.7	More Details
CVE-2026-28879	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. Processing maliciously crafted web content may lead to an unexpected process crash.	6.5	More Details
CVE-2026-25437	Missing Authorization vulnerability in سید محمدامین هاشمی GZSEO gzseo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects GZSEO: from n/a through <= 2.0.14.	6.5	More Details
CVE-2026-3527	Missing Authentication for Critical Function vulnerability in Drupal AJAX Dashboard allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AJAX Dashboard: from 0.0.0 before 3.1.0.	6.5	More Details
CVE-2026-3531	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal OpenID Connect / OAuth client allows Authentication Bypass.This issue affects OpenID Connect / OAuth client: from 0.0.0 before 1.5.0.	6.5	More Details
CVE-2026-24029	When the early_acl_drop (earlyACLDrop in Lua) option is disabled (default is enabled) on a DNS over HTTPs frontend using the nghttp2 provider, the ACL check is skipped, allowing all clients to send DoH queries regardless of the configured ACL.	6.5	More Details
CVE-2026-28880	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, visionOS 26.4. An app may be able to enumerate a user's installed apps.	6.5	More Details

CVE-2026-33576	OpenClaw before 2026.3.28 downloads and stores inbound media from Zalo channels before validating sender authorization. Unauthorized senders can force network fetches and disk writes to the media store by sending messages that are subsequently rejected.	6.5	More Details
CVE-2026-25430	Missing Authorization vulnerability in CRM Perks Integration for Mailchimp and Contact Form 7, WPForms, Elementor, Ninja Forms cf7-mailchimp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Integration for Mailchimp and Contact Form 7, WPForms, Elementor, Ninja Forms: from n/a through <= 1.2.2.	6.5	More Details
CVE-2026-29905	Kirby CMS through 5.1.4 allows an authenticated user with 'Editor' permissions to cause a persistent Denial of Service (DoS) via a malformed image upload. The application fails to properly validate the return value of the PHP getimagesize() function. When the system attempts to process this file for metadata or thumbnail generation, it triggers a fatal TypeError.	6.5	More Details
CVE-2026-34508	OpenClaw before 2026.3.12 applies rate limiting only after webhook authentication succeeds, allowing attackers to bypass rate limits and brute-force webhook secrets without triggering 429 responses. Attackers can repeatedly guess invalid secrets to discover valid credentials and subsequently submit forged Zalo webhook traffic.	6.5	More Details
CVE-2026-34505	OpenClaw before 2026.3.12 applies rate limiting only after successful webhook authentication, allowing attackers to bypass rate limits and brute-force webhook secrets. Attackers can submit repeated authentication requests with invalid secrets without triggering rate limit responses, enabling systematic secret guessing and subsequent forged webhook submission.	6.5	More Details
CVE-2026-32976	OpenClaw before 2026.3.11 contains an authorization bypass vulnerability allowing channel commands to mutate protected sibling-account configuration despite configWrites restrictions. Attackers with authorized access on one account can execute channel commands like /config set channels.<provider>.accounts.<id> to modify configuration on target accounts with configWrites: false.	6.5	More Details
CVE-2026-27496	n8n is an open source workflow automation platform. Prior to versions 1.123.22, 2.9.3, and 2.10.1, an authenticated user with permission to create or modify workflows could use the JavaScript Task Runner to allocate uninitialized memory buffers. Uninitialized buffers may contain residual data from the same Node.js process — including data from prior requests, tasks, secrets, or tokens — resulting in information disclosure of sensitive in-process data. Task Runners must be enabled using `N8N_RUNNERS_ENABLED=true`. In external runner mode, the impact is limited to data within the external runner process. The issue has been fixed in n8n versions 1.123.22, 2.10.1 , and 2.9.3. Users should upgrade to this version or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations: Limit workflow creation and editing permissions to fully trusted users only, and/or use external runner mode (`N8N_RUNNERS_MODE=external`) to isolate the runner process. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	6.5	More Details
CVE-2026-27663	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.10), RTUM85 RTU Base (All versions < V26.10). The affected application contains denial-of-service (DoS) vulnerability. The remote operation mode is susceptible to a resource exhaustion condition when subjected to a high volume of requests. Sending multiple requests can exhaust resources, preventing parameterization and requiring a reset or reboot to restore functionality.	6.5	More Details
CVE-2026-25417	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Metagauss ProfileGrid profilegrid-user-profiles-groups-and-communities allows Stored XSS.This issue affects ProfileGrid : from n/a through <= 5.9.8.1.	6.5	More Details
CVE-2026-34887	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Extend Themes Kubio AI Page Builder allows Stored XSS.This issue affects Kubio AI Page Builder: from n/a through 2.7.0.	6.5	More Details
CVE-2026-33983	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.24.2, progressive_decompress_tile_upgrade() detects a mismatch via progressive_rfx_quant_cmp_equal() but only emits WLog_WARN, execution continues. The wrapped value (247) is used as a shift exponent, causing undefined behavior and an approximately 80 billion iteration loop (CPU DoS). This issue has been patched in version 3.24.2.	6.5	More Details
CVE-2026-33693	Lemmy is a link aggregator and forum for the fediverse. Prior to version 0.7.0-beta.9, the `v4_is_invalid()` function in `activitypub-federation-rust` (`src/utils.rs`) does not check for `Ipv4Addr::UNSPECIFIED` (0.0.0.0). An unauthenticated attacker controlling a remote domain can point it to 0.0.0.0, bypass the SSRF protection introduced by the fix for CVE-2025-25194 (GHSA-7723-35v7-qcxw), and reach localhost services on the target server. Version 0.7.0-beta.9 patches the issue.	6.5	More Details
CVE-2026-33515	Squid is a caching proxy for the Web. Prior to version 7.5, due to improper input validation, Squid is vulnerable to out of bounds read when handling ICP traffic. This problem allows a remote attacker to receive small amounts of memory potentially containing sensitive information when responding with errors to invalid ICP requests. This attack is limited to Squid deployments that explicitly enable ICP support (i.e. configure non-zero `icp_port`). This problem cannot be mitigated by denying ICP queries using `icp_access` rules. Version 7.5 contains a patch.	6.5	More Details
CVE-2026-29597	Incorrect access control in the file_details.asp endpoint of DDSN Interactive Acora CMS v10.7.1 allows attackers with editor privileges to access sensitive files via crafted requests.	6.5	More Details
CVE-2026-25390	Missing Authorization vulnerability in Saad Iqbal New User Approve new-user-approve allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects New User Approve: from n/a through <= 3.2.3.	6.5	More Details
CVE-2026-25627	NanoMQ MQTT Broker (NanoMQ) is an all-around Edge Messaging Platform. Prior to version 0.24.8, NanoMQ's MQTT-over-WebSocket transport can be crashed by sending an MQTT packet with a deliberately large Remaining Length in the fixed header while providing a much shorter actual payload. The code path copies Remaining Length bytes without verifying that the current receive buffer contains that many bytes, resulting in an out-of-bounds read (ASAN reports OOB / crash). This is remotely triggerable over the WebSocket listener. This issue has been patched in version 0.24.8.	6.5	More Details
CVE-2026-32533	Authorization Bypass Through User-Controlled Key vulnerability in LatePoint LatePoint latepoint allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects LatePoint: from n/a through <= 5.2.6.	6.5	More Details
CVE-2026-32535	Authorization Bypass Through User-Controlled Key vulnerability in JoomSky JS Help Desk js-support-ticket allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JS Help Desk: from n/a through <= 3.0.3.	6.5	More Details
CVE-2026-32541	Missing Authorization vulnerability in Premmerce Premmerce Redirect Manager premmerce-redirect-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Premmerce Redirect Manager: from n/a through <= 1.0.12.	6.5	More Details

CVE-2026-33663	n8n is an open source workflow automation platform. Prior to versions 2.14.1, 2.13.3, and 1.123.27, an authenticated user with the `global:member` role could exploit chained authorization flaws in n8n's credential pipeline to steal plaintext secrets from generic HTTP credentials (`httpBasicAuth`, `httpHeaderAuth`, `httpQueryAuth`) belonging to other users on the same instance. The attack abuses a name-based credential resolution path that does not enforce ownership or project scope, combined with a bypass in the credentials permission checker that causes generic HTTP credential types to be skipped during pre-execution validation. Together, these flaws allow a member-role user to resolve another user's credential ID and execute a workflow that decrypts and uses that credential without authorization. Native integration credential types (e.g. `slackApi`, `openAiApi`, `postgres`) are not affected by this issue. This vulnerability affects Community Edition only. Enterprise Edition has additional permission gates on workflow creation and execution that independently block this attack chain. The issue has been fixed in n8n versions 1.123.27, 2.13.3, and 2.14.1. Users should upgrade to one of these versions or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations: Restrict instance access to fully trusted users only, and/or audit credentials stored on the instance and rotate any generic HTTP credentials (`httpBasicAuth`, `httpHeaderAuth`, `httpQueryAuth`) that may have been exposed. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	6.5	More Details
CVE-2026-25398	Missing Authorization vulnerability in Webilia Inc. Vertex Addons for Elementor addons-for-elementor-builder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Vertex Addons for Elementor: from n/a through <= 1.6.4.	6.5	More Details
CVE-2026-34036	Dolibarr is an enterprise resource planning (ERP) and customer relationship management (CRM) software package. In versions 22.0.4 and prior, there is a Local File Inclusion (LFI) vulnerability in the core AJAX endpoint /core/ajax/selectobject.php. By manipulating the objectdesc parameter and exploiting a fail-open logic flaw in the core access control function restrictedArea(), an authenticated user with no specific privileges can read the contents of arbitrary non-PHP files on the server (such as .env, .htaccess, configuration backups, or logs...). At time of publication, there are no publicly available patches.	6.5	More Details
CVE-2026-33743	Incus is a system container and virtual machine manager. Prior to version 6.23.0, a specially crafted storage bucket backup can be used by an user with access to Incus' storage bucket feature to crash the Incus daemon. Repeated use of this attack can be used to keep the server offline causing a denial of service of the control plane API. This does not impact any running workload, existing containers and virtual machines will keep operating. Version 6.23.0 fixes the issue.	6.5	More Details
CVE-2026-1710	The WooPayments: Integrated WooCommerce Payments plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'save_upe_appearance_ajax' function in all versions up to, and including, 10.5.1. This makes it possible for unauthenticated attackers to update plugin settings.	6.5	More Details
CVE-2026-33580	OpenClaw before 2026.3.28 contains a missing rate limiting vulnerability in the Nextcloud Talk webhook authentication that allows attackers to brute-force weak shared secrets. Attackers who can reach the webhook endpoint can exploit this to forge inbound webhook events by repeatedly attempting authentication without throttling.	6.5	More Details
CVE-2026-28878	A privacy issue was addressed by removing sensitive data. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sonoma 14.8.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An app may be able to enumerate a user's installed apps.	6.5	More Details
CVE-2026-33541	TSPortal is the WikiTide Foundation’s in-house platform used by the Trust and Safety team to manage reports, investigations, appeals, and transparency work. Prior to version 34, a flaw in TSPortal allowed attackers to create arbitrary user records in the database by abusing validation logic. While validation correctly rejected invalid usernames, a side effect within a validation rule caused user records to be created regardless of whether the request succeeded. This could be exploited to cause uncontrolled database growth, leading to a potential denial of service (DoS). Version 34 contains a fix for the issue.	6.5	More Details
CVE-2026-33581	OpenClaw before 2026.3.24 contains a sandbox bypass vulnerability in the message tool that allows attackers to read arbitrary local files by using mediaUrl and fileUrl alias parameters that bypass localRoots validation. Remote attackers can exploit this by routing file requests through unvalidated alias parameters to access files outside the intended sandbox directory.	6.5	More Details
CVE-2026-33730	Open Source Point of Sale (opensourcepos) is a web based point of sale application written in PHP using CodeIgniter framework. Prior to version 3.4.2, an Insecure Direct Object Reference (IDOR) vulnerability allows an authenticated low-privileged user to access the password change functionality of other users, including administrators, by manipulating the `employee_id` parameter. The application does not verify object ownership or enforce authorization checks. Version 3.4.2 adds object-level authorization checks to validate that the current user owns the employee_id being accessed.	6.5	More Details
CVE-2026-20690	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. Processing an audio stream in a maliciously crafted media file may terminate the process.	6.5	More Details
CVE-2026-25455	Missing Authorization vulnerability in PickPlugins Product Slider for WooCommerce woocommerce-products-slider allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Product Slider for WooCommerce: from n/a through <= 1.13.60.	6.5	More Details
CVE-2026-33495	ORY Oathkeeper is an Identity & Access Proxy (IAP) and Access Control Decision API that authorizes HTTP requests based on sets of Access Rules. Ory Oathkeeper is often deployed behind other components like CDNs, WAFs, or reverse proxies. Depending on the setup, another component might forward the request to the Oathkeeper proxy with a different protocol (http vs. https) than the original request. In order to properly match the request against the configured rules, Oathkeeper considers the `X-Forwarded-Proto` header when evaluating rules. The configuration option `serve.proxy.trust_forwarded_headers` (defaults to false) governs whether this and other `X-Forwarded-*` headers should be trusted. Prior to version 26.2.0, Oathkeeper did not properly respect this configuration, and would always consider the `X-Forwarded-Proto` header. In order for an attacker to abuse this, an installation of Ory Oathkeeper needs to have distinct rules for HTTP and HTTPS requests. Also, the attacker needs to be able to trigger one but not the other rule. In this scenario, the attacker can send the same request but with the `X-Forwarded-Proto` header in order to trigger the other rule. We do not expect many configurations to meet these preconditions. Version 26.2.0 contains a patch. Ory Oathkeeper will correctly respect the `serve.proxy.trust_forwarded_headers` configuration going forward, thereby eliminating the attack scenario. We recommend upgrading to a fixed version even if the preconditions are not met. As an additional mitigation, it is generally recommended to drop any unexpected headers as early as possible when a request is handled, e.g. in the WAF.	6.5	More Details
CVE-2026-34733	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the AVideo installation script install/deleteSystemdPrivate.php contains a PHP operator precedence bug in its CLI-only access guard. The script is intended to run exclusively from the command line, but the guard condition !php_sapi_name() === 'cli' never evaluates to true due to how PHP resolves operator precedence. The ! (logical NOT) operator binds more tightly than === (strict comparison), causing the expression to always evaluate to false, which means the die() statement never executes. As a result, the script is accessible via HTTP without authentication and will delete files from the server's temp directory while also disclosing the temp directory contents in its response. At time of publication, there are no publicly available patches.	6.5	More Details
CVE-	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the StripeYPT plugin includes a test.php debug endpoint that is accessible to any logged-in user, not just administrators. This endpoint processes Stripe webhook-style payloads and triggers subscription		More

2026-34737	operations, including cancellation. Due to a bug in the retrieveSubscriptions() method that cancels subscriptions instead of merely retrieving them, any authenticated user can cancel arbitrary Stripe subscriptions by providing a subscription ID. At time of publication, there are no publicly available patches.	6.5	Details
CVE-2026-34740	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the EPG (Electronic Program Guide) link feature in AVideo allows authenticated users with upload permissions to store arbitrary URLs that the server fetches on every EPG page visit. The URL is validated only with PHP's FILTER_VALIDATE_URL, which accepts internal network addresses. Although AVideo has a dedicated isSSRFSafeURL() function for preventing SSRF, it is not called in this code path. This results in a stored server-side request forgery vulnerability that can be used to scan internal networks, access cloud metadata services, and interact with internal services. At time of publication, there are no publicly available patches.	6.5	More Details
CVE-2026-2436	A flaw was found in libsoup's SoupServer. A remote attacker could exploit a use-after-free vulnerability where the `soup_server_disconnect()` function frees connection objects prematurely, even if a TLS handshake is still pending. If the handshake completes after the connection object has been freed, a dangling pointer is accessed, leading to a server crash and a Denial of Service.	6.5	More Details
CVE-2026-20665	This issue was addressed through improved state management. This issue is fixed in Safari 26.4, iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.	6.5	More Details
CVE-2026-28503	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. In versions prior to 2.6.0, the `SyncViewSet.query_synced_folder()` action in `cookbook/views/api.py` (line 903) fetches a Sync object using `get_object_or_404(Sync, pk=pk)` without including `space=request.space` in the filter. This allows an admin user in Space A to trigger sync operations (Dropbox/Nextcloud/Local import) on Sync configurations belonging to Space B, and view the resulting sync logs. Version 2.6.0 patches the issue.	6.5	More Details
CVE-2026-20657	The issue was addressed with improved memory handling. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5. Parsing a maliciously crafted file may lead to an unexpected app termination.	6.5	More Details
CVE-2026-3121	A flaw was found in Keycloak. An administrator with `manage-clients` permission can exploit a misconfiguration where this permission is equivalent to `manage-permissions`. This allows the administrator to escalate privileges and gain control over roles, users, or other administrative functions within the realm. This privilege escalation can occur when admin permissions are enabled at the realm level.	6.5	More Details
CVE-2026-34401	XML Notepad is a Windows program that provides a simple intuitive User Interface for browsing and editing XML documents. Prior to version 2.9.0.21, XML Notepad does not disable DTD processing by default which means external entities are resolved automatically. There is a well known attack related to malicious DTD files where an attacker to craft a malicious XML file that loads a DTD that causes XML Notepad to make outbound HTTP/SMB requests, potentially leaking local file contents or capturing the victim's NTLM credentials. This issue has been patched in version 2.9.0.21.	6.5	More Details
CVE-2026-33148	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. In versions prior to 2.6.0, the FDC (USDA FoodData Central) search endpoint constructs an upstream API URL by directly interpolating the user-supplied `query` parameter into the URL string without URL-encoding. An attacker can inject additional URL parameters by including `&` characters in the query value. This allows overriding the API key, manipulating upstream query behavior, and causing server crashes (HTTP 500) via malformed requests — a Denial of Service condition. Version 2.6.0 patches the issue.	6.5	More Details
CVE-2026-33153	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. In versions prior to 2.6.0, the Recipe API endpoint exposes a hidden `?debug=true` query parameter that returns the complete raw SQL query being executed, including all table names, column names, JOIN relationships, WHERE conditions (revealing access control logic), and multi-tenant space IDs. This parameter works even when Django's `DEBUG=False` (production mode) and is accessible to any authenticated user regardless of their privilege level. This allows a low-privilege attacker to map the entire database schema and reverse-engineer the authorization model. Version 2.6.0 patches the issue.	6.5	More Details
CVE-2026-33954	LinkAce is a self-hosted archive to collect website links. In versions prior to 2.5.3, a private note attached to a non-private link can be disclosed to a different authenticated user via the web interface. The API appears to correctly enforce note visibility, but the web link detail page renders notes without applying equivalent visibility filtering. As a result, an authenticated user who is allowed to view another user's `internal` or `public` link can read that user's `private` notes attached to the link. Version 2.5.3 patches the issue.	6.5	More Details
CVE-2026-25454	Missing Authorization vulnerability in MVPThemes The League the-league allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The League: from n/a through <= 4.4.1.	6.5	More Details
CVE-2026-34613	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the AVideo endpoint objects/pluginSwitch.json.php allows administrators to enable or disable any installed plugin. The endpoint checks for an active admin session but does not validate a CSRF token. Additionally, the plugins database table is explicitly listed in ignoreTableSecurityCheck(), which means the ORM-level Referer/Origin domain validation in ObjectYPT::save() is also bypassed. Combined with SameSite=None on session cookies, an attacker can disable critical security plugins (such as LoginControl for 2FA, subscription enforcement, or access control plugins) by luring an admin to a malicious page. At time of publication, there are no publicly available patches.	6.5	More Details
CVE-2026-34611	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the AVideo endpoint objects/emailAllUsers.json.php allows administrators to send HTML emails to every registered user on the platform. While the endpoint verifies admin session status, it does not validate a CSRF token. Because AVideo sets SameSite=None on session cookies, a cross-origin POST request from an attacker-controlled page will include the admin's session cookie automatically. An attacker who lures an admin to a malicious page can send an arbitrary HTML email to every user on the platform, appearing to originate from the instance's legitimate SMTP address. At time of publication, there are no publicly available patches.	6.5	More Details
CVE-2026-33469	Frigate is a network video recorder (NVR) with realtime local object detection for IP cameras. In version 0.17.0, an authenticated non-admin user can retrieve the full raw Frigate configuration through `/api/config/raw`. This exposes sensitive values that are intentionally redacted from `/api/config`, including camera credentials, go2rtc stream credentials, MQTT passwords, proxy secrets, and any other secrets stored in `config.yml`. This appears to be a broken access control issue introduced by the admin-by-default API refactor: `/api/config/raw_paths` is admin-only, but `/api/config/raw` is still accessible to any authenticated user. Version 0.17.1 contains a patch.	6.5	More Details
CVE-2026-33375	The Grafana MSSQL data source plugin contains a logic flaw that allows a low-privileged user (Viewer) to bypass API restrictions and trigger a catastrophic Out-Of-Memory (OOM) memory exhaustion, crashing the host container.	6.5	More Details
CVE-2026-	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 26.4 and iPadOS 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An app may be able to fingerprint the user.	6.5	More Details

28863			
CVE-2026-32120	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, an Insecure Direct Object Reference (IDOR) vulnerability in the fee sheet product save logic (`library/FeeSheet.class.php`) allows any authenticated user with fee sheet ACL access to delete, modify, or read `drug_sales` records belonging to arbitrary patients by manipulating the hidden `prod[][sale_id]` form field. The `save()` method uses the user-supplied `sale_id` in five SQL queries (SELECT, UPDATE, DELETE) without verifying that the record belongs to the current patient and encounter. Version 8.0.0.3 contains a patch.	6.5	More Details
CVE-2026-33438	Stirling-PDF is a locally hosted web application that allows you to perform various operations on PDF files. Versions starting in 2.1.5 and prior to 2.5.2 have Denial of Service (DoS) vulnerability in the Stirling-PDF watermark functionality (`/api/v1/security/add-watermark` endpoint). The vulnerability allows authenticated users to cause resource exhaustion and server crashes by providing extreme values for the `fontSize` and `widthSpacer` parameters. Version 2.5.2 patches the issue.	6.5	More Details
CVE-2026-28857	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.4, iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, visionOS 26.4. Processing maliciously crafted web content may lead to an unexpected process crash.	6.5	More Details
CVE-2026-28844	A file access issue was addressed with improved input validation. This issue is fixed in macOS Tahoe 26.4. An attacker may gain access to protected parts of the file system.	6.5	More Details
CVE-2026-33470	Frigate is a network video recorder (NVR) with realtime local object detection for IP cameras. In version 0.17.0, a low-privilege authenticated user restricted to one camera can access snapshots from other cameras. This is possible through a chain of two authorization problems: `/api/timeline` returns timeline entries for cameras outside the caller's allowed camera set, then `/api/events/{event_id}/snapshot-clean.webp` declares `Depends(require_camera_access)` but never actually validates `event.camera` after looking up the event. Together, this allows a restricted user to enumerate event IDs from unauthorized cameras and then fetch clean snapshots for those events. Version 0.17.1 fixes the issue.	6.5	More Details
CVE-2026-34586	PdfDing is a selfhosted PDF manager, viewer and editor offering a seamless user experience on multiple devices. Prior to version 1.7.1, check_shared_access_allowed() validates only session existence — it does not check SharedPdf.inactive (expiration / max views) or SharedPdf.deleted. The Serve and Download endpoints rely solely on this function, allowing previously-authorized users to access shared PDF content after expiration, view limit, or soft-deletion. This issue has been patched in version 1.7.1.	6.5	More Details
CVE-2026-28835	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. Mounting a maliciously crafted SMB network share may lead to system termination.	6.5	More Details
CVE-2026-25465	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codepeople CP Multi View Event Calendar cp-multi-view-calendar allows Stored XSS.This issue affects CP Multi View Event Calendar : from n/a through <= 1.4.35.	6.5	More Details
CVE-2026-2950	Impact: Lodash versions 4.17.23 and earlier are vulnerable to prototype pollution in the _.unset and _.omit functions. The fix for (CVE-2025-13465: https://github.com/lodash/lodash/security/advisories/GHSA-xxjr-mmjv-4gpg) only guards against string key members, so an attacker can bypass the check by passing array-wrapped path segments. This allows deletion of properties from built-in prototypes such as Object.prototype, Number.prototype, and String.prototype. The issue permits deletion of prototype properties but does not allow overwriting their original behavior. Patches: This issue is patched in 4.18.0. Workarounds: None. Upgrade to the patched version.	6.5	More Details
CVE-2026-3114	Mattermost versions 11.4.x <= 11.4.0, 11.3.x <= 11.3.1, 11.2.x <= 11.2.3, 10.11.x <= 10.11.11 fail to validate decompressed archive entry sizes during file extraction which allows authenticated users with file upload permissions to cause a denial of service via crafted zip archives containing highly compressed entries (zip bombs) that exhaust server memory.. Mattermost Advisory ID: MMSA-2026-00598	6.5	More Details
CVE-2026-33528	GoDoxy is a reverse proxy and container orchestrator for self-hosters. Prior to version 0.27.5, the file content API endpoint at `/api/v1/file/content` is vulnerable to path traversal. The `filename` query parameter is passed directly to `path.Join(common.ConfigBasePath, filename)` where `ConfigBasePath = "config"` (a relative path). No sanitization or validation is applied beyond checking that the field is non-empty (`binding:"required"`). An authenticated attacker can use `../` sequences to read or write files outside the intended `config/` directory, including TLS private keys, OAuth refresh tokens, and any file accessible to the container's UID. Version 0.27.5 fixes the issue.	6.5	More Details
CVE-2026-34395	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the plugin/YPTWallet/view/users.json.php endpoint returns all platform users with their personal information and wallet balances to any authenticated user. The endpoint checks User::isLogged() but does not check User::isAdmin(), so any registered user can dump the full user database. At time of publication, there are no publicly available patches.	6.5	More Details
CVE-2026-25469	Missing Authorization vulnerability in ViaBill for WooCommerce ViaBill – WooCommerce viabill-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ViaBill – WooCommerce: from n/a through <= 1.1.53.	6.5	More Details
CVE-2026-31914	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hookandhook WP Courses LMS wp-courses allows DOM-Based XSS.This issue affects WP Courses LMS: from n/a through <= 3.2.26.	6.5	More Details
CVE-2026-5025	The '/logs' and '/logs-stream' endpoints in the log router allow any authenticated user to read the full application log buffer. These endpoints only require basic authentication ('get_current_active_user') without any privilege checks (e.g., 'is_superuser').	6.5	More Details
CVE-2026-24364	Missing Authorization vulnerability in weDevs WP User Frontend wp-user-frontend allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP User Frontend: from n/a through <= 4.2.5.	6.5	More Details
CVE-2026-27879	A resample query can be used to trigger out-of-memory crashes in Grafana.	6.5	More Details
CVE-2026-27877	When using public dashboards and direct data-sources, all direct data-sources' passwords are exposed despite not being used in dashboards. No passwords of proxied data-sources are exposed. We encourage all direct data-sources to be converted to proxied data-sources as far as possible to improve your deployments' security.	6.5	More Details
CVE-2025-	BS Producten Petcam 33.1.0.0818 is vulnerable to Incorrect Access Control. An unauthenticated attacker in physical proximity can associate with this open network. Once connected, the attacker gains access to the camera's private network interface and can retrieve sensitive	6.5	More

69988	information, including the live video and audio stream, without providing credentials.		Details
CVE-2026-24376	Missing Authorization vulnerability in Javier Casares WPVulnerability wpvulnerability allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPVulnerability: from n/a through <= 4.2.1.	6.5	More Details
CVE-2026-24370	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Theme-one The Grid the-grid allows Stored XSS.This issue affects The Grid: from n/a through < 2.8.0.	6.5	More Details
CVE-2023-7339	Stack-based buffer overflow vulnerability in Softing Industrial Automation GmbH gateways allows overflow buffers. This issue affects pnGate: through 1.30 epGate: through 1.30 mbGate: through 1.30 smartLink HW-DP: through 1.30 smartLink HW-PN: through 1.01.	6.5	More Details
CVE-2026-33907	Ella Core is a 5G core designed for private networks. Versions prior to 1.7.0 panic when processing Authentication Response and Authentication Failure NAS message missing IEs. An attacker able to send crafted NAS messages to Ella Core can crash the process, causing service disruption for all connected subscribers. No authentication is required. Version 1.7.0 added IE presence verification to NAS message handling.	6.5	More Details
CVE-2026-33886	Statamic is a Laravel and Git powered content management system (CMS). Starting in version 5.7.12 and prior to versions 5.73.16 and 6.7.2, a control panel user with access to Antlers-enabled fields could access sensitive application configuration values by inserting config variables into their content. This has been fixed in 5.73.16 and 6.7.2.	6.5	More Details
CVE-2026-33931	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, an Insecure Direct Object Reference (IDOR) vulnerability in the patient portal payment page allows any authenticated portal patient to access other patients' payment records — including invoice/billing data (PHI) and payment card metadata — by manipulating the `recid` query parameter in `portal/portal_payment.php`. Version 8.0.0.3 patches the issue.	6.5	More Details
CVE-2026-23972	Missing Authorization vulnerability in magepeopleteam Booking and Rental Manager booking-and-rental-manager-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Booking and Rental Manager: from n/a through <= 2.6.0.	6.5	More Details
CVE-2026-23635	Kiteworks is a private data network (PDN). In Kiteworks Secure Data Forms prior to version 9.2.1, a misconfiguration of the security attributes could potentially lead to Unprotected Transport of Credentials under certain circumstances. Upgrade Kiteworks to version 9.2.1 or later to receive a patch.	6.5	More Details
CVE-2026-33904	Ella Core is a 5G core designed for private networks. Prior to version 1.7.0, a deadlock in the AMF's SCTP notification handler causes the entire AMF control plane to hang until the process is restarted. An attacker with access to the N2 interface can cause Ella Core to hang, resulting in a denial of service for all subscribers. Version 1.7.0 adds deferred Radio cleanup in serveConn SCTP server so that every connection exit path removes the radio. Remove the stale-entry scan from SCTP Notification handling.	6.5	More Details
CVE-2025-14790	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 could allow an attacker to obtain sensitive information due to insufficiently protected credentials.	6.5	More Details
CVE-2026-33903	Ella Core is a 5G core designed for private networks. Versions prior to 1.7.0 panic when processing a specially crafted NGAP LocationReport message. An attacker able to send crafted NGAP messages to Ella Core can crash the process, causing service disruption for all connected subscribers. Version 1.7.0 adds guards in NGAP Location Report handler.	6.5	More Details
CVE-2026-32514	Missing Authorization vulnerability in Anton Voytenko Petitioner petitioner allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Petitioner: from n/a through <= 0.7.3.	6.5	More Details
CVE-2026-22485	Missing Authorization vulnerability in Ruhul Amin My Album Gallery my-album-gallery allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects My Album Gallery: from n/a through <= 1.0.4.	6.5	More Details
CVE-2026-24972	Missing Authorization vulnerability in Elated-Themes Elated Listing eltd-listing allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Elated Listing: from n/a through <= 1.4.	6.5	More Details
CVE-2025-15488	The Responsive Plus WordPress plugin before 3.4.3 is vulnerable to arbitrary shortcode execution due to the software allowing unauthenticated users to execute the update_responsive_woo_free_shipping_left_shortcode AJAX action that does not properly validate the content_rech_data parameter before processing it as a shortcode.	6.5	More Details
CVE-2025-15617	Wazuh version 4.12.0 contains an exposure vulnerability in GitHub Actions workflow artifacts that allows attackers to extract the GITHUB_TOKEN from uploaded artifacts. Attackers can use the exposed token within a limited time window to perform unauthorized actions such as pushing malicious commits or altering release tags.	6.5	More Details
CVE-2026-28375	A testdata data-source can be used to trigger out-of-memory crashes in Grafana.	6.5	More Details
CVE-2026-32483	Missing Authorization vulnerability in codepeople Contact Form Email contact-form-to-email allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Contact Form Email: from n/a through <= 1.3.63.	6.5	More Details
CVE-2026-25339	Insertion of Sensitive Information Into Sent Data vulnerability in Syed Balkhi Contact Form by WPForms wpforms-lite allows Retrieve Embedded Sensitive Data.This issue affects Contact Form by WPForms: from n/a through <= 1.9.8.7.	6.5	More Details
CVE-2026-25344	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in RadiusTheme Review Schema review-schema allows Retrieve Embedded Sensitive Data.This issue affects Review Schema: from n/a through <= 2.2.6.	6.5	More Details
CVE-2026-25327	Missing Authorization vulnerability in Rustaurius Five Star Restaurant Reservations restaurant-reservations allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Five Star Restaurant Reservations: from n/a through <= 2.7.9.	6.5	More Details

CVE-2026-32489	Missing Authorization vulnerability in bPlugins B Blocks b-blocks allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects B Blocks: from n/a through < 2.0.30.	6.5	More Details
CVE-2026-33766	WWBN AVideo is an open source video platform. In versions up to and including 26.0, `isSSRFSafeURL()` validates URLs against private/reserved IP ranges before fetching, but `url_get_contents()` follows HTTP redirects without re-validating the redirect target. An attacker can bypass SSRF protection by redirecting from a public URL to an internal target. Commit 8b7e9dad359d5fac69e0cbbb370250e0b284bc12 contains a patch.	6.5	More Details
CVE-2026-25034	Missing Authorization vulnerability in Iqonic Design KiviCare kivicare-clinic-management-system allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects KiviCare: from n/a through <= 3.6.16.	6.5	More Details
CVE-2025-14915	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.3 IBM WebSphere Application Server Liberty is affected by privilege escalation. A privileged user could gain additional access to the application server.	6.5	More Details
CVE-2026-33750	The brace-expansion library generates arbitrary strings containing a common prefix and suffix. Prior to versions 5.0.5, 3.0.2, 2.0.3, and 1.1.13, a brace pattern with a zero step value (e.g., `{1..2..0}`) causes the sequence generation loop to run indefinitely, making the process hang for seconds and allocate heaps of memory. Versions 5.0.5, 3.0.2, 2.0.3, and 1.1.13 fix the issue. As a workaround, sanitize strings passed to `expand()` to ensure a step value of `0` is not used.	6.5	More Details
CVE-2026-32490	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jgwhite33 WP TripAdvisor Review Slider wp-tripadvisor-review-slider allows Stored XSS.This issue affects WP TripAdvisor Review Slider: from n/a through <= 14.1.	6.5	More Details
CVE-2026-25009	Missing Authorization vulnerability in raratheme Education Zone education-zone allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Education Zone: from n/a through <= 1.3.8.	6.5	More Details
CVE-2026-24987	Missing Authorization vulnerability in activity-log.com WP System Log winterlock allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP System Log: from n/a through <= 1.2.7.	6.5	More Details
CVE-2026-32491	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jgwhite33 WP Review Slider wp-facebook-reviews allows Stored XSS.This issue affects WP Review Slider: from n/a through <= 13.9.	6.5	More Details
CVE-2025-14807	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking.	6.5	More Details
CVE-2026-1014	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable to exposure of sensitive information via JSON server response manipulation.	6.5	More Details
CVE-2026-25355	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Sanzo sanzo allows Stored XSS.This issue affects Sanzo: from n/a through < 2.4.3.	6.5	More Details
CVE-2026-33882	Statamic is a Laravel and Git powered content management system (CMS). Prior to versions 5.73.16 and 6.7.2, the markdown preview endpoint could be manipulated to return augmented data from arbitrary fieldtypes. With the users fieldtype specifically, an authenticated control panel user could retrieve sensitive user data including email addresses, encrypted passkey data, and encrypted two-factor authentication codes. This has been fixed in 5.73.16 and 6.7.2.	6.5	More Details
CVE-2026-33268	Nanoleaf Lines 12.3.2 does not authenticate firmware file uploads. A remote, unauthenticated attacker can upload firmware files on the device and consume storage resources. Fixed in 12.3.6.	6.5	More Details
CVE-2026-32527	Missing Authorization vulnerability in CRM Perks WP Insightly for Contact Form 7, WPForms, Elementor, Formidable and Ninja Forms cf7-insightly allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Insightly for Contact Form 7, WPForms, Elementor, Formidable and Ninja Forms: from n/a through <= 1.1.5.	6.5	More Details
CVE-2026-1307	The Ninja Forms - The Contact Form Builder That Grows With You plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.14.1 via a callback function for the admin_enqueue_scripts action handler in blocks/bootstrap.php. This makes it possible for authenticated attackers, with Contributor-level access and above, to gain access to an authorization token to view form submissions for arbitrary forms, which could potentially contain sensitive information.	6.5	More Details
CVE-2026-20110	A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incorrect privileges are associated with the start maintenance command. An attacker could exploit this vulnerability by accessing the management CLI of the affected device as a low-privileged user and using the start maintenance command. A successful exploit could allow the attacker to put the device in maintenance mode, which shuts down interfaces, resulting in a denial of service (DoS) condition. In case of exploitation, a device administrator can connect to the CLI and use the stop maintenance command to restore operations.	6.5	More Details
CVE-2026-3214	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal CAPTCHA allows Functionality Bypass.This issue affects CAPTCHA: from 0.0.0 before 1.17.0, from 2.0.0 before 2.0.10.	6.5	More Details
CVE-2026-33992	pyLoad is a free and open-source download manager written in Python. Prior to version 0.5.0b3.dev97, PyLoad's download engine accepts arbitrary URLs without validation, enabling Server-Side Request Forgery (SSRF) attacks. An authenticated attacker can exploit this to access internal network services and exfiltrate cloud provider metadata. On DigitalOcean droplets, this exposes sensitive infrastructure data including droplet ID, network configuration, region, authentication keys, and SSH keys configured in user-data/cloud-init. Version 0.5.0b3.dev97 contains a patch.	6.5	More Details
CVE-2026-20083	A vulnerability in the Secure Copy Protocol (SCP) server feature of Cisco IOS XE Software could allow an authenticated, local attacker with low privileges to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of a malformed SCP request. An attacker could exploit this vulnerability by issuing a crafted command through SSH. A successful exploit could allow the attacker to	6.5	More Details

	cause the device to reload unexpectedly, resulting in a DoS condition.		
CVE-2024-14028	Use after free vulnerability in Softing smartLink HW-DP or smartLink HW-PN webserver allows HTTP DoS. This issue affects: smartLink HW-DP: through 1.31 smartLink HW-PN: before 1.02.	6.5	More Details
CVE-2026-27046	Missing Authorization vulnerability in Kaira StoreCustomizer woocustomizer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects StoreCustomizer: from n/a through <= 2.6.3.	6.5	More Details
CVE-2026-3119	Under certain conditions, `named` may crash when processing a correctly signed query containing a TKEY record. The affected code can only be reached if an incoming request has a valid transaction signature (TSIG) from a key declared in the `named` configuration. This issue affects BIND 9 versions 9.20.0 through 9.20.20, 9.21.0 through 9.21.19, and 9.20.9-S1 through 9.20.20-S1. BIND 9 versions 9.18.0 through 9.18.46 and 9.18.11-S1 through 9.18.46-S1 are NOT affected.	6.5	More Details
CVE-2025-55265	HCL Aftermarket DPC is affected by File Discovery which allows attacker could exploit this issue to read sensitive files present in the system and may use it to craft further attacks.	6.5	More Details
CVE-2026-25365	Missing Authorization vulnerability in Özgür KARALAR Kargo Takip kargo-takip-turkiye allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Kargo Takip: from n/a through < 0.2.4.	6.5	More Details
CVE-2025-13078	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.10 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1 that could have allowed an authenticated user to cause a denial of service due to excessive resource consumption when processing certain webhook configuration inputs.	6.5	More Details
CVE-2026-3098	The Smart Slider 3 plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 3.5.1.33 via the 'actionExportAll' function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	6.5	More Details
CVE-2025-13436	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 13.7 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1 that could have allowed an authenticated user to cause a denial of service due to excessive resource consumption when handling certain CI-related inputs.	6.5	More Details
CVE-2026-25462	Missing Authorization vulnerability in avalex avalex avalex allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects avalex: from n/a through <= 3.1.3.	6.5	More Details
CVE-2026-32521	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Northern Beaches Websites WP Custom Admin Interface wp-custom-admin-interface allows DOM-Based XSS.This issue affects WP Custom Admin Interface: from n/a through <= 7.42.	6.5	More Details
CVE-2026-33246	NATS-Server is a High-Performance server for NATS.io, a cloud and edge native messaging system. The nats-server offers a `Nats-Request-Info:` message header, providing information about a request. This is supposed to provide enough information to allow for account/user identification, such that NATS clients could make their own decisions on how to trust a message, provided that they trust the nats-server as a broker. A leafnode connecting to a nats-server is not fully trusted unless the system account is bridged too. Thus identity claims should not have propagated unchecked. Prior to versions 2.11.15 and 2.12.6, NATS clients relying upon the Nats-Request-Info: header could be spoofed. This does not directly affect the nats-server itself, but the CVSS Confidentiality and Integrity scores are based upon what a hypothetical client might choose to do with this NATS header. Versions 2.11.15 and 2.12.6 contain a fix. No known workarounds are available.	6.4	More Details
CVE-2026-34716	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the AVideo YPTSocket plugin's caller feature renders incoming call notifications using the jQuery Toast Plugin, passing the caller's display name directly as the heading parameter. The toast plugin constructs the heading as raw HTML (' ' + heading + ' ') and inserts it into the DOM via jQuery's .html() method, which parses and executes any embedded HTML or script content. An attacker can set their display name to an XSS payload and trigger code execution on any online user's browser simply by initiating a call - no victim interaction is required beyond being connected to the WebSocket. At time of publication, there are no publicly available patches.	6.4	More Details
CVE-2026-4278	The Simple Download Counter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'sdc_menu' shortcode in all versions up to, and including, 2.3. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes, specifically the 'text' and 'cat' attributes. The 'text' attribute is output directly into HTML content on line 159 without any escaping (e.g., esc_html()). The 'cat' attribute is used unescaped in HTML class attributes on lines 135 and 157 without esc_attr(). This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4075	The BWL Advanced FAQ Manager Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'baf_sbox' shortcode in all versions up to and including 1.1.1. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes such as 'sbox_id', 'sbox_class', 'placeholder', 'highlight_color', 'highlight_bg', and 'cont_ext_class'. These attributes are directly interpolated into HTML element attributes without any esc_attr() escaping in the baf_sbox() function. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-2480	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'max_width' attribute of the `su_box` shortcode in all versions up to, and including, 7.4.10 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-2026-4389	The DSGVO snippet for Leaflet Map and its Extensions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `leafext-cookie-time` and `leafext-delete-cookie` shortcodes in all versions up to, and including, 3.1. This is due to insufficient input sanitization and output escaping on user supplied attributes (`unset`, `before`, `after`). 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-2026-2602	The Twentig plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'featuredImageSizeWidth' parameter in versions up to, and including, 1.9.7 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-2026-24964	Server-Side Request Forgery (SSRF) vulnerability in Wasiliy Strecker / ContestGallery developer Contest Gallery contest-gallery allows Server Side Request Forgery.This issue affects Contest Gallery: from n/a through <= 28.1.2.1.	6.4	More Details

CVE-2026-24362	Missing Authorization vulnerability in bdthemes Ultimate Post Kit ultimate-post-kit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ultimate Post Kit: from n/a through <= 4.0.21.	6.4	More Details
CVE-2026-33223	NATS-Server is a High-Performance server for NATS.io, a cloud and edge native messaging system. Prior to versions 2.11.15 and 2.12.6, the NATS message header `Nats-Request-Info:` is supposed to be a guarantee of identity by the NATS server, but the stripping of this header from inbound messages was not fully effective. An attacker with valid credentials for any regular client interface could thus spoof their identity to services which rely upon this header. Versions 2.11.15 and 2.12.6 contain a fix. No known workarounds are available.	6.4	More Details
CVE-2026-1834	The Ibtana – WordPress Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ive' shortcode in all versions up to, and including, 1.2.5.7 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-2026-4766	The Easy Image Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Gallery shortcode post meta field in all versions up to, and including, 1.5.3. This is due to insufficient input sanitization and output escaping on user-supplied gallery shortcode values. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5197	A vulnerability was found in code-projects Student Membership System 1.0. The affected element is an unknown function of the file /delete_user.php. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-5011	A vulnerability was detected in elecV2 elecV2P up to 3.8.3. This vulnerability affects the function runJSFile of the file /webhook of the component JSON Parser. Performing a manipulation of the argument rawcode results in code injection. Remote exploitation of the attack is possible. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-5101	A vulnerability was identified in Totolink A3300R 17.0.0cu.557_b20221024. This affects the function setLanCfg of the file /cgi-bin/cstecgi.cgi of the component Parameter Handler. The manipulation of the argument lanIp leads to command injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-4999	A security vulnerability has been detected in z-9527 admin up to 72aaf2dd05cf4ec2e98f390668b41e128eec5ad2. This issue affects the function uploadFile of the file /server/utils/upload.js of the component isImg Check. The manipulation of the argument fileType leads to path traversal. 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.	6.3	More Details
CVE-2026-4954	A security vulnerability has been detected in mingSoft MCMS up to 5.5.0. Impacted is the function list of the file net/mingsoft/cms/action/web/ContentAction.java of the component Web Content List Endpoint. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-33206	calibre is a cross-platform e-book manager for viewing, converting, editing, and cataloging e-books. Prior to version 9.6.0, a path traversal vulnerability exists in Calibre' handling of images in Markdown and other similar text-based files allowing an attacker to include arbitrary files from the file system into the converted book. Additionally, missing authentication and server-side request forgery in the background-image endpoint in the ebook reader web view allow the files to be exfiltrated without additional interaction. Version 9.6.0 contains a fix.	6.3	More Details
CVE-2026-4980	A local file disclosure vulnerability in the XInclude processing component of Inkscape 1.1 before 1.3 allows a remote attacker to read local files via a crafted SVG file containing malicious xi:include tags.	6.3	More Details
CVE-2026-5103	A weakness has been identified in Totolink A3300R 17.0.0cu.557_b20221024. This issue affects the function setUPnPCfg of the file /cgi-bin/cstecgi.cgi. This manipulation of the argument enable causes command injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-32977	OpenClaw before 2026.3.11 contains a sandbox boundary bypass vulnerability in the fs-bridge writeFile commit step that uses an unanchored container path during the final move operation. An attacker can exploit a time-of-check-time-of-use race condition by modifying parent paths inside the sandbox to redirect committed files outside the validated writable path within the container mount namespace.	6.3	More Details
CVE-2026-5020	A vulnerability was detected in Totolink A3600R 4.1.2cu.5182_B20201102. Affected by this issue is the function setNoticeCfg of the file /cgi-bin/cstecgi.cgi of the component Parameter Handler. The manipulation of the argument NoticeUrl results in command injection. The attack may be launched remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-5104	A security vulnerability has been detected in Totolink A3300R 17.0.0cu.557_b20221024. Impacted is the function setStaticRoute of the file /cgi-bin/cstecgi.cgi. Such manipulation of the argument ip leads to command injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-4970	A security flaw has been discovered in code-projects Social Networking Site 1.0. This affects an unknown function of the file delete_photos.php of the component Endpoint. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-5105	A vulnerability was detected in Totolink A3300R 17.0.0cu.557_b20221024. The affected element is the function setVpnPassCfg of the file /cgi-bin/cstecgi.cgi of the component Parameter Handler. Performing a manipulation of the argument pptpPassThru results in command injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-4907	A vulnerability was identified in Page-Replica Page Replica up to e4a7f52e75093ee318b4d5a9a9db6751050d2ad0. The impacted element is the function sitemap.fetch of the file /sitemap of the component Endpoint. The manipulation of the argument url leads to server-side request forgery. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-5102	A security flaw has been discovered in Totolink A3300R 17.0.0cu.557_b20221024. This vulnerability affects the function setSmartQosCfg of the file /cgi-bin/cstecgi.cgi of the component Parameter Handler. The manipulation of the argument qos_up_bw results in command injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-5184	A vulnerability was identified in TRENDnet TEW-713RE up to 1.02. The impacted element is an unknown function of the file /goform/setSysAdm. The manipulation of the argument admuser leads to command injection. The attack can 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-2026-5196	A vulnerability has been found in code-projects Student Membership System 1.0. Impacted is an unknown function of the file /delete_member.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-5177	A weakness has been identified in Totolink A3300R 17.0.0cu.557_b20221024. Affected by this vulnerability is the function setWiFiBasicCfg of the file /cgi-bin/cstecgi.cgi. Executing a manipulation of the argument rxRate can lead to command injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-5183	A vulnerability was determined in TRENDnet TEW-713RE up to 1.02. The affected element is the function sub_421494 of the file /goform/addRouting. Executing a manipulation of the argument dest can lead to command injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-5030	A vulnerability has been found in Totolink NR1800X 9.1.0u.6279_B20210910. This issue affects the function NTPSyncWithHost of the file /cgi-bin/cstecgi.cgi of the component Telnet Service. The manipulation of the argument host_time leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-34245	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `plugin/PlayLists/View/Playlists_schedules/add.json.php` endpoint allows any authenticated user with streaming permission to create or modify broadcast schedules targeting any playlist on the platform, regardless of ownership. When the schedule executes, the rebroadcast runs under the victim playlist owner's identity, allowing content hijacking and stream disruption. Commit 1e6dc20172de986f60641eb4fdb4090f079ffdce contains a patch.	6.3	More Details
CVE-2026-4966	A flaw has been found in itsourcecode Free Hotel Reservation System 1.0. Impacted is an unknown function of the file /admin/mod_room/index.php?view=edit. Executing a manipulation of the argument ID can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-5126	A flaw has been found in SourceCodester RSS Feed Parser 1.0. Affected by this issue is the function file_get_contents. This manipulation causes server-side request forgery. The attack is possible to be carried out remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-4963	A weakness has been identified in huggingface smolagents 1.25.0.dev0. This affects the function evaluate_augassign/evaluate_call/evaluate_with of the file src/smolagents/local_python_executor.py of the component Incomplete Fix CVE-2025-9959. This manipulation causes code 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 but did not respond in any way.	6.3	More Details
CVE-2026-4781	A flaw has been found in SourceCodester Sales and Inventory System 1.0. The affected element is an unknown function of the file update_purchase.php of the component HTTP GET Parameter Handler. Executing a manipulation of the argument sid can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.	6.3	More Details
CVE-2026-5206	A security vulnerability has been detected in code-projects Simple Gym Management System 1.0. This vulnerability affects unknown code of the component Payment Handler. The manipulation of the argument Payment_id/Amount/customer_id/payment_type/customer_name leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-5205	A vulnerability was identified in chatwoot up to 4.11.2. Affected by this vulnerability is the function Webhooks::Trigger in the library lib/webhooks/trigger.rb of the component Webhook API. Such manipulation of the argument url leads to server-side request forgery. 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.	6.3	More Details
CVE-2026-4964	A security vulnerability has been detected in letta-ai letta 0.16.4. This vulnerability affects the function _convert_message_create_to_message of the file letta/helpers/message_helper.py of the component File URL Handler. Such manipulation of the argument ImageContent leads to server-side request forgery. 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 but did not respond in any way.	6.3	More Details
CVE-2026-5181	A vulnerability has been found in SourceCodester Simple Doctors Appointment System up to 1.0. This issue affects some unknown processing of the file /doctors_appointment/admin/ajax.php?action=save_category. Such manipulation of the argument img leads to unrestricted upload. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-5153	A flaw has been found in Tenda CH22 1.0.0.1. The affected element is the function FormWriteFacMac of the file /goform/WriteFacMac. Executing a manipulation of the argument mac can lead to command injection. The attack may be launched remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-5178	A security vulnerability has been detected in Totolink A3300R 17.0.0cu.557_b20221024. Affected by this issue is the function setIptvCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument vlanPriLan3 leads to command injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-32921	OpenClaw before 2026.3.8 contains an approval bypass vulnerability in system.run where mutable script operands are not bound across approval and execution phases. Attackers can obtain approval for script execution, modify the approved script file before execution, and execute different content while maintaining the same approved command shape.	6.3	More Details
CVE-2026-4780	A vulnerability was detected in SourceCodester Sales and Inventory System 1.0. Impacted is an unknown function of the file update_out_standing.php of the component HTTP GET Parameter Handler. Performing a manipulation of the argument sid results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-4826	A vulnerability was determined in SourceCodester Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /update_stock.php of the component HTTP GET Parameter Handler. This manipulation of the argument sid causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-4876	A vulnerability was identified in itsourcecode Free Hotel Reservation System 1.0. The impacted element is an unknown function of the file /admin/mod_amenities/index.php?view=editpic. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-4836	A vulnerability was detected in code-projects Accounting System 1.0. The affected element is an unknown function of the file /my_account/delete.php. Performing a manipulation of the argument cos_id results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-	A vulnerability has been found in itsourcecode College Management System 1.0. The impacted element is an unknown function of the file		More

2026-4783	/admin/add-single-student-results.php of the component Parameter Handler. The manipulation of the argument course_code leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	Details
CVE-2026-4825	A vulnerability was found in SourceCodester Sales and Inventory System 1.0. This affects an unknown part of the file /update_sales.php of the component HTTP GET Parameter Handler. The manipulation of the argument sid results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-25460	Missing Authorization vulnerability in LiquidThemes Ave Core ave-core allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ave Core: from n/a through <= 2.9.1.	6.3	More Details
CVE-2025-14810	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 does not invalidate a session after privileges have been modified which could allow an authenticated user to retain access to sensitive information. CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L CWE: CWE-613: Insufficient Session Expiration CVSS Source: IBM CVSS Base score: 6.3 CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L)	6.3	More Details
CVE-2018-25214	MegaPing contains a local buffer overflow vulnerability that allows local attackers to crash the application by supplying an oversized payload to the Destination Address List field in the Finger function. Attackers can paste a crafted buffer exceeding expected input limits into the vulnerable field and trigger the Start button to cause a denial of service crash.	6.2	More Details
CVE-2018-25234	SmartFTP Client 9.0.2615.0 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Host field. Attackers can paste a buffer of 300 repeated characters into the Host connection parameter to trigger an application crash.	6.2	More Details
CVE-2026-20651	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.4, macOS Tahoe 26.3. An app may be able to access sensitive user data.	6.2	More Details
CVE-2026-33574	OpenClaw before 2026.3.8 contains a path traversal vulnerability in the skills download installer that validates the tools root lexically but reuses the mutable path during archive download and copy operations. A local attacker can rebind the tools-root path between validation and final write to redirect the installer outside the intended tools directory.	6.2	More Details
CVE-2019-25648	MyVideoConverter Pro 3.14 contains a local buffer overflow vulnerability that allows attackers to crash the application by supplying an excessively long string to the registration code input field. Attackers can paste a malicious payload containing 10000 bytes into the 'Copy and Paste Registration Code' field to trigger a denial of service condition.	6.2	More Details
CVE-2018-25226	FTPShell Server 6.83 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string in the account name field. Attackers can trigger a denial of service by pasting a 417-byte payload into the 'Account name to ban' parameter within the Manage FTP Accounts interface.	6.2	More Details
CVE-2018-25227	Valentina Studio 9.0.4 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Host field. Attackers can trigger the crash by pasting a 256-byte buffer of repeated characters into the Host parameter during server connection attempts.	6.2	More Details
CVE-2018-25228	NetSetMan 4.7.1 contains a buffer overflow vulnerability in the Workgroup feature that allows local attackers to crash the application by supplying oversized input. Attackers can create a malicious configuration file with excessive data and paste it into the Workgroup field to trigger a denial of service condition.	6.2	More Details
CVE-2018-25216	AnyBurn 4.3 contains a local buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string in the image file name field. Attackers can paste a 10000-byte payload into the 'Image file name' parameter during the 'Copy disk to Image' operation to trigger a denial of service condition.	6.2	More Details
CVE-2018-25231	HeidiSQL 9.5.0.5196 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long file path in the logging preferences. Attackers can input a buffer-overflow payload through the SQL log file path field in Preferences > Logging to trigger an application crash.	6.2	More Details
CVE-2018-25233	WebDrive 18.00.5057 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the username field during Secure WebDAV connection setup. Attackers can input a buffer-overflow payload of 5000 bytes in the username parameter and trigger a connection test to cause the application to crash.	6.2	More Details
CVE-2019-25653	Navicat for Oracle 12.1.15 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string in the password field. Attackers can paste a buffer of 550 repeated characters into the password parameter during Oracle connection configuration to trigger an application crash.	6.2	More Details
CVE-2018-25235	NetworkActiv Web Server 4.0 contains a buffer overflow vulnerability in the username field of the Security options that allows local attackers to crash the application by supplying an excessively long string. Attackers can trigger a denial of service by entering a crafted username value exceeding the expected buffer size through the Set username interface.	6.2	More Details
CVE-2019-25655	Device Monitoring Studio 8.10.00.8925 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string to the server connection dialog. Attackers can trigger the crash by entering a malformed server name or address containing repeated characters through the Tools menu Connect to New Server interface.	6.2	More Details
CVE-2026-20637	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.3 and iPadOS 26.3, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.3, tvOS 26.3, visionOS 26.3, watchOS 26.3. An app may be able to cause unexpected system termination.	6.2	More Details
CVE-2026-29976	Buffer Overflow vulnerability in ZerBea hcxpcapngtool v. 7.0.1-43-g2ee308e allows a local attacker to obtain sensitive information via the getradiotapfield() function	6.2	More Details
CVE-2026-20699	A downgrade issue affecting Intel-based Mac computers was addressed with additional code-signing restrictions. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.3, macOS Tahoe 26.4. An app may be able to access user-sensitive data.	6.2	More Details
CVE-2026-28889	A permissions issue was addressed with additional restrictions. This issue is fixed in Xcode 26.4. An app may be able to read arbitrary files as root.	6.2	More Details
CVE-2026-	This issue was addressed with improved authentication. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS	6.2	More

28867	Sequoia 15.7.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An app may be able to leak sensitive kernel state.		Details
CVE-2026-28822	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An attacker may be able to cause unexpected app termination.	6.2	More Details
CVE-2026-28866	This issue was addressed with improved validation of symlinks. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access sensitive user data.	6.2	More Details
CVE-2026-28841	A buffer overflow was addressed with improved size validation. This issue is fixed in macOS Tahoe 26.4. A buffer overflow may result in memory corruption and unexpected app termination.	6.2	More Details
CVE-2026-20695	An information disclosure issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to determine kernel memory layout.	6.2	More Details
CVE-2026-28833	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, visionOS 26.4. An app may be able to enumerate a user's installed apps.	6.2	More Details
CVE-2025-64646	IBM Concert 1.0.0 through 2.2.0 could allow an attacker to access sensitive information in memory due to the buffer not properly clearing resources.	6.2	More Details
CVE-2026-34540	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, a crafted ICC profile can trigger a heap-buffer-overflow (HBO) in icMemDump() when iccDumpProfile attempts to dump/describe malformed tag contents. The issue is observable under AddressSanitizer as an out-of-bounds heap read in icMemDump(...) at IccProfLib/IccUtil.cpp:1002, reachable via CIccTagUnknown::Describe(). This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34548	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, there is an Undefined Behavior (UB) condition in the XML conversion tooling path (iccToXml) caused by an implicit conversion from a negative signed integer to icUInt32Number (unsigned 32-bit), which changes the value. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34547	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, an Undefined Behavior (UB) condition in IccUtil.cpp can be triggered by a crafted ICC profile when running iccDumpProfile. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34550	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, there is an Undefined Behavior (UB) condition in IccProfLib/IccIO.cpp caused by an implicit conversion from a negative signed integer to size_t (unsigned), which changes the value. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34533	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, a crafted ICC profile can trigger Undefined Behavior (UB) in CIccCalculatorFunc::ApplySequence() due to invalid enum values being loaded for icChannelFuncSignature. The issue is observable under UBSan as a “load of value ... not a valid value for type icChannelFuncSignature”, indicating a type/enum value confusion scenario during ICC profile processing. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34546	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, a crafted TIFF input can trigger Undefined Behavior (UB) due to division by zero in the TIFF handling code paths used by iccTiffDump. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34551	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, a null-pointer dereference (NPD) in CIccTagLut16::Write() can be triggered when processing a crafted ICC profile (embedded in a TIFF and extracted during iccTiffDump). This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34552	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, there is an Undefined Behavior (UB) issue in IccTagLut.cpp where the code performs member access through a null pointer of type CIccApplyCLUT. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34554	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, a heap-buffer-overflow (HBO) in CIccApplyCmmSearch::costFunc() can be triggered via malformed JSON configuration input to the iccApplySearch tool. AddressSanitizer reports an out-of-bounds READ of size 8 originating from CIccApplyCmmSearch::costFunc(CIccSearchVec&) at IccProfLib/IccCmmSearch.cpp:112:5. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34542	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, a crafted ICC profile can trigger a stack-buffer-overflow (SBO) in CIccCalculatorFunc::Apply() when processed via iccApplyNamedCmm. Under AddressSanitizer, the failure is reported as a 4-byte write stack-buffer-overflow in IccProfLib/IccMpeCalc.cpp:3873, reachable through the MPE calculator / curve set initialization path. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34541	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, a crafted ICC profile can trigger Undefined Behavior (UB) via a null-pointer member call in CIccCombinedConnectionConditions::CIccCombinedConnectionConditions() (reported by UBSan as “member call on null pointer of type CIccTagSpectralViewingConditions”). The issue is reachable when running iccApplyNamedCmm with -PCC using a malformed .icc profile. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34549	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, there is an Undefined Behavior (UB) condition in IccUtil.cpp triggered by a crafted input profile. Under UndefinedBehaviorSanitizer, the issue is reported as invalid left shift operations on icUInt32Number (unsigned 32-bit) where the shifted value “cannot be represented” in that type. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34539	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, a crafted ICC profile and TIFF input can trigger a heap-buffer-overflow (HBO) in CTiffImg::WriteLine(). The issue is observable under AddressSanitizer as an out-of-bounds heap read when running iccSpecSepToTiff on a malicious .icc + .tif pair, leading to a crash during TIFF strip writing. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, there is a stack-buffer-overflow (SBO) in CIccTagFixedNum<>::GetValues() and a related bug chain. The primary crash is an AddressSanitizer-reported WRITE of size 4 that overflows a 4-byte stack variable (rv) via the call chain CIccTagFixedNum::GetValues() -> CIccTagStruct::GetElemNumberValue(). This	6.2	More Details

34555	issue has been patched in version 2.3.1.6.		
CVE-2025-12708	IBM Concert 1.0.0 through 2.2.0 contains hard-coded credentials that could be obtained by a local user.	6.2	More Details
CVE-2026-34534	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, a crafted ICC profile can trigger a heap-buffer-overflow (HBO) in CIccMpeSpectralMatrix::Describe(). The issue is observable under AddressSanitizer as an out-of-bounds heap read when running iccDumpProfile on a malicious profile. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34556	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, there is a heap-buffer-overflow (HBO) in icAnsiToUtf8() in the XML conversion path. The issue is triggered by a crafted ICC profile which causes icAnsiToUtf8(std::string&, char const*) to treat an input buffer as a C-string and call operations that rely on strlen()/null-termination. AddressSanitizer reports an out-of-bounds READ of size 115 past a 114-byte heap allocation, with the failure observed while running the iccToXml tool. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34535	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, a crafted ICC profile can trigger a segmentation fault (SEGV) in CIccTagArray::Cleanup(). The issue is observable under UBSan/ASan as misaligned member access / misaligned pointer loads followed by an invalid read leading to process crash when running iccRoundTrip on a malicious profile. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34536	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, a crafted ICC profile can trigger a stack overflow (SO) in SIccCalcOp::ArgsUsed(). The issue is observable under AddressSanitizer as a stack-overflow when iccApplyProfiles processes a malicious profile, with the crash occurring while computing argument usage during calculator underflow/overflow checks. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34537	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, a crafted ICC profile can trigger Undefined Behavior (UB) in CIccOpDefEnvVar::Exec() due to invalid enum values being loaded for icSigCmmEnvVar. The issue is observable under UBSan as a “load of value ... not a valid value for type icSigCmmEnvVar”, indicating an invalid enum/type value being consumed during ICC profile processing. This issue has been patched in version 2.3.1.6.	6.2	More Details
CVE-2026-34237	MCP Java SDK is the official Java SDK for Model Context Protocol servers and clients. Prior to versions 1.0.1 and 1.1.1, there is a hardcoded wildcard CORS vulnerability. This issue has been patched in versions 1.0.1 and 1.1.1.	6.1	More Details
CVE-2026-34231	Slippers is a UI component framework for Django. Prior to version 0.6.3, a Cross-Site Scripting (XSS) vulnerability exists in the {% attrs %} template tag of the slippers Django package. When a context variable containing untrusted data is passed to {% attrs %}, the value is interpolated into an HTML attribute string without escaping, allowing an attacker to break out of the attribute context and inject arbitrary HTML or JavaScript into the rendered page. This issue has been patched in version 0.6.3.	6.1	More Details
CVE-2025-41027	Reflected Cross Site Scripting (XSS) vulnerabilities in GDTaller. These vulnerabilities allows an attacker execute JavaScript code in the victim's browser by sending a malicious URL in 'site' parameter in 'app_recuperarclave.php'.	6.1	More Details
CVE-2025-41026	Reflected Cross Site Scripting (XSS) vulnerabilities in GDTaller. These vulnerabilities allows an attacker execute JavaScript code in the victim's browser by sending a malicious URL in 'site' parameter in 'app_login.php'.	6.1	More Details
CVE-2026-4887	A flaw was found in GIMP. This issue is a heap buffer over-read in GIMP PCX file loader due to an off-by-one error. A remote attacker could exploit this by convincing a user to open a specially crafted PCX image. Successful exploitation could lead to out-of-bounds memory disclosure and a possible application crash, resulting in a Denial of Service (DoS).	6.1	More Details
CVE-2026-3217	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal SAML SSO - Service Provider allows Cross-Site Scripting (XSS).This issue affects SAML SSO - Service Provider: from 0.0.0 before 3.1.3.	6.1	More Details
CVE-2026-1877	The Auto Post Scheduler plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.84. This is due to missing nonce validation on the 'aps_options_page' function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-33883	Statamic is a Laravel and Git powered content management system (CMS). Prior to versions 5.73.16 and 6.7.2, the `user:reset_password_form` tag could render user-input directly into HTML without escaping, allowing an attacker to craft a URL that executes arbitrary JavaScript in the victim's browser. This has been fixed in 5.73.16 and 6.7.2.	6.1	More Details
CVE-2026-30571	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0 in the view_category.php file via the "limit" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	6.1	More Details
CVE-2026-30564	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the view_payments.php file via the "limit" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	6.1	More Details
CVE-2025-61190	A Reflected Cross-Site Scripting (XSS) vulnerability has been identified in DSpace JSPUI 6.5 within the search/discover filtering functionality. The vulnerability exists due to improper sanitization of user-supplied input via the filter_type_1 parameter.	6.1	More Details
CVE-2026-30556	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the index.php file via the "msg" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	6.1	More Details
CVE-2026-30570	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0 in the view_sales.php file via the "limit" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL	6.1	More Details
CVE-2026-30569	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the view_stock_availability.php file via the "limit" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	6.1	More Details

CVE-2026-33933	OpenEMR is a free and open source electronic health records and medical practice management application. Starting in version 7.0.2.1 and prior to version 8.0.0.3, a reflected cross-site scripting (XSS) vulnerability in the custom template editor allows an attacker to execute arbitrary JavaScript in an authenticated staff member's browser session by sending them a crafted URL. The attacker does not need an OpenEMR account. Version 8.0.0.3 patches the issue.	6.1	More Details
CVE-2026-32919	OpenClaw before 2026.3.11 contains an authorization bypass vulnerability allowing write-scoped callers to reach admin-only session reset logic. Attackers with operator.write scope can issue agent requests containing /new or /reset slash commands to reset targeted conversation state without holding operator.admin privileges.	6.1	More Details
CVE-2025-40842	Ericsson Indoor Connect 8855 versions prior to 2025.Q3 contains a Cross-Site Scripting (XSS) vulnerability which, if exploited, can lead to unauthorized disclosure and modification of certain information.	6.1	More Details
CVE-2026-20104	A vulnerability in the bootloader of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches, Cisco Catalyst ESS9300 Embedded Series Switches, Cisco Catalyst IE9310 and IE9320 Rugged Series Switches, and Cisco IE3500 and IE3505 Rugged Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to an affected device to execute arbitrary code at boot time and break the chain of trust. This vulnerability is due to insufficient validation of software at boot time. An attacker could exploit this vulnerability by manipulating the loaded binaries on an affected device to bypass some of the integrity checks that are performed during the boot process. A successful exploit could allow the attacker to execute code that bypasses the requirement to run Cisco-signed images. Cisco has assigned this security advisory a Security Impact Rating (SIR) of High rather than Medium as the score indicates because this vulnerability allows an attacker to bypass a major security feature of a device.	6.1	More Details
CVE-2026-1986	The FloristPress for Woo – Customize your eCommerce store for your Florist plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'noresults' parameter in all versions up to, and including, 7.8.2 due to insufficient input sanitization and output escaping on the user supplied 'noresults' parameter. 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-2026-33758	OpenBao is an open source identity-based secrets management system. Prior to version 2.5.2, OpenBao installations that have an OIDC/JWT authentication method enabled and a role with `callback_mode=direct` configured are vulnerable to XSS via the `error_description` parameter on the page for a failed authentication. This allows an attacker access to the token used in the Web UI by a victim. The `error_description` parameter has been replaced with a static error message in v2.5.2. The vulnerability can be mitigated by removing any roles with `callback_mode` set to `direct`.	6.1	More Details
CVE-2026-20115	A vulnerability in Cisco IOS XE Software for Cisco Meraki could allow a remote, unauthenticated attacker to view confidential device information. This vulnerability is due to a device configuration upload being performed over an insecure tunnel. An attacker could exploit this vulnerability by conducting an on-path attack between the affected device and the Cisco Meraki Dashboard. A successful exploit could allow the attacker to view sensitive device configuration information.	6.1	More Details
CVE-2026-30567	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0 in the view_product.php file via the "limit" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	6.1	More Details
CVE-2026-2349	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal UI Icons allows Cross-Site Scripting (XSS).This issue affects UI Icons: from 0.0.0 before 1.0.1, from 1.1.0 before 1.1.1.	6.1	More Details
CVE-2026-30082	Multiple stored cross-site scripting (XSS) vulnerabilities in the Edit feature of the Software Package List page of IngEstate Server v11.14.0 allow attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the About application, What's news, or Release note parameters.	6.1	More Details
CVE-2026-30563	A Stored Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the update_details.php file. The application fails to sanitize the "website" parameter provided in a POST request. This allows authenticated attackers to inject arbitrary web script or HTML that is stored in the database and executed whenever the store details page is accessed.	6.1	More Details
CVE-2026-30565	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the view_supplier.php file via the "limit" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	6.1	More Details
CVE-2026-30566	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the view_customers.php file via the "limit" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	6.1	More Details
CVE-2026-29969	A cross-site scripting (XSS) vulnerability in the wff_cols_pref.css.aspx endpoint of staffwiki v7.0.1.19219 allows attackers to execute arbitrary Javascript in the context of the user's browser via a crafted HTTP request.	6.1	More Details
CVE-2026-4146	The Loco Translate plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘update_href’ parameter in all versions up to, and including, 2.8.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-33885	Statamic is a Laravel and Git powered content management system (CMS). Prior to versions 5.73.16 and 6.7.2, the external URL detection used for redirect validation on unauthenticated endpoints could be bypassed, allowing users to be redirected to external URLs after actions like form submissions and authentication flows. This has been fixed in 5.73.16 and 6.7.2.	6.1	More Details
CVE-2026-34739	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the User_Location plugin's testIP.php page reflects the ip request parameter directly into an HTML input element without applying htmlspecialchars() or any other output encoding. This allows an attacker to inject arbitrary HTML and JavaScript via a crafted URL. Although the page is restricted to admin users, AVideo's SameSite=None cookie configuration allows cross-origin exploitation, meaning an attacker can lure an admin to a malicious link that executes JavaScript in their authenticated session. At time of publication, there are no publicly available patches.	6.1	More Details
CVE-2026-3528	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Calculation Fields allows Cross-Site Scripting (XSS).This issue affects Calculation Fields: from 0.0.0 before 1.0.4.	6.1	More Details
CVE-2026-3529	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Google Analytics GA4 allows Cross-Site Scripting (XSS).This issue affects Google Analytics GA4: from 0.0.0 before 1.1.14.	6.1	More Details

CVE-2026-33402	Sakai is a Collaboration and Learning Environment (CLE). In versions 23.0 through 23.4 and 25.0 through 25.1, group titles and description can contain cross-site scripting scripts. The patch is included in releases 25.2 and 23.5. As a workaround, one can check the SAKAI_SITE_GROUP table for titles and descriptions that contain this info.	6.1	More Details
CVE-2026-29933	A reflected cross-site scripting (XSS) vulnerability in the /index/login.html component of YZMCMS v7.4 allows attackers to execute arbitrary Javascript in the context of the user's browser via modifying the referrer value in the request header.	6.1	More Details
CVE-2026-29934	A reflected cross-site scripting (XSS) vulnerability in the /admin/menus component of Lightcms v2.0 allows attackers to execute arbitrary Javascript in the context of the user's browser via modifying the referer value in the request header.	6.1	More Details
CVE-2026-34405	Nuxt OG Image generates OG Images with Vue templates in Nuxt. Prior to version 6.2.5, the image-generation component by the URI: /_og/d/ (and, in older versions, /og-image/) contains a vulnerability that allows injection of arbitrary attributes into the HTML page body. This issue has been patched in version 6.2.5.	6.1	More Details
CVE-2026-28297	SolarWinds Observability Self-Hosted was found to be affected by a stored cross-site scripting vulnerability, which when exploited, can lead to unintended script execution.	6.1	More Details
CVE-2026-34206	Captcha Protect is a Traefik middleware to add an anti-bot challenge to individual IPs in a subnet when traffic spikes are detected from that subnet. Prior to version 1.12.2, a reflected cross-site scripting (XSS) vulnerability exists in github.com/libops/captcha-protect. The challenge page accepted a client-supplied destination value and rendered it into HTML using Go's text/template. Because text/template does not perform contextual HTML escaping, an attacker could supply a crafted destination value that breaks out of the hidden input attribute and injects arbitrary script into the challenge page. This issue has been patched in version 1.12.2.	6.1	More Details
CVE-2026-30162	Cross Site Scripting (xss) vulnerability in Timo 2.0.3 via crafted links in the title field.	6.1	More Details
CVE-2026-34396	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the AVideo admin panel renders plugin configuration values in HTML forms without applying htmlspecialchars() or any other output encoding. The jsonToFormElements() function in admin/functions.php directly interpolates user-controlled values into textarea contents, option elements, and input attributes. An attacker who can set a plugin configuration value (either as a compromised admin or by chaining with CSRF on admin/save.json.php) can inject arbitrary JavaScript that executes whenever any administrator visits the plugin configuration page. At time of publication, there are no publicly available patches.	6.1	More Details
CVE-2026-33985	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.24.2, pixel data from adjacent heap memory is rendered to screen, potentially leaking sensitive data to the attacker. This issue has been patched in version 3.24.2.	5.9	More Details
CVE-2026-28886	A null pointer dereference was addressed with improved input validation. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. A user in a privileged network position may be able to cause a denial-of-service.	5.9	More Details
CVE-2026-33909	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, several variables in the MedEx recall/reminder processing code are concatenated directly into SQL queries without parameterization or type casting, enabling SQL injection. Version 8.0.0.3 contains a patch.	5.9	More Details
CVE-2025-55266	HCL Aftermarket DPC is affected by Session Fixation which allows attacker to takeover the user's session and use it carry out unauthorized transaction behalf of the user.	5.9	More Details
CVE-2025-64648	IBM Concert 1.0.0 through 2.2.0 transmits data in clear text that could allow an attacker to obtain sensitive information using man in the middle techniques.	5.9	More Details
CVE-2026-34043	Serialize JavaScript to a superset of JSON that includes regular expressions and functions. Prior to version 7.0.5, there is a Denial of Service (DoS) vulnerability caused by CPU exhaustion. When serializing a specially crafted "array-like" object (an object that inherits from Array.prototype but has a very large length property), the process enters an intensive loop that consumes 100% CPU and hangs indefinitely. This issue has been patched in version 7.0.5.	5.9	More Details
CVE-2026-32883	Botan is a C++ cryptography library. From version 3.0.0 to before version 3.11.0, during X509 path validation, OCSP responses were checked for an appropriate status code, but critically omitted verifying the signature of the OCSP response itself. This issue has been patched in version 3.11.0.	5.9	More Details
CVE-2026-28298	SolarWinds Observability Self-Hosted was found to be affected by a stored cross-site scripting vulnerability, which when exploited, can lead to unintended script execution.	5.9	More Details
CVE-2026-27853	An attacker might be able to trigger an out-of-bounds write by sending crafted DNS responses to a DNSdist using the DNSQuestion:changeName or DNSResponse:changeName methods in custom Lua code. In some cases the rewritten packet might become larger than the initial response and even exceed 65535 bytes, potentially leading to a crash resulting in denial of service.	5.9	More Details
CVE-2026-34353	In OCaml through 4.14.3, Bigarray.reshape allows an integer overflow, and resultant reading of arbitrary memory, when untrusted data is processed.	5.9	More Details
CVE-2026-32884	Botan is a C++ cryptography library. Prior to version 3.11.0, during processing of an X.509 certificate path using name constraints which restrict the set of allowable DNS names, if no subject alternative name is defined in the end-entity certificate Botan would check that the CN was allowed by the DNS name constraints, even though this check is technically not required by RFC 5280. However this check failed to account for the possibility of a mixed-case CN. Thus a certificate with CN=Sub.EVIL.COM and no subject alternative name would bypasses an excludedSubtrees constraint for evil.com because the comparison is case-sensitive. This issue has been patched in version 3.11.0.	5.9	More Details
CVE-2025-64647	IBM Concert 1.0.0 through 2.2.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information	5.9	More Details
	Impact: When using multiple wildcards, combined with at least one parameter, a regular expression can be generated that is vulnerable to		

CVE-2026-4923	ReDoS. This backtracking vulnerability requires the second wildcard to be somewhere other than the end of the path. Unsafe examples: /*foo-*bar-:baz /*a-:b-*c-:d /x/*a-:b/*c/y Safe examples: /*foo-:bar /*foo-:bar-*baz Patches: Upgrade to version 8.4.0. Workarounds: If you are using multiple wildcard parameters, you can check the regex output with a tool such as https://makenowjust-labs.github.io/recheck/playground/ to confirm whether a path is vulnerable.	5.9	More Details
CVE-2026-5119	A flaw was found in libsoup. When establishing HTTPS tunnels through a configured HTTP proxy, sensitive session cookies are transmitted in cleartext within the initial HTTP CONNECT request. A network-positioned attacker or a malicious HTTP proxy can intercept these cookies, leading to potential session hijacking or user impersonation.	5.9	More Details
CVE-2026-34085	fontconfig before 2.17.1 has an off-by-one error in allocation during sfnt capability handling, leading to a one-byte out-of-bounds write, and potentially a crash or code execution. This is in FcFontCapabilities in fcfreetype.c.	5.9	More Details
CVE-2026-26073	EVerest is an EV charging software stack. Versions prior to 2026.02.0 have a data race leading to possible `std::queue`/`std::deque` corruption. The trigger is powermeter public key update and EV session/error events (while OCPP not started). This results in a TSAN data race report and an ASAN/UBSAN misaligned address runtime error being observed. Version 2026.02.0 contains a patch.	5.9	More Details
CVE-2026-34360	HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. Prior to version 6.9.4, the /loadIG HTTP endpoint in the FHIR Validator HTTP service accepts a user-supplied URL via JSON body and makes server-side HTTP requests to it without any hostname, scheme, or domain validation. An unauthenticated attacker with network access to the validator can probe internal network services, cloud metadata endpoints, and map network topology through error-based information leakage. With explore=true (the default for this code path), each request triggers multiple outbound HTTP calls, amplifying reconnaissance capability. This issue has been patched in version 6.9.4.	5.8	More Details
CVE-2026-3881	The Performance Monitor WordPress plugin through 1.0.6 does not validate a parameter before making a request to it, which could allow unauthenticated users to perform SSRF attacks	5.8	More Details
CVE-2025-15615	Wazuh Manager authd service in wazuh-manager packages through version 4.7.3 contains an improper restriction of client-initiated SSL/TLS renegotiation vulnerability that allows remote attackers to cause a denial of service by sending excessive renegotiation requests. Attackers can exploit the lack of renegotiation limits to consume CPU resources and render the authd service unavailable.	5.8	More Details
CVE-2026-32983	Wazuh Manager authd service in wazuh-manager packages through version 4.7.3 contains an improper restriction of client-initiated SSL/TLS renegotiation vulnerability that allows remote attackers to cause a denial of service by sending excessive renegotiation requests. Attackers can exploit the lack of renegotiation limits to consume CPU resources and render the authd service unavailable.	5.8	More Details
CVE-2025-14974	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable due to Insecure Direct Object Reference (IDOR).	5.7	More Details
CVE-2025-55267	HCL Aftermarket DPC is affected by Unrestricted File Upload vulnerability, allows attacker to upload and execute malicious scripts, gaining full control over the server.	5.7	More Details
CVE-2026-33739	FOG is a free open-source cloning/imaging/rescue suite/inventory management system. Prior to 1.5.10.1812, the listing tables on multiple management pages (Host, Storage, Group, Image, Printer, Snapin) are vulnerable to Stored Cross-Site Scripting (XSS), due to insufficient server-side parameter sanitization in record creations/updates and a lack of HTML escaping in listing tables. Version 1.5.10.1812 patches the issue.	5.7	More Details
CVE-2026-27656	Mattermost versions 11.4.x <= 11.4.0, 11.3.x <= 11.3.1, 11.2.x <= 11.2.3, 10.11.x <= 10.11.11 fail to properly validate user identity in the OpenID {{IsSameUser()}} comparison logic, which allows an attacker to take over arbitrary user accounts via an overly permissive substring matching flaw in the user discovery flow.. Mattermost Advisory ID: MMSA-2026-00590	5.7	More Details
CVE-2026-4830	A vulnerability was identified in kalcaddle kodbox 1.64. This issue affects the function Add of the file app/controller/explorer/userShare.class.php of the component Public Share Handler. Such manipulation leads to unrestricted upload. The attack can be executed remotely. This attack is characterized by high complexity. The exploitability is assessed as difficult. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-2026-20694	This issue was addressed with improved handling of symlinks. This issue is fixed in iOS 26.3 and iPadOS 26.3, macOS Sequoia 15.7.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.4, macOS Sonoma 14.8.5, macOS Tahoe 26.3, macOS Tahoe 26.4. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2018-25230	Free IP Switcher 3.1 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Computer Name field. Attackers can paste a malicious payload into the Computer Name input field and click Activate to trigger a denial of service condition that crashes the application.	5.5	More Details
CVE-2026-20668	A logging issue was addressed with improved data redaction. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.3 and iPadOS 26.3, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.3, visionOS 26.3. An app may be able to access sensitive user data.	5.5	More Details
CVE-2018-25229	BulletProof FTP Server 2019.0.0.50 contains a denial of service vulnerability in the SMTP configuration interface that allows local attackers to crash the application by supplying an oversized string. Attackers can input a buffer of 257 'A' characters in the SMTP Server field and trigger a crash by clicking the Test button.	5.5	More Details
CVE-2026-20670	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.8.4, macOS Tahoe 26.3. An app may be able to access sensitive user data.	5.5	More Details
CVE-2026-33996	LibJWT is a C JSON Web Token Library. Starting in version 3.0.0 and prior to version 3.3.0, the JWK parsing for RSA-PSS did not protect against a NULL value when expecting to parse JSON string values. A specially crafted JWK file could exploit this behavior by using integers in places where the code expected a string. This was fixed in v3.3.0. A workaround is available. Users importing keys through a JWK file should not do so from untrusted sources. Use the `jwk2key` tool to check for validity of a JWK file. Likewise, if possible, do not use JWK files with RSA-PSS keys.	5.5	More Details
CVE-2026-23636	Kiteworks is a private data network (PDN). In Kiteworks Secure Data Forms prior to version 9.2.1, the manager of a form could potentially exploit an Unrestricted Upload of File with Dangerous Type due to a missing validation. Upgrade Kiteworks to version 9.2.1 or later to receive a patch.	5.5	More Details
CVE-	calibre is a cross-platform e-book manager for viewing, converting, editing, and cataloging e-books. Prior to version 9.6.0, a Server-Side		More

2026-33205	Request Forgery vulnerability in the background-image endpoint of calibre e-book reader's web view allows an attacker to perform blind GET requests to arbitrary URLs and exfiltrate information out from the ebook sandbox. Version 9.6.0 patches the issue.	5.5	Details
CVE-2026-4897	A flaw was found in polkit. A local user can exploit this by providing a specially crafted, excessively long input to the `polkit-agent-helper-1` setuid binary via standard input (stdin). This unbounded input can lead to an out-of-memory (OOM) condition, resulting in a Denial of Service (DoS) for the system.	5.5	More Details
CVE-2026-4948	A flaw was found in firewalld. A local unprivileged user can exploit this vulnerability by mis-authorizing two runtime D-Bus (Desktop Bus) setters, setZoneSettings2 and setPolicySettings. This mis-authorization allows the user to modify the runtime firewall state without proper authentication, leading to unauthorized changes in network security configurations.	5.5	More Details
CVE-2026-28870	An information leakage was addressed with additional validation. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An app may be able to access sensitive user data.	5.5	More Details
CVE-2026-28881	A privacy issue was addressed by moving sensitive data. This issue is fixed in macOS Tahoe 26.4. An app may be able to access sensitive user data.	5.5	More Details
CVE-2026-28852	A stack overflow was addressed with improved input validation. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An app may be able to cause a denial-of-service.	5.5	More Details
CVE-2026-28825	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2026-28829	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2026-28831	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access sensitive user data.	5.5	More Details
CVE-2018-25215	Excel Password Recovery Professional 8.2.0.0 contains a local buffer overflow vulnerability that allows attackers to cause a denial of service by supplying an excessively long string to the 'E-Mail and Registrations Code' field. Attackers can paste a crafted payload containing 5000 bytes of data into the registration field to trigger a crash when the Register button is clicked.	5.5	More Details
CVE-2026-28868	A logging issue was addressed with improved data redaction. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, visionOS 26.4, watchOS 26.4. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2026-28877	An authorization issue was addressed with improved state management. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Tahoe 26.4, visionOS 26.4, watchOS 26.4. An app may be able to access sensitive user data.	5.5	More Details
CVE-2026-28845	An authorization issue was addressed with improved state management. This issue is fixed in macOS Tahoe 26.4. An app may be able to access protected user data.	5.5	More Details
CVE-2019-25649	River Past Audio Converter 7.7.16 contains a local buffer overflow vulnerability in the activation code field that allows local attackers to crash the application by supplying an oversized input string. Attackers can paste a large payload of repeated characters into the 'E-Mail and Activation Code' field and click 'Activate' to trigger a denial of service condition.	5.5	More Details
CVE-2026-28890	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 26.4. An app may be able to cause unexpected system termination.	5.5	More Details
CVE-2025-55264	HCL Aftermarket DPC is affected by Failure to Invalidate Session on Password Change will allow attacker to access to a session, then they can maintain control over the account despite the password change leading to account takeover.	5.5	More Details
CVE-2026-28892	A permissions issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2026-20633	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2018-25232	Softros LAN Messenger 9.2 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string to the custom log files location field. Attackers can input a buffer of 2000 characters in the Log Files Location custom path parameter to trigger a crash when the OK button is clicked.	5.5	More Details
CVE-2026-33738	Lychee is a free, open-source photo-management tool. Prior to version 7.5.3, the photo `description` field is stored without HTML sanitization and rendered using `{!! $item->summary !!}` (Blade unescaped output) in the RSS, Atom, and JSON feed templates. The `/feed` endpoint is publicly accessible without authentication, allowing any RSS reader to execute attacker-controlled JavaScript. Version 7.5.3 fixes the issue.	5.4	More Details
CVE-2026-34362	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `verifyTokenSocket()` function in `plugin/YPTSocket/functions.php` has its token timeout validation commented out, causing WebSocket tokens to never expire despite being generated with a 12-hour timeout. This allows captured or legitimately obtained tokens to provide permanent WebSocket access, even after user accounts are deleted, banned, or demoted from admin. Admin tokens grant access to real-time connection data for all online users including IP addresses, browser info, and page locations. Commit 5d5237121bf82c24e9e0fdd5bc1699f1157783c5 fixes the issue.	5.4	More Details
CVE-2026-34247	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `plugin/Live/uploadPoster.php` endpoint allows any authenticated user to overwrite the poster image for any scheduled live stream by supplying an arbitrary `live_schedule_id`. The endpoint only checks `User::isLogged()` but never verifies that the authenticated user owns the targeted schedule. After overwriting the poster, the endpoint broadcasts a `socketLiveOFFCallback` notification containing the victim's broadcast key and user ID to all connected WebSocket clients.	5.4	More Details

	Commit 5fcb3bdf59f26d65e203cfbc8a685356ba300b60 fixes the issue.		
CVE-2026-20108	A vulnerability in the web-based management interface of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of the web-based management interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	5.4	More Details
CVE-2026-21724	A vulnerability has been discovered in Grafana OSS where an authorization bypass in the provisioning contact points API allows users with Editor role to modify protected webhook URLs without the required alert.notifications.receivers.protected:write permission.	5.4	More Details
CVE-2026-33742	Invoice Ninja is a source-available invoice, quote, project and time-tracking app built with Laravel. Product notes fields in Invoice Ninja v5.13.0 allow raw HTML via Markdown rendering, enabling stored XSS. The Markdown parser output was not sanitized with `purify::clean()` before being included in invoice templates. This is fixed in v5.13.4 by the vendor by adding `purify::clean()` to sanitize Markdown output.	5.4	More Details
CVE-2026-4335	The ShortPixel Image Optimizer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the attachment post_title in all versions up to, and including, 6.4.3. This is due to insufficient output escaping in the getEditorPopup() function and its corresponding media-popup.php template. Specifically, the attachment's post_title is retrieved from the database via get_post() in AjaxController.php (line 435) and passed directly to the view template (line 449), where it is rendered into an HTML input element's value attribute without esc_attr() escaping (media-popup.php line 139). Since WordPress allows Authors to set arbitrary attachment titles (including double-quote characters) via the REST API, a malicious author can craft an attachment title that breaks out of the HTML attribute and injects arbitrary JavaScript event handlers. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts that execute whenever a higher-privileged user (such as an administrator) opens the ShortPixel AI editor popup (Background Removal or Image Upscale) for the poisoned attachment.	5.4	More Details
CVE-2026-4816	A Reflected Cross Site Scripting (XSS) vulnerability has been found in Support Board v3.7.7. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by sending the victim a malicious URL using the 'search' parameter in '/supportboard/include/articles.php'. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user.	5.4	More Details
CVE-2026-2348	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Quick Edit allows Cross-Site Scripting (XSS).This issue affects Quick Edit: from 0.0.0 before 1.0.5, from 2.0.0 before 2.0.1.	5.4	More Details
CVE-2026-2595	The Quads Ads Manager for Google AdSense plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 2.0.98.1 due to insufficient input sanitization and output escaping of multiple ad metadata parameters. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2026-3591	A use-after-return vulnerability exists in the `named` server when handling DNS queries signed with SIG(0). Using a specially-crafted DNS request, an attacker may be able to cause an ACL to improperly (mis)match an IP address. In a default-allow ACL (denying only specific IP addresses), this may lead to unauthorized access. Default-deny ACLs should fail-secure. This issue affects BIND 9 versions 9.20.0 through 9.20.20, 9.21.0 through 9.21.19, and 9.20.9-S1 through 9.20.20-S1. BIND 9 versions 9.18.0 through 9.18.46 and 9.18.11-S1 through 9.18.46-S1 are NOT affected.	5.4	More Details
CVE-2026-2483	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable to cross-site scripting. This vulnerability allows users 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-2026-34442	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Prior to version 1.8.211, host header manipulation in FreeScout version (http://localhost:8080/system/status) allows an attacker to inject an arbitrary domain into generated absolute URLs. This leads to External Resource Loading and Open Redirect behavior. When the application constructs links and assets using the unvalidated Host header, user requests can be redirected to attacker-controlled domains and external resources may be loaded from malicious servers. This issue has been patched in version 1.8.211.	5.4	More Details
CVE-2026-33628	Invoice Ninja is a source-available invoice, quote, project and time-tracking app built with Laravel. Invoice line item descriptions in Invoice Ninja v5.13.0 bypass the XSS denylist filter, allowing stored XSS payloads to execute when invoices are rendered in the PDF preview or client portal. The line item description field was not passed through `purify::clean()` before rendering. This is fixed in v5.13.4 by the vendor by adding `purify::clean()` to sanitize line item descriptions.	5.4	More Details
CVE-2026-1561	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.3 IBM WebSphere Application Server Liberty is vulnerable to server-side request forgery (SSRF). This may allow remote attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	5.4	More Details
CVE-2026-34071	Stirling-PDF is a locally hosted web application that allows you to perform various operations on PDF files. In version 2.7.3, the /api/v1/convert/eml/pdf endpoint with parameter downloadHtml=true returns unsanitized HTML from the email body with Content-Type: text/html. An attacker who sends a malicious email to a Stirling-PDF user can achieve JavaScript execution when that user exports the email using the "Download HTML intermediate file" feature. Version 2.8.0 fixes the issue.	5.4	More Details
CVE-2026-34051	OpenEMR is a free and open source electronic health records and medical practice management application. Versions prior to 8.0.0.3 have an improper access control on the Import/Export functionality, allowing unauthorized users to perform import and export actions through direct request manipulation despite UI restrictions. This can lead to unauthorized data access, bulk data extraction, and manipulation of system data. Version 8.0.0.3 contains a fix.	5.4	More Details
CVE-2026-32923	OpenClaw before 2026.3.11 contains an authorization bypass vulnerability in Discord guild reaction ingestion that fails to enforce member users and roles allowlist checks. Non-allowlisted guild members can trigger reaction events accepted as trusted system events, injecting reaction text into downstream session context.	5.4	More Details
CVE-2026-1015	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	5.4	More Details
CVE-2026-33911	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, the POST parameter `title` is reflected back in a JSON response built with `json_encode()`. Because the response is served with a `text/html` Content-Type, the browser interprets injected HTML/script tags rather than treating the output as JSON. An authenticated attacker can craft a request that executes arbitrary JavaScript in a victim's session. Version 8.0.0.3 contains a fix.	5.4	More Details

CVE-2026-30527	A Stored Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Online Food Ordering System v1.0 in the Category management module within the admin panel. The application fails to properly sanitize user input supplied to the "Category Name" field when creating or updating a category. When an administrator or user visits the Category list page (or any page where this category is rendered), the injected JavaScript executes immediately in their browser.	5.4	More Details
CVE-2026-33912	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, an authenticated attacker could craft a malicious form that, when submitted by a victim, executes arbitrary JavaScript in the victim's browser session. Version 8.0.0.3 patches the issue.	5.4	More Details
CVE-2026-33915	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, five insurance company REST API routes are missing the `RestConfig::request_authorization_check()` call that every other data-modifying route in the standard API uses. This allows any authenticated API user to create and modify insurance company records even if their OpenEMR user account does not have administrative ACL permissions. Version 8.0.0.3 patches the issue.	5.4	More Details
CVE-2025-15445	The Restaurant Cafeteria WordPress theme through 0.4.6 exposes insecure admin-ajax actions without nonce or capability checks, allowing any logged-in user, like subscriber, to perform privileged operations. An attacker can install and activate a from a user-supplied URL, leading to arbitrary PHP code execution, and also import demo content that rewrites site configuration, including Restaurant Cafeteria WordPress theme through 0.4.6_mods, pages, menus, and front page settings.	5.4	More Details
CVE-2026-30560	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the add_supplier.php file via the "msg" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	5.4	More Details
CVE-2026-20114	A vulnerability in the Lobby Ambassador web-based management API of Cisco IOS XE Software could allow an authenticated, remote attacker to elevate their privileges and access management APIs that would not normally be available for Lobby Ambassador users. This vulnerability exists because parameters that are received by an API endpoint are not sufficiently validated. An attacker could exploit this vulnerability by authenticating as a Lobby Ambassador user and sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to create a new user with privilege level 1 access to the web-based management API. The attacker would then be able to access the device with these new credentials and privileges.	5.4	More Details
CVE-2026-3191	The Minify HTML plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1.12. This is due to missing or incorrect nonce validation on the 'minify_html_menu_options' function. This makes it possible for unauthenticated attackers to update plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details
CVE-2026-32506	Deserialization of Untrusted Data vulnerability in Edge-Themes Archicon archicon allows Object Injection.This issue affects Archicon: from n/a through < 1.7.	5.4	More Details
CVE-2026-32507	Deserialization of Untrusted Data vulnerability in Elated-Themes Leroux leroux allows Object Injection.This issue affects Leroux: from n/a through < 1.4.	5.4	More Details
CVE-2026-32508	Deserialization of Untrusted Data vulnerability in Mikado-Themes Halstein halstein allows Object Injection.This issue affects Halstein: from n/a through < 1.8.	5.4	More Details
CVE-2026-2973	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.7 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1 that could have allowed an authenticated user to execute arbitrary JavaScript in a user's browser due to improper sanitization of entity-encoded content in Mermaid diagrams.	5.4	More Details
CVE-2026-34475	Varnish Cache before 8.0.1 and Varnish Enterprise before 6.0.16r12, in certain unchecked req.url scenarios, mishandle URLs with a path of / for HTTP/1.1, potentially leading to cache poisoning or authentication bypass.	5.4	More Details
CVE-2026-3212	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Tagify allows Cross-Site Scripting (XSS).This issue affects Tagify: from 0.0.0 before 1.2.49.	5.4	More Details
CVE-2026-33045	Home Assistant is open source home automation software that puts local control and privacy first. Starting in version 2025.02 and prior to version 2026.01 the "remaining charge time"-sensor for mobile phones (imported/included from Android Auto it appears) is vulnerable cross-site scripting, similar to CVE-2025-62172. Version 2026.01 fixes the issue.	5.4	More Details
CVE-2026-33044	Home Assistant is open source home automation software that puts local control and privacy first. Starting in version 2020.02 and prior to version 2026.01, an authenticated party can add a malicious name to their device entity, allowing for Cross-Site Scripting attacks against anyone who can see a dashboard with a Map-card which includes that entity. It requires that the victim hovers over an information point. Version 2026.01 fixes the issue.	5.4	More Details
CVE-2026-32509	Deserialization of Untrusted Data vulnerability in Edge-Themes Gracey gracey allows Object Injection.This issue affects Gracey: from n/a through < 1.4.	5.4	More Details
CVE-2026-22569	An incorrect startup configuration of affected versions of Zscaler Client Connector on Windows may cause a limited amount of traffic from being inspected under rare circumstances.	5.4	More Details
CVE-2026-33726	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.17.14, 1.18.8, and 1.19.2, Ingress Network Policies are not enforced for traffic from pods to L7 Services (Envoy, GAMMA) with a local backend on the same node, when Per-Endpoint Routing is enabled and BPF Host Routing is disabled. Per-Endpoint Routing is disabled by default, but is automatically enabled in deployments using cloud IPAM, including Cilium ENI on EKS (`eni.enabled`), AlibabaCloud ENI (`alibabacloud.enabled`), Azure IPAM (`azure.enabled`, but not AKS BYOCNI), and some GKE deployments (`gke.enabled`; managed offerings such as GKE Dataplane V2 may use different defaults). It is typically not enabled in tunneled deployments, and chaining deployments are not affected. In practice, Amazon EKS with Cilium ENI mode is likely the most common affected environment. Versions 1.17.14, 1.18.8, and 1.19.2 contain a patch. There is currently no officially verified or comprehensive workaround for this issue. The only option would be to disable per-endpoint routes, but this will likely cause disruptions to ongoing connections, and potential conflicts if running in cloud providers.	5.4	More Details
CVE-2026-27508	Smoothwall Express versions prior to 3.1 Update 13 contain a reflected cross-site scripting vulnerability in the /redirect.cgi endpoint due to improper sanitation of the url parameter. Attackers can craft malicious URLs with javascript: schemes that execute arbitrary JavaScript in victims' browsers when clicked through the unsanitized link.	5.4	More Details

CVE-2026-26352	Smoothwall Express versions prior to 3.1 Update 13 contain a stored cross-site scripting vulnerability in the /cgi-bin/vpnmain.cgi script due to improper sanitation of the VPN_IP parameter. Authenticated attackers can inject arbitrary JavaScript through VPN configuration settings that executes when the affected page is viewed by other users.	5.4	More Details
CVE-2025-14912	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	5.4	More Details
CVE-2026-30561	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the add_purchase.php file via the "msg" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	5.4	More Details
CVE-2026-32510	Deserialization of Untrusted Data vulnerability in Edge-Themes Kamperen kamperen allows Object Injection.This issue affects Kamperen: from n/a through < 1.3.	5.4	More Details
CVE-2026-30559	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the add_sales.php file via the "msg" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	5.4	More Details
CVE-2026-32511	Deserialization of Untrusted Data vulnerability in Mikado-Themes Stål stal allows Object Injection.This issue affects Stål: from n/a through < 1.7.	5.4	More Details
CVE-2026-32859	ByteDance Deer-Flow versions prior to commit 5dbb362 contain a stored cross-site scripting vulnerability in the artifacts API that allows attackers to execute arbitrary scripts by uploading malicious HTML or script content as artifacts. Attackers can store malicious content that executes in the browser context when users view artifacts, leading to session compromise, credential theft, and arbitrary script execution.	5.4	More Details
CVE-2026-30558	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the add_customer.php file via the "msg" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	5.4	More Details
CVE-2026-32562	Missing Authorization vulnerability in WP Folio Team PPWP password-protect-page allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PPWP: from n/a through <= 1.9.15.	5.4	More Details
CVE-2026-30557	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the add_category.php file via the "msg" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	5.4	More Details
CVE-2026-29070	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to version 0.8.6, an access control check is missing when deleting a file from a knowledge base. The only check being done is that the user has write access to the knowledge base (or is admin), but NOT that the file actually belongs to this knowledge base. It is thus possible to delete arbitrary files from arbitrary knowledge bases (as long as one knows the file id). Version 0.8.6 patches the issue.	5.4	More Details
CVE-2026-33887	Statamic is a Laravel and Git powered content management system (CMS). Prior to versions 5.73.16 and 6.7.2, authenticated Control Panel users could view entry revisions for any collection with revisions enabled, regardless of whether they had the required collection permissions. This bypasses the authorization checks that the main entry controllers enforce, exposing entry field values and blueprint data. Users could also create entry revisions without edit permission, though this only snapshots the existing content state and does not affect published content. This has been fixed in 5.73.16 and 6.7.2.	5.4	More Details
CVE-2026-32273	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, updating a category description via API is not sanitizing the description string, which can lead to XSS attacks. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.	5.4	More Details
CVE-2026-3215	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Islandora allows Cross-Site Scripting (XSS).This issue affects Islandora: from 0.0.0 before 2.17.5.	5.4	More Details
CVE-2026-4274	Mattermost versions 11.2.x <= 11.2.2, 10.11.x <= 10.11.10, 11.4.x <= 11.4.0, 11.3.x <= 11.3.1 fail to restrict team-level access when processing membership sync from a remote cluster, which allows a malicious remote cluster to grant a user access to an entire private team instead of only the shared channel via sending crafted membership sync messages that trigger team membership assignment. Mattermost Advisory ID: MMSA-2026-00574	5.4	More Details
CVE-2026-33722	n8n is an open source workflow automation platform. Prior to versions 2.6.4 and 1.123.23, an authenticated user without permission to list external secrets could reference a secret by the external name in a credential and retrieve its plaintext value when saving the credential. This bypassed the `externalSecret:list` permission check and allowed access to secrets stored in connected vaults without admin or owner privileges. This issue requires the instance to have an external secrets vault configured. The attacker must know or be able to guess the name of a target secret. The issue has been fixed in n8n versions 1.123.23 and 2.6.4. Users should upgrade to one of these versions or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations: Restrict n8n access to fully trusted users only, and/or disable external secrets integration until the patch can be applied. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	5.3	More Details
CVE-2026-34369	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `get_api_video_file` and `get_api_video` API endpoints in AVideo return full video playback sources (direct MP4 URLs, HLS manifests) for password-protected videos without verifying the video password. While the normal web playback flow enforces password checks via the `CustomizeUser::getModeYouTube()` hook, this enforcement is completely absent from the API code path. An unauthenticated attacker can retrieve direct playback URLs for any password-protected video by calling the API directly. Commit be344206f2f461c034ad2f1c5d8212dd8a52b8c7 fixes the issue.	5.3	More Details
CVE-2026-32497	Weak Authentication vulnerability in PickPlugins User Verification user-verification allows Authentication Abuse.This issue affects User Verification: from n/a through <= 2.0.45.	5.3	More Details
CVE-2026-33809	A maliciously crafted TIFF file can cause image decoding to attempt to allocate up 4GiB of memory, causing either excessive resource consumption or an out-of-memory error.	5.3	More Details
CVE-			

2026-32492	Authentication Bypass by Spoofing vulnerability in Joe Dolson My Tickets my-tickets allows Identity Spoofing.This issue affects My Tickets: from n/a through <= 2.1.1.	5.3	More Details
CVE-2026-34364	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `categories.json.php` endpoint, which serves the category listing API, fails to enforce user group-based access controls on categories. In the default request path (no `?user=` parameter), user group filtering is entirely skipped, exposing all non-private categories including those restricted to specific user groups. When the `?user=` parameter is supplied, a type confusion bug causes the filter to use the admin user's (user_id=1) group memberships instead of the current user's, rendering the filter ineffective. Commit 6e8a673eed07be5628d0b60fbfabd171f3ce74c9 contains a fix.	5.3	More Details
CVE-2026-34368	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `transferBalance()` method in `plugin/YPTWallet/YPTWallet.php` contains a Time-of-Check-Time-of-Use (TOCTOU) race condition. The method reads the sender's wallet balance, checks sufficiency in PHP, then writes the new balance — all without database transactions or row-level locking. An attacker with multiple authenticated sessions can send concurrent transfer requests that all read the same stale balance, each passing the balance check independently, resulting in only one deduction being applied while the recipient is credited multiple times. Commit 34132ad5159784bfc7ba0d7634bb5c79b769202d contains a fix.	5.3	More Details
CVE-2026-33219	NATS-Server is a High-Performance server for NATS.io, a cloud and edge native messaging system. Prior to versions 2.11.15 and 2.12.6, a malicious client which can connect to the WebSockets port can cause unbounded memory use in the nats-server before authentication; this requires sending a corresponding amount of data. This is a milder variant of CVE-2026-27571. That earlier issue was a compression bomb, this vulnerability is not. Attacks against this new issue thus require significant client bandwidth. Versions 2.11.15 and 2.12.6 contain a fix. As a workaround, disable websockets if not required for project deployment.	5.3	More Details
CVE-2026-31950	LibreChat is a ChatGPT clone with additional features. In versions 0.8.2-rc2 through 0.8.2-rc3, the SSE streaming endpoint `/api/agents/chat/stream/:streamId` does not verify that the requesting user owns the stream. Any authenticated user who obtains or guesses a valid stream ID can subscribe and read another user's real-time chat content, including messages, AI responses, and tool invocations. Version 0.8.2 patches the issue.	5.3	More Details
CVE-2026-5236	A vulnerability was identified in Axiomatic Bento4 up to 1.6.0-641. Affected is the function AP4_BitReader::SkipBits of the file Ap4Dac4Atom.cpp of the component DSI v1 Parser. Such manipulation of the argument n_presentations leads to heap-based buffer overflow. The attack needs to be performed locally. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-20113	A vulnerability in the web-based Cisco IOx application hosting environment management interface of Cisco IOS XE Software could allow an unauthenticated, remote attacker to perform a carriage return line feed (CRLF) injection attack against a user. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending crafted packets to an affected device. A successful exploit could allow the attacker to arbitrarily inject log entries, manipulate the structure of log files, or obscure legitimate log events.	5.3	More Details
CVE-2026-20632	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Tahoe 26.4. An app may be able to access sensitive user data.	5.3	More Details
CVE-2026-3210	Incorrect Authorization vulnerability in Drupal Material Icons allows Forceful Browsing.This issue affects Material Icons: from 0.0.0 before 2.0.4.	5.3	More Details
CVE-2026-33936	The `ecdsa` PyPI package is a pure Python implementation of ECC (Elliptic Curve Cryptography) with support for ECDSA (Elliptic Curve Digital Signature Algorithm), EdDSA (Edwards-curve Digital Signature Algorithm) and ECDH (Elliptic Curve Diffie-Hellman). Prior to version 0.19.2, an issue in the low-level DER parsing functions can cause unexpected exceptions to be raised from the public API functions. `ecdsa.der.remove_octet_string()` accepts truncated DER where the encoded length exceeds the available buffer. For example, an OCTET STRING that declares a length of 4096 bytes but provides only 3 bytes is parsed successfully instead of being rejected. Because of that, a crafted DER input can cause `SigningKey.from_der()` to raise an internal exception (`IndexError: index out of bounds on dimension 1`) rather than cleanly rejecting malformed DER (e.g., raising `UnexpectedDER` or `ValueError`). Applications that parse untrusted DER private keys may crash if they do not handle unexpected exceptions, resulting in a denial of service. Version 0.19.2 patches the issue.	5.3	More Details
CVE-2026-5235	A vulnerability was determined in Axiomatic Bento4 up to 1.6.0-641. This impacts the function AP4_BitReader::ReadCache of the file Ap4Dac4Atom.cpp of the component MP4 File Parser. This manipulation causes heap-based buffer overflow. The attack needs to be launched locally. 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.	5.3	More Details
CVE-2026-33481	Syft is a a CLI tool and Go library for generating a Software Bill of Materials (SBOM) from container images and filesystems. Syft versions before v1.42.3 would not properly cleanup temporary storage if the temporary storage was exhausted during a scan. When scanning archives Syft will unpack those archives into temporary storage then inspect the unpacked contents. Under normal operation Syft will remove the temporary data it writes after completing a scan. This vulnerability would affect users of Syft that were scanning content that could cause Syft to fill the temporary storage that would then cause Syft to raise an error and exit. When the error is triggered Syft would exit without properly removing the temporary files in use. In our testing this was most easily reproduced by scanning very large artifacts or highly compressed artifacts such as a zipbomb. Because Syft would not clean up its temporary files, the result would be filling temporary file storage preventing future runs of Syft or other system utilities that rely on temporary storage being available. The patch has been released in v1.42.3. Syft now cleans up temporary files when an error condition is encountered. There are no workarounds for this vulnerability in Syft. Users that find their temporary storage depleted can manually remove the temporary files.	5.3	More Details
CVE-2026-2442	The Page Builder: Pagelayer – Drag and Drop website builder plugin for WordPress is vulnerable to Improper Neutralization of CRLF Sequences ('CRLF Injection') in all versions up to, and including, 2.0.7. This is due to the contact form handler performing placeholder substitution on attacker-controlled form fields and then passing the resulting values into email headers without removing CR/LF characters. This makes it possible for unauthenticated attackers to inject arbitrary email headers (for example Bcc / Cc) and abuse form email delivery via the 'email' parameter granted they can target a contact form configured to use placeholders in mail template headers.	5.3	More Details
CVE-2026-29055	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. In versions prior to 2.6.0, the image processing pipeline in Tandoor Recipes explicitly skips EXIF metadata stripping, image rescaling, and size validation for WebP and GIF image formats. A developer TODO comment in the source code acknowledges this as a known issue. As a result, when users upload recipe photos in WebP format (the default format for modern smartphone cameras), their sensitive EXIF data — including GPS coordinates, camera model, timestamps, and software information — is stored and served to all users who can view the recipe. Version 2.6.0 fixes the issue.	5.3	More Details
CVE-2026-33763	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `get_api_video_password_is_correct` API endpoint allows any unauthenticated user to verify whether a given password is correct for any password-protected video. The endpoint returns a boolean `passwordIsCorrect` field with no rate limiting, CAPTCHA, or authentication requirement, enabling efficient offline-speed brute-force attacks against video passwords. Commit 01a0614fedcdaee47832c0d913a0fb86d8c28135 contains a patch.	5.3	More Details

CVE-2026-34411	Appsmith versions prior to 1.98 expose sensitive instance management API endpoints without authentication. Unauthenticated attackers can query endpoints like /api/v1/consolidated-api/view and /api/v1/tenants/current to retrieve configuration metadata, license information, and unsalted SHA-256 hashes of admin email domains for reconnaissance and targeted attack planning.	5.3	More Details
CVE-2026-29909	MRCMS V3.1.2 contains an unauthenticated directory enumeration vulnerability in the file management module. The /admin/file/list.do endpoint lacks authentication controls and proper input validation, allowing remote attackers to enumerate directory contents on the server without any credentials.	5.3	More Details
CVE-2026-33995	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.24.2, a double-free vulnerability in kerberos_AcceptSecurityContext() and kerberos_InitializeSecurityContextA() (WinPR, winpr/libwinpr/sspi/Kerberos/kerberos.c) can cause a crash in any FreeRDP clients on systems where Kerberos and/or Kerberos U2U is configured (Samba AD member, or krb5 for NFS). The crash is triggered during NLA connection teardown and requires a failed authentication attempt. This issue has been patched in version 3.24.2.	5.3	More Details
CVE-2026-30878	baserCMS is a website development framework. Prior to version 5.2.3, a public mail submission API allows unauthenticated users to submit mail form entries even when the corresponding form is not accepting submissions. This bypasses administrative controls intended to stop form intake and enables spam or abuse via the API. This issue has been patched in version 5.2.3.	5.3	More Details
CVE-2026-1797	The Appointment Booking and Scheduler Plugin – Truebooker plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.1.4 through views php files. This makes it possible for unauthenticated attackers to view potentially sensitive information contained in the exposed views php files via direct access.	5.3	More Details
CVE-2026-27859	A mail message containing excessive amount of RFC 2231 MIME parameters causes LMTP to use too much CPU. A suitably formatted mail message causes mail delivery process to consume large amounts of CPU time. Use MTA capabilities to limit RFC 2231 MIME parameters in mail messages, or upgrade to fixed version where the processing is limited. No publicly available exploits are known.	5.3	More Details
CVE-2026-28818	A logging issue was addressed with improved data redaction. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access sensitive user data.	5.3	More Details
CVE-2026-5185	A security flaw has been discovered in Nothings stb_image up to 2.30. This affects the function stbi__gif_load_next of the file stb_image.h of the component Multi-frame GIF File Handler. The manipulation results in heap-based buffer overflow. The attack requires a local approach. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-5186	A weakness has been identified in Nothings stb up to 2.30. This impacts the function stbi__load_gif_main of the file stb_image.h of the component Multi-frame GIF File Handler. This manipulation causes double free. 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 but did not respond in any way.	5.3	More Details
CVE-2026-0394	When dovecot has been configured to use per-domain passwd files, and they are placed one path component above /etc, or slash has been added to allowed characters, path traversal can happen if the domain component is directory partial. This allows inadvertently reading /etc/passwd (or some other path which ends with passwd). If this file contains passwords, it can be used to authenticate wrongly, or if this is userdb, it can unexpectly make system users appear valid users. Upgrade to fixed version, or use different authentication scheme that does not rely on paths. Alternatively you can also ensure that the per-domain passwd files are in some other location, such as /etc/dovecot/auth/%d. No publicly available exploits are known.	5.3	More Details
CVE-2026-24028	An attacker might be able to trigger an out-of-bounds read by sending a crafted DNS response packet, when custom Lua code uses newDNSPacketOverlay to parse DNS packets. The out-of-bounds read might trigger a crash, leading to a denial of service, or access unrelated memory, leading to potential information disclosure.	5.3	More Details
CVE-2026-24030	An attacker might be able to trick DNSdist into allocating too much memory while processing DNS over QUIC or DNS over HTTP/3 payloads, resulting in a denial of service. In setups with a large quantity of memory available this usually results in an exception and the QUIC connection is properly closed, but in some cases the system might enter an out-of-memory state instead and terminate the process.	5.3	More Details
CVE-2025-59028	When sending invalid base64 SASL data, login process is disconnected from the auth server, causing all active authentication sessions to fail. Invalid BASE64 data can be used to DoS a vulnerable server to break concurrent logins. Install fixed version or disable concurrency in login processes (heavy perfomance penalty on large deployments). No publicly available exploits are known.	5.3	More Details
CVE-2026-2343	The PeproDev Ultimate Invoice WordPress plugin through 2.2.5 has a bulk download invoices action that generates ZIP archives containing exported invoice PDFs. The ZIP files are named predictably making it possible to brute force and retreive PII.	5.3	More Details
CVE-2026-33672	Picomatch is a glob matcher written JavaScript. Versions prior to 4.0.4, 3.0.2, and 2.3.2 are vulnerable to a method injection vulnerability affecting the `POSIX_REGEX_SOURCE` object. Because the object inherits from `Object.prototype`, specially crafted POSIX bracket expressions (e.g., `[[:constructor:]]`) can reference inherited method names. These methods are implicitly converted to strings and injected into the generated regular expression. This leads to incorrect glob matching behavior (integrity impact), where patterns may match unintended filenames. The issue does not enable remote code execution, but it can cause security-relevant logic errors in applications that rely on glob matching for filtering, validation, or access control. All users of affected `picomatch` versions that process untrusted or user-controlled glob patterns are potentially impacted. This issue is fixed in picomatch 4.0.4, 3.0.2 and 2.3.2. Users should upgrade to one of these versions or later, depending on their supported release line. If upgrading is not immediately possible, avoid passing untrusted glob patterns to picomatch. Possible mitigations include sanitizing or rejecting untrusted glob patterns, especially those containing POSIX character classes like `[[:...:]]`; avoiding the use of POSIX bracket expressions if user input is involved; and manually patching the library by modifying `POSIX_REGEX_SOURCE` to use a null prototype.	5.3	More Details
CVE-2026-28820	This issue was addressed with improved checks. This issue is fixed in macOS Tahoe 26.4. An app may be able to access sensitive user data.	5.3	More Details
CVE-2026-28824	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access sensitive user data.	5.3	More Details
CVE-2026-28862	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access user-sensitive data.	5.3	More Details
CVE-2026-	MapServer is a system for developing web-based GIS applications. Starting in version 4.2 and prior to version 8.6.1, a heap-buffer-overflow write in MapServer's SLD (Styled Layer Descriptor) parser lets a remote, unauthenticated attacker crash the MapServer process by sending a crafted SLD with more than 100 Threshold elements inside a ColorMap/Categorize structure (commonly reachable via WMS GetMap with	5.3	More Details

33721	SLD_BODY). Version 8.6.1 patches the issue.		
CVE-2026-28828	A permissions issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access sensitive user data.	5.3	More Details
CVE-2026-28839	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access sensitive user data.	5.3	More Details
CVE-2026-4900	A weakness has been identified in code-projects Online Food Ordering System 1.0. This affects an unknown part of the file /dbfood/localhost.sql. This manipulation causes files or directories accessible. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. It is advisable to modify the configuration settings.	5.3	More Details
CVE-2026-28838	A permissions issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to break out of its sandbox.	5.3	More Details
CVE-2026-2100	A flaw was found in p11-kit. A remote attacker could exploit this vulnerability by calling the C_DeriveKey function on a remote token with specific IBM kyber or IBM btc derive mechanism parameters set to NULL. This could lead to the RPC-client attempting to return an uninitialized value, potentially resulting in a NULL dereference or undefined behavior. This issue may cause an application level denial of service or other unpredictable system states.	5.3	More Details
CVE-2026-5125	A vulnerability was detected in raine consult-llm-mcp up to 2.5.3. Affected by this vulnerability is the function child_process.execSync of the file src/server.ts. The manipulation of the argument git_diff.base_ref/git_diff.files results in os command injection. The attack is only possible with local access. The exploit is now public and may be used. Upgrading to version 2.5.4 addresses this issue. The patch is identified as 4abf297b34e5e8a9cb364b35f52c5f0ca1d599d3. Upgrading the affected component is recommended.	5.3	More Details
CVE-2026-5170	A user with access to the cluster with a limited set of privilege actions can trigger a crash of a mongod process during the limited and unpredictable window when the cluster is being promoted from a replica set to a sharded cluster. This may cause a denial of service by taking down the primary of the replica set. This issue affects MongoDB Server v8.2 versions prior to 8.2.2, MongoDB Server v8.0 versions between 8.0.18, MongoDB Server v7.0 versions between 7.0.31.	5.3	More Details
CVE-2026-20686	This issue was addressed with improved input validation. This issue is fixed in iOS 26.3 and iPadOS 26.3. An app may be able to access sensitive user data.	5.3	More Details
CVE-2026-33545	MobSF is a mobile application security testing tool used. Prior to version 4.4.6, MobSF's `read_sqlite()` function in `mobsf/MobSF/utils.py` (lines 542-566) uses Python string formatting (`%`) to construct SQL queries with table names read from a SQLite database's `sqlite_master` table. When a security analyst uses MobSF to analyze a malicious mobile application containing a crafted SQLite database, attacker-controlled table names are interpolated directly into SQL queries without parameterization or escaping. This allows an attacker to cause denial of service and achieve SQL injection. Version 4.4.6 patches the issue.	5.3	More Details
CVE-2026-4997	A security flaw has been discovered in Sinaptik AI PandasAI up to 3.0.0. This affects the function is_sql_query_safe of the file pandasai/helpers/sql_sanitizer.py. Performing a manipulation 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.	5.3	More Details
CVE-2026-5003	A vulnerability was found in PromtEngineer localGPT up to 4d41c7d1713b16b216d8e062e51a5dd88b20b054. This affects the function handle_index of the file rag_system/api_server.py of the component Web Interface. Performing a manipulation results in information disclosure. It is possible to initiate the attack remotely. The exploit has been made public and could be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-5007	A vulnerability was identified in kazuph mcp-docs-rag up to 0.5.0. Affected is the function cloneRepository of the file src/index.ts of the component add_git_repository/add_text_file. The manipulation leads to os command injection. The attack needs to be performed locally. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-5013	A vulnerability has been found in elecV2 elecV2P up to 3.8.3. Impacted is the function path.join of the file /store/:key. The manipulation of the argument URL leads to path traversal. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-5014	A vulnerability was found in elecV2 elecV2P up to 3.8.3. The affected element is the function path.join of the file /log/ of the component Wildcard Handler. The manipulation results in path traversal. The attack may be performed from remote. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-5023	A vulnerability has been found in DeDeveloper23 codebase-mcp up to 3ec749d237dd8eabbeef48657cf917275792fde6. This vulnerability affects the function getCodebase/getRemoteCodebase/saveCodebase of the file src/tools/codebase.ts of the component RepoMix Command Handler. Such manipulation leads to os command injection. The attack needs to be performed locally. The exploit has been disclosed to the public and may be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-20697	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access sensitive user data.	5.3	More Details
CVE-2026-33638	Ech0 is an open-source, self-hosted publishing platform for personal idea sharing. Prior to version 4.2.0, `GET /api/allusers` is mounted as a public endpoint and returns user records without authentication. This allows remote unauthenticated user enumeration and exposure of user profile metadata. A fix is available in v4.2.0.	5.3	More Details
CVE-2026-33761	WWBN AVideo is an open source video platform. In versions up to and including 26.0, three `list.json.php` endpoints in the Scheduler plugin lack any authentication check, while every other endpoint in the same plugin directories (`add.json.php`, `delete.json.php`, `index.php`) requires `User::isAdmin()`. An unauthenticated attacker can retrieve all scheduled tasks (including internal callback URLs and parameters), admin-composed email messages, and user-to-email targeting mappings by sending simple GET requests. Commit 83390ab1fa8dca2de3f8fa76116a126428405431 contains a patch.	5.3	More Details
	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the `objects/playlistsVideos.json.php` endpoint returns		

CVE-2026-33759	the full video contents of any playlist by ID without any authentication or authorization check. Private playlists (including `watch_later` and `favorite` types) are correctly hidden from listing endpoints via `playlistsFromUser.json.php`, but their contents are directly accessible through this endpoint by providing the sequential integer `playlists_id` parameter. Commit bb716fbece656c9fe39784f11e4e822b5867f1ca has a patch for the issue.	5.3	More Details
CVE-2026-3525	Incorrect Authorization vulnerability in Drupal File Access Fix (deprecated) allows Forceful Browsing.This issue affects File Access Fix (deprecated): from 0.0.0 before 1.2.0.	5.3	More Details
CVE-2026-3526	Incorrect Authorization vulnerability in Drupal File Access Fix (deprecated) allows Forceful Browsing.This issue affects File Access Fix (deprecated): from 0.0.0 before 1.2.0.	5.3	More Details
CVE-2026-27813	EVerest is an EV charging software stack. Versions prior to 2026.02.0 have a data race leading to use-after-free. This is triggered by EV plug-in/unplug and RFID/RemoteStart/OCPP authorization events (or delayed authorization response). Version 2026.2.0 contains a patch.	5.3	More Details
CVE-2026-4281	The FormLift for Infusionsoft Web Forms plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 7.5.21. This is due to missing capability checks on the connect() and listen_for_tokens() methods of the FormLift_Infusionsoft_Manager class, both of which are hooked to 'plugins_loaded' and execute on every page load. The connect() function generates an OAuth connection password and leaks it in the redirect Location header without verifying the requesting user is authenticated or authorized. The listen_for_tokens() function only validates the temporary password but performs no user authentication before calling update_option() to save attacker-controlled OAuth tokens and app domain. This makes it possible for unauthenticated attackers to hijack the site's Infusionsoft connection by first triggering the OAuth flow to obtain the temporary password, then using that password to set arbitrary OAuth tokens and app domain via update_option(), effectively redirecting the plugin's API communication to an attacker-controlled server.	5.3	More Details
CVE-2026-34732	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the AVideo CreatePlugin template for list.json.php does not include any authentication or authorization check. While the companion templates add.json.php and delete.json.php both require admin privileges, the list.json.php template was shipped without this guard. Every plugin that uses the CreatePlugin code generator inherits this omission, resulting in 21 unauthenticated data listing endpoints across the platform. These endpoints expose sensitive data including user PII, payment transaction logs, IP addresses, user agents, and internal system records. At time of publication, there are no publicly available patches.	5.3	More Details
CVE-2026-20692	A privacy issue was addressed with improved handling of user preferences. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. "Hide IP Address" and "Block All Remote Content" may not apply to all mail content.	5.3	More Details
CVE-2026-1890	The LeadConnector WordPress plugin before 3.0.22 does not have authorization in a REST route, allowing unauthenticated users to call it and overwrite existing data	5.3	More Details
CVE-2026-33014	EVerest is an EV charging software stack. Prior to version 2026.02.0, during RemoteStop processing, a delayed authorization response restores `authorized` back to true, defeating the `stop_transaction()` call condition on PowerOff events. As a result, the transaction can remain open even after a remote stop. Version 2026.02.0 contains a patch.	5.2	More Details
CVE-2026-24153	NVIDIA Jetson Linux has a vulnerability in initrd, where the nvluks trusted application is not disabled. A successful exploit of this vulnerability might lead to information disclosure.	5.2	More Details
CVE-2026-33015	EVerest is an EV charging software stack. Prior to version 2026.02.0, even immediately after CSMS performs a RemoteStop (StopTransaction), the EVSE can return to `PrepareCharging` via the EV's BCB toggle, allowing session restart. This breaks the irreversibility of remote stop and can bypass operational/billing/safety controls. Version 2026.02.0 contains a patch.	5.2	More Details
CVE-2026-28888	A race condition was addressed with improved state handling. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to gain root privileges.	5.1	More Details
CVE-2026-28834	A race condition was addressed with improved state handling. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to cause unexpected system termination.	5.1	More Details
CVE-2026-33536	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-18 and 6.9.13-43, due to an incorrect return value on certain platforms a pointer is incremented past the end of a buffer that is on the stack and that could result in an out of bounds write. Versions 7.1.2-18 and 6.9.13-43 patch the issue.	5.1	More Details
CVE-2025-36440	IBM Concert 1.0.0 through 2.2.0 could allow a local user to obtain sensitive information due to missing function level access control.	5.1	More Details
CVE-2025-36438	IBM Concert 1.0.0 through 2.2.0 could allow a privileged user to perform unauthorized actions due to improper restriction of channel communication to intended endpoints.	5.1	More Details
CVE-2026-29044	EVerest is an EV charging software stack. Prior to version 2026.02.0, when WithdrawAuthorization is processed before the TransactionStarted event, AuthHandler determines `transaction_active=false` and only calls `withdraw_authorization_callback`. This path ultimately calls `Charger::deauthorize()`, but no actual stop (StopTransaction) occurs in the Charging state. As a result, authorization withdrawal can be defeated by timing, allowing charging to continue. Version 2026.02.0 contains a patch.	5.0	More Details
CVE-2026-34881	OpenStack Glance <29.1.1, >=30.0.0 <30.1.1, ==31.0.0 is affected by Server-Side Request Forgery (SSRF). By use of HTTP redirects, an authenticated user can bypass URL validation checks and redirect to internal services. Only glance image import functionality is affected. In particular, the web-download and glance-download import methods are subject to this vulnerability, as is the optional (not enabled by default) ovf_process image import plugin.	5.0	More Details
CVE-2026-3216	Server-Side Request Forgery (SSRF) vulnerability in Drupal Drupal Canvas allows Server Side Request Forgery.This issue affects Drupal Canvas: from 0.0.0 before 1.1.1.	5.0	More Details
CVE-2026-	Mattermost versions 11.4.x <= 11.4.0, 11.3.x <= 11.3.1, 11.2.x <= 11.2.3, 10.11.x <= 10.11.11 fail to set permissions on downloaded bulk	5.0	More

3113	export which allows other local users on the server to be able to read contents of the bulk export.. Mattermost Advisory ID: MMSA-2026-00593		Details
CVE-2026-34165	go-git is an extensible git implementation library written in pure Go. From version 5.0.0 to before version 5.17.1, a vulnerability has been identified in which a maliciously crafted .idx file can cause asymmetric memory consumption, potentially exhausting available memory and resulting in a denial-of-service (DoS) condition. Exploitation requires write access to the local repository's .git directory, it order to create or alter existing .idx files. This issue has been patched in version 5.17.1.	5.0	More Details
CVE-2026-31799	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. From version 2.14.2 to before version 2.17.0 for parameters "before" and "after" and from version 2.1.0-beta to before version 2.17.0 for parameters "section_id" and "user_id", the /api/v2?cmd=get_home_stats endpoint passes the section_id, user_id, before, and after query parameters directly into SQL via Python %-string formatting without parameterization. An attacker who holds the Tautulli admin API key can inject arbitrary SQL and exfiltrate any value from the Tautulli SQLite database via boolean-blind inference. This issue has been patched in version 2.17.0.	4.9	More Details
CVE-2026-3116	Mattermost Plugins versions <=11.4 11.0.4 11.1.3 11.3.2 10.11.11.0 fail to validate incoming request size which allows an authenticated attacker to cause service disruption via the webhook endpoint. Mattermost Advisory ID: MMSA-2026-00589	4.9	More Details
CVE-2026-33222	NATS-Server is a High-Performance server for NATS.io, a cloud and edge native messaging system. Prior to versions 2.11.15 and 2.12.6, users with JetStream admin API access to restore one stream could restore to other stream names, impacting data which should have been protected against them. Versions 2.11.15 and 2.12.6 contain a fix. As a workaround, if developers have configured users to have limited JetStream restore permissions, temporarily remove those permissions.	4.9	More Details
CVE-2026-4819	In Search Guard FLX versions from 1.0.0 up to 4.0.1, the audit logging feature might log user credentials from users logging into Kibana.	4.9	More Details
CVE-2026-20693	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An attacker with root privileges may be able to delete protected system files.	4.9	More Details
CVE-2026-29092	Kiteworks is a private data network (PDN). Prior to version 9.2.1, a vulnerability in Kiteworks Email Protection Gateway session management allows blocked users to maintain active sessions after their account is disabled. This could allow unauthorized access to continue until the session naturally expires. Upgrade Kiteworks to version 9.2.1 or later to receive a patch.	4.9	More Details
CVE-2026-28823	A path handling issue was addressed with improved validation. This issue is fixed in macOS Tahoe 26.4. An app with root privileges may be able to delete protected system files.	4.9	More Details
CVE-2026-2389	The Complianz – GDPR/CCPA Cookie Consent plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 7.4.4.2. This is due to the `revert_divs_to_summary` function replacing `&#8221;` HTML entities with literal double-quote characters (`"`) in post content without subsequent sanitization. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the injected page. The Classic Editor plugin is required to be installed and activated in order to exploit this vulnerability.	4.9	More Details
CVE-2021-4474	Ruckus Access Point products contain an arbitrary file read vulnerability in the command-line interface that allows authenticated remote attackers with administrative privileges to read arbitrary files from the underlying filesystem. Attackers can exploit this vulnerability to access sensitive information including configuration files, credentials, and system data stored on the device.	4.9	More Details
CVE-2026-33542	Incus is a system container and virtual machine manager. Prior to version 6.23.0, a lack of validation of the image fingerprint when downloading from simplestreams image servers opens the door to image cache poisoning and under very narrow circumstances exposes other tenants to running attacker controlled images rather than the expected one. Version 6.23.0 patches the issue.	4.8	More Details
CVE-2026-27854	An attacker might be able to trigger a use-after-free by sending crafted DNS queries to a DNSdist using the DNSQuestion:getEDNSOptions method in custom Lua code. In some cases DNSQuestion:getEDNSOptions might refer to a version of the DNS packet that has been modified, thus triggering a use-after-free and potentially a crash resulting in denial of service.	4.8	More Details
CVE-2026-3468	A stored Cross-Site Scripting (XSS) vulnerability has been identified in the SonicWall Email Security appliance due to improper neutralization of user-supplied input during web page generation, allowing a remote authenticated attacker as admin user to potentially execute arbitrary JavaScript code.	4.8	More Details
CVE-2026-32794	Improper Certificate Validation vulnerability in Apache Airflow Provider for Databricks. Provider code did not validate certificates for connections to Databricks back-end which could result in a man-of-a-middle attack that traffic is intercepted and manipulated or credentials exfiltrated w/o notice. This issue affects Apache Airflow Provider for Databricks: from 1.10.0 before 1.12.0. Users are recommended to upgrade to version 1.12.0, which fixes the issue.	4.8	More Details
CVE-2025-15612	Wazuh provisioning scripts and Dockerfiles contain an insecure transport vulnerability where curl is invoked with the -k/--insecure flag, disabling SSL/TLS certificate validation. Attackers with network access can perform man-in-the-middle attacks to intercept and modify downloaded dependencies or code during the build process, leading to remote code execution and supply chain compromise.	4.8	More Details
CVE-2026-30568	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0 in in the view_purchase.php file via the "limit" parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	4.8	More Details
CVE-2026-2485	IBM Infosphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	4.8	More Details
CVE-2026-20112	A vulnerability in the web-based Cisco IOx application hosting environment management interface of Cisco IOS XE Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid administrative credentials.	4.8	More Details
CVE-2026-3218	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Responsive Favicons allows Cross-Site Scripting (XSS).This issue affects Responsive Favicons: from 0.0.0 before 2.0.2.	4.8	More Details

CVE-2026-33751	n8n is an open source workflow automation platform. Prior to versions 1.123.27, 2.13.3, and 2.14.1, a flaw in the LDAP node's filter escape logic allowed LDAP metacharacters to pass through unescaped when user-controlled input was interpolated into LDAP search filters. In workflows where external user input is passed via expressions into the LDAP node's search parameters, an attacker could manipulate the constructed filter to retrieve unintended LDAP records or bypass authentication checks implemented in the workflow. Exploitation requires a specific workflow configuration. The LDAP node must be used with user-controlled input passed via expressions (e.g., from a form or webhook). The issue has been fixed in n8n versions 1.123.27, 2.13.3, and 2.14.1. Users should upgrade to one of these versions or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations: Limit workflow creation and editing permissions to fully trusted users only, disable the LDAP node by adding `n8n-nodes-base.ldap` to the `NODES_EXCLUDE` environment variable, and/or avoid passing unvalidated external user input into LDAP node search parameters via expressions. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	4.8	More Details
CVE-2026-33621	PinchTab is a standalone HTTP server that gives AI agents direct control over a Chrome browser. PinchTab `v0.7.7` through `v0.8.4` contain incomplete request-throttling protections for auth-checkable endpoints. In `v0.7.7` through `v0.8.3`, a fully implemented `RateLimitMiddleware` existed in `internal/handlers/middleware.go` but was not inserted into the production HTTP handler chain, so requests were not subject to the intended per-IP throttle. In the same pre-`v0.8.4` range, the original limiter also keyed clients using `X-Forwarded-For`, which would have allowed client-controlled header spoofing if the middleware had been enabled. `v0.8.4` addressed those two issues by wiring the limiter into the live handler chain and switching the key to the immediate peer IP, but it still exempted `/health` and `/metrics` from rate limiting even though `/health` remained an auth-checkable endpoint when a token was configured. This issue weakens defense in depth for deployments where an attacker can reach the API, especially if a weak human-chosen token is used. It is not a direct authentication bypass or token disclosure issue by itself. PinchTab is documented as local-first by default and uses `127.0.0.1` plus a generated random token in the recommended setup. PinchTab's default deployment model is a local-first, user-controlled environment between the user and their agents; wider exposure is an intentional operator choice. This lowers practical risk in the default configuration, even though it does not by itself change the intrinsic base characteristics of the bug. This was fully addressed in `v0.8.5` by applying `RateLimitMiddleware` in the production handler chain, deriving the client address from the immediate peer IP instead of trusting forwarded headers by default, and removing the `/health` and `/metrics` exemption so auth-checkable endpoints are throttled as well.	4.8	More Details
CVE-2026-33732	srvx is a universal server based on web standards. Prior to version 0.11.13, a pathname parsing discrepancy in srvx's `FastURL` allows middleware bypass on the Node.js adapter when a raw HTTP request uses an absolute URI with a non-standard scheme (e.g. `file://`). Starting in version 0.11.13, the `FastURL` constructor now deopts to native `URL` for any string not starting with `/`, ensuring consistent pathname resolution.	4.8	More Details
CVE-2026-1430	The WP Lightbox 2 WordPress plugin before 3.0.7 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2026-30520	A Blind SQL Injection vulnerability exists in SourceCodester Loan Management System v1.0. The vulnerability is located in the ajax.php file (specifically the save_loan action). The application fails to properly sanitize user input supplied to the "borrower_id" parameter in a POST request, allowing an authenticated attacker to inject malicious SQL commands.	4.8	More Details
CVE-2026-33869	Mastodon is a free, open-source social network server based on ActivityPub. In versions on the 4.5.x branch prior to 4.5.8 and on the 4.4.x branch prior to 4.4.15, an attacker that knows of a quote before it has reached a server can prevent it from being correctly processed on that server. The vulnerability has been patched in Mastodon 4.5.8 and 4.4.15. Mastodon 4.3 and earlier are not affected because they do not support quotes.	4.8	More Details
CVE-2026-34441	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to version 0.40.0, cpp-httplib is vulnerable to HTTP Request Smuggling. The server's static file handler serves GET responses without consuming the request body. On HTTP/1.1 keep-alive connections, the unread body bytes remain on the TCP stream and are interpreted as the start of a new HTTP request. An attacker can embed an arbitrary HTTP request inside the body of a GET request, which the server processes as a separate request. This issue has been patched in version 0.40.0.	4.8	More Details
CVE-2026-5203	A vulnerability was found in CMS Made Simple up to 2.2.22. This impacts the function _copyFilesToFolder in the library modules/UserGuide/lib/class.UserGuideImporterExporter.php of the component UserGuide Module XML Import. The manipulation results in path traversal. It is possible to launch the attack remotely. The exploit has been made public and could be used. This issue has been reported early to the project. They confirmed, that "this has already been discovered and fixed for the next release."	4.7	More Details
CVE-2026-4875	A vulnerability was determined in itsourcecode Free Hotel Reservation System 1.0. The affected element is an unknown function of the file /admin/mod_amenities/index.php?view=add. This manipulation of the argument image causes unrestricted upload. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2026-3213	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Anti-Spam by CleanTalk allows Cross-Site Scripting (XSS).This issue affects Anti-Spam by CleanTalk: from 0.0.0 before 9.7.0.	4.7	More Details
CVE-2026-33682	Streamlit is a data oriented application development framework for python. Streamlit Open Source versions prior to 1.54.0 running on Windows hosts have an unauthenticated Server-Side Request Forgery (SSRF) vulnerability. The vulnerability arises from improper validation of attacker-supplied filesystem paths. In certain code paths, including within the `ComponentRequestHandler`, filesystem paths are resolved using `os.path.realpath()` or `Path.resolve()` before sufficient validation occurs. On Windows systems, supplying a malicious UNC path (e.g., `\\attacker-controlled-host\share`) can cause the Streamlit server to initiate outbound SMB connections over port 445. When Windows attempts to authenticate to the remote SMB server, NTLMv2 challenge-response credentials of the Windows user running the Streamlit process may be transmitted. This behavior may allow an attacker to perform NTLM relay attacks against other internal services and/or identify internally reachable SMB hosts via timing analysis. The vulnerability has been fixed in Streamlit Open Source version 1.54.0.	4.7	More Details
CVE-2026-5148	A weakness has been identified in YunaiV yudao-cloud up to 2026.01. This vulnerability affects unknown code of the file /admin-api/system/mail-log/page. This manipulation of the argument toMail causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-5041	A vulnerability was identified in code-projects Chamber of Commerce Membership Management System 1.0. Impacted is the function fwrite of the file admin/pageMail.php. The manipulation of the argument mailSubject/mailMessage leads to command injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	4.7	More Details
CVE-2026-33916	Handlebars provides the power necessary to let users build semantic templates. In versions 4.0.0 through 4.7.8, `resolvePartial()` in the Handlebars runtime resolves partial names via a plain property lookup on `options.partials` without guarding against prototype-chain traversal. When `Object.prototype` has been polluted with a string value whose key matches a partial reference in a template, the polluted string is used as the partial body and rendered without HTML escaping, resulting in reflected or stored XSS. Version 4.7.9 fixes the issue. Some workarounds are available. Apply `Object.freeze(Object.prototype)` early in application startup to prevent prototype pollution. Note: this may break other libraries, and/or use the Handlebars runtime-only build (`handlebars/runtime`), which does not compile templates and reduces the attack	4.7	More Details

	surface.		
CVE-2026-27599	CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input within System Settings – Mail Settings. Several configuration fields, including Mail Server, Mail Port, Email Address, Email Password, Mail Protocol, and TLS settings, accept attacker-controlled input that is stored server-side and later rendered without proper output encoding. This issue has been patched in version 0.31.0.0.	4.7	More Details
CVE-2026-26070	EVerest is an EV charging software stack. Versions prior to 2026.02.0 have a data race leading to `std::map<std::optional>` concurrent access (container/optional corruption possible). The trigger is an EV SoC update with powermeter periodic update and unplugging/SessionFinished state. Version 2026.2.0 contains a patch.	4.6	More Details
CVE-2026-28528	BlueKitchen BTstack versions prior to 1.8.1 contain an out-of-bounds read vulnerability in the AVRCP Browsing Target GET_FOLDER_ITEMS handler that fails to validate packet boundaries and attribute count data. An attacker with a paired Bluetooth Classic connection can exploit insufficient bounds checking on the attr_id parameter to cause crashes and corrupt attribute bitmap state.	4.6	More Details
CVE-2026-27659	Mattermost versions 11.2.x <= 11.2.2, 10.11.x <= 10.11.10, 11.4.x <= 11.4.0, 11.3.x <= 11.3.1 fail to properly validate CSRF tokens in the /api/v4/access_control_policies/{policy_id}/activate endpoint, which allows an attacker to trick an admin into changing access control policy active status via a crafted request.. Mattermost Advisory ID: MMSA-2026-00578	4.6	More Details
CVE-2026-33653	Ulloady is a file uploader script with multi-file upload support. A Stored Cross-Site Scripting (XSS) vulnerability exists in versions prior to 3.1.2 due to improper sanitization of filenames during the file upload process. An attacker can upload a file with a malicious filename containing JavaScript code, which is later rendered in the application without proper escaping. When the filename is displayed in the file list or file details page, the malicious script executes in the browser of any user who views the page. Version 3.1.2 fixes the issue.	4.6	More Details
CVE-2026-28856	The issue was addressed with improved authentication. This issue is fixed in iOS 26.4 and iPadOS 26.4, visionOS 26.4, watchOS 26.4. An attacker with physical access to a locked device may be able to view sensitive user information.	4.6	More Details
CVE-2026-34382	Admidio is an open-source user management solution. From version 5.0.0 to before version 5.0.8, the delete mode handler in mylist_function.php permanently deletes list configurations without validating a CSRF token. An attacker who can lure an authenticated user to a malicious page can silently destroy that user's list configurations — including organization-wide shared lists when the victim holds administrator rights. This issue has been patched in version 5.0.8.	4.6	More Details
CVE-2026-28895	The issue was addressed with improved checks. This issue is fixed in iOS 26.4 and iPadOS 26.4. An attacker with physical access to an iOS device with Stolen Device Protection enabled may be able to access biometrics-gated Protected Apps with the passcode.	4.6	More Details
CVE-2026-34384	Admidio is an open-source user management solution. Prior to version 5.0.8, the create_user, assign_member, and assign_user action modes in modules/registration.php approve pending user registrations via GET request without validating a CSRF token. Unlike the delete_user mode in the same file (which correctly validates the token), these three approval actions read their parameters from $_GET and perform irreversible state changes without any protection. An attacker who has submitted a pending registration can extract their own user UUID from the registration confirmation email URL, then trick any user with the rol_approve_users right into visiting a crafted URL that automatically approves the registration. This bypasses the manual registration approval workflow entirely. This issue has been patched in version 5.0.8.	4.5	More Details
CVE-2025-36187	IBM Knowledge Catalog Standard Cartridge 5.0.0, 5.0.1, 5.0.2, 5.0.3, 5.1, 5.1.1, 5,1.2, 5.1.3, 5.2.0, 5.2.1 stores potentially sensitive information in log files that could be read by a local privileged user.	4.4	More Details
CVE-2026-25645	Requests is a HTTP library. Prior to version 2.33.0, the `requests.utils.extract_zipped_paths()` utility function uses a predictable filename when extracting files from zip archives into the system temporary directory. If the target file already exists, it is reused without validation. A local attacker with write access to the temp directory could pre-create a malicious file that would be loaded in place of the legitimate one. Standard usage of the Requests library is not affected by this vulnerability. Only applications that call `extract_zipped_paths()` directly are impacted. Starting in version 2.33.0, the library extracts files to a non-deterministic location. If developers are unable to upgrade, they can set `TMPDIR` in their environment to a directory with restricted write access.	4.4	More Details
CVE-2026-3190	A flaw was found in Keycloak. The User-Managed Access (UMA) 2.0 Protection API endpoint for permission tickets fails to enforce the `uma_protection` role check. This allows any authenticated user with a token issued for a resource server client, even without the `uma_protection` role, to enumerate all permission tickets in the system. This vulnerability partial leads to information disclosure.	4.3	More Details
CVE-2025-59031	Dovecot has provided a script to use for attachment to text conversion. This script unsafely handles zip-style attachments. Attacker can use specially crafted OOXML documents to cause unintended files on the system to be indexed and subsequently ending up in FTS indexes. Do not use the provided script, instead, use something else like FTS tika. No publicly available exploits are known.	4.3	More Details
CVE-2026-4846	A vulnerability has been found in dameng100 muucmf 1.9.5.20260309. The affected element is an unknown function of the file channel/admin.Account/autoReply.html. Such manipulation of the argument keyword leads to cross site scripting. It is possible to launch the attack 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-2026-33620	PinchTab is a standalone HTTP server that gives AI agents direct control over a Chrome browser. PinchTab `v0.7.8` through `v0.8.3` accepted the API token from a `token` URL query parameter in addition to the `Authorization` header. When a valid API credential is sent in the URL, it can be exposed through request URIs recorded by intermediaries or client-side tooling, such as reverse proxy access logs, browser history, shell history, clipboard history, and tracing systems that capture full URLs. This issue is an unsafe credential transport pattern rather than a direct authentication bypass. It only affects deployments where a token is configured and a client actually uses the query-parameter form. PinchTab's security guidance already recommended `Authorization: Bearer <token>`, but `v0.8.3` still accepted `?token=` and included first-party flows that generated and consumed URLs containing the token. This was addressed in v0.8.4 by removing query-string token authentication and requiring safer header- or session-based authentication flows.	4.3	More Details
CVE-2026-34506	OpenClaw before 2026.3.8 contains a sender allowlist bypass vulnerability in its Microsoft Teams plugin that allows unauthorized senders to bypass intended authorization checks. When a team/channel route allowlist is configured with an empty groupAllowFrom parameter, the message handler synthesizes wildcard sender authorization, permitting any sender in the matched team/channel to trigger replies in allowlisted Teams routes.	4.3	More Details
CVE-2025-55268	HCL Aftermarket DPC is affected by Spamming Vulnerability which can allow the actor to excessive spamming can consume server bandwidth and processing resources which may lead to Denial of Service.	4.3	More Details
CVE-2026-	A flaw has been found in dameng100 muucmf 1.9.5.20260309. Impacted is an unknown function of the file /admin/Member/index.html. This manipulation of the argument Search causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been published	4.3	More

4845	and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		Details
CVE-2026-33764	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the AI plugin's `save.json.php` endpoint loads AI response objects using an attacker-controlled `$_REQUEST['id']` parameter without validating that the AI response belongs to the specified video. An authenticated user with AI permissions can reference any AI response ID — including those generated for other users' private videos — and apply the stolen AI-generated content (titles, descriptions, keywords, summaries, or full transcriptions) to their own video, effectively exfiltrating the information. Commit aa2c46a806960a0006105df47765913394eec142 contains a patch.	4.3	More Details
CVE-2026-32951	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, an authenticated user can obtain shared draft topic titles by sending an inline onebox request with a category_id parameter matching the shared drafts category. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.	4.3	More Details
CVE-2026-4848	A vulnerability was determined in dameng100 muucmf 1.9.5.20260309. This affects an unknown function of the file /admin/extend/list.html. Executing a manipulation of the argument Name can lead to cross site scripting. The attack can be launched 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.	4.3	More Details
CVE-2026-5015	A vulnerability was determined in elecV2 elecV2P up to 3.8.3. The impacted element is an unknown function of the file /logs of the component Endpoint. This manipulation of the argument filename causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-20691	An authorization issue was addressed with improved state management. This issue is fixed in Safari 26.4, iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, visionOS 26.4, watchOS 26.4. A maliciously crafted webpage may be able to fingerprint the user.	4.3	More Details
CVE-2026-20664	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.4, iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, visionOS 26.4. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
CVE-2026-4849	A vulnerability was identified in code-projects Simple Laundry System 1.0. This impacts an unknown function of the file /modify.php of the component Parameter Handler. The manipulation of the argument firstName leads to cross site scripting. The attack may be initiated remotely. The exploit is publicly available and might be used.	4.3	More Details
CVE-2026-1206	The Elementor Website Builder plugin for WordPress is vulnerable to Incorrect Authorization to Sensitive Information Exposure in all versions up to, and including, 3.35.7. This is due to a logic error in the is_allowed_to_read_template() function permission check that treats non-published templates as readable without verifying edit capabilities. This makes it possible for authenticated attackers, with contributor-level access and above, to read private or draft Elementor template content via the 'template_id' supplied to the 'get_template_data' action of the 'elementor_ajax' endpoint.	4.3	More Details
CVE-2026-34509	OpenClaw before 2026.3.8 contains a sender allowlist bypass vulnerability in its Microsoft Teams plugin that allows unauthorized senders to bypass intended authorization checks. When a team/channel route allowlist is configured with an empty groupAllowFrom parameter, the message handler synthesizes wildcard sender authorization, permitting any sender in the matched team/channel to trigger replies in allowlisted Teams routes.	4.3	More Details
CVE-2026-4331	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to unauthorized data loss in all versions up to, and including, 8.8.2. This is due to the resetSocialMetaTags() function only verifying that the user has the 'read' capability and a valid b2s_security_nonce, both of which are available to Subscriber-level users, as the plugin grants 'blog2social_access' capability to all roles upon activation, allowing them to access the plugin's admin pages where the nonce is output. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete all _b2s_post_meta records from the wp_postmeta table, permanently removing all custom social media meta tags for every post on the site.	4.3	More Details
CVE-2026-34738	WWBN AVideo is an open source video platform. In versions 26.0 and prior, AVideo's video processing pipeline accepts an overrideStatus request parameter that allows any uploader to set a video's status to any valid state, including "active" (a). This bypasses the admin-controlled moderation and draft workflows. The setStatus() method validates the status code against a list of known values but does not verify that the caller has permission to set that particular status. As a result, any user with upload permissions can publish videos directly, circumventing content review processes. At time of publication, there are no publicly available patches.	4.3	More Details
CVE-2026-33644	Lychee is a free, open-source photo-management tool. Prior to version 7.5.2, the SSRF protection in `PhotoUrlRule.php` can be bypassed using DNS rebinding. The IP validation check (line 86-89) only activates when the hostname is an IP address. When a domain name is used, `filter_var($host, FILTER_VALIDATE_IP)` returns `false`, skipping the entire check. Version 7.5.2 patches the issue.	4.3	More Details
CVE-2026-4393	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Automated Logout allows Cross Site Request Forgery.This issue affects Automated Logout: from 0.0.0 before 1.7.0, from 2.0.0 before 2.0.2.	4.3	More Details
CVE-2026-33934	OpenEMR is a free and open source electronic health records and medical practice management application. Versions prior to 8.0.0.3 have a missing authorization check in `portal/sign/lib/show-signature.php` that allows any authenticated patient portal user to retrieve the drawn signature image of any staff member by supplying an arbitrary `user` value in the POST body. The companion write endpoint (`save-signature.php`) was already hardened against this same issue, but the read endpoint was not updated to match. Version 8.0.0.3 patches the issue.	4.3	More Details
CVE-2026-5031	A vulnerability was found in BichitroGan ISP Billing Software 2025.3.20. Impacted is an unknown function of the file /?_route=settings/users-view/ of the component Endpoint. The manipulation of the argument ID results in improper control of resource identifiers. 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.	4.3	More Details
CVE-2026-32618	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, there is possible channel membership inference from chat user search without authorization. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.	4.3	More Details
CVE-2026-33635	iCalendar is a Ruby library for dealing with iCalendar files in the iCalendar format defined by RFC-5545. Starting in version 2.0.0 and prior to version 2.12.2, .ics serialization does not properly sanitize URI property values, enabling ICS injection through attacker-controlled input, adding arbitrary calendar lines to the output. `Icalendar::Values::Uri` falls back to the raw input string when `URI.parse` fails and later serializes it with `value.to_s` without removing or escaping `\r` or `\n` characters. That value is embedded directly into the final ICS line by the normal serializer, so a payload containing CRLF can terminate the original property and create a new ICS property or component. (It looks like you can inject via url, source, image, organizer, attach, attendee, conference, tzurl because of this). Applications that generate `.ics` files from partially untrusted metadata are impacted. As a result, downstream calendar clients or importers may process attacker-supplied content as if it were legitimate event data, such as added attendees, modified URLs, alarms, or other calendar fields. Version 2.12.2 contains a patch for the issue.	4.3	More Details

CVE-2026-1166	Open Redirect vulnerability in Hitachi Ops Center Administrator.This issue affects Hitachi Ops Center Administrator: from 10.2.0 before 11.0.8.	4.3	More Details
CVE-2026-5157	A vulnerability was identified in code-projects Online Food Ordering System 1.0. Affected is an unknown function of the file /form/order.php of the component Order Module. Such manipulation of the argument cust_id leads to cross site scripting. The attack may be performed from remote. The exploit is publicly available and might be used.	4.3	More Details
CVE-2026-4898	A vulnerability was identified in code-projects Online Food Ordering System 1.0. Affected by this vulnerability is an unknown functionality of the file /dbfood/contact.php. The manipulation of the argument Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	4.3	More Details
CVE-2026-3139	The User Profile Builder – Beautiful User Registration Forms, User Profiles & User Role Editor plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 3.15.5 via the wppb_save_avatar_value() function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to reassign ownership of arbitrary posts and attachments by changing 'post_author'.	4.3	More Details
CVE-2026-34383	Admidio is an open-source user management solution. Prior to version 5.0.8, the inventory module's item_save endpoint accepts a user-controllable POST parameter imported that, when set to true, completely bypasses both CSRF token validation and server-side form validation. An authenticated user can craft a direct POST request to save arbitrary inventory item data without CSRF protection and without the field value checks that the FormPresenter validation normally enforces. This issue has been patched in version 5.0.8.	4.3	More Details
CVE-2026-3530	Server-Side Request Forgery (SSRF) vulnerability in Drupal OpenID Connect / OAuth client allows Server Side Request Forgery.This issue affects OpenID Connect / OAuth client: from 0.0.0 before 1.5.0.	4.3	More Details
CVE-2026-33249	NATS-Server is a High-Performance server for NATS.io, a cloud and edge native messaging system. Starting in version 2.11.0 and prior to versions 2.11.15 and 2.12.6, a valid client which uses message tracing headers can indicate that the trace messages can be sent to an arbitrary valid subject, including those to which the client does not have publish permission. The payload is a valid trace message and not chosen by the attacker. Versions 2.11.15 and 2.12.6 contain a fix. No known workarounds are available.	4.3	More Details
CVE-2026-4877	A security flaw has been discovered in itsourcecode Payroll Management System up to 1.0. This affects an unknown function of the file /index.php. Performing a manipulation of the argument page results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	4.3	More Details
CVE-2026-3115	Mattermost versions 11.2.x <= 11.2.2, 10.11.x <= 10.11.10, 11.4.x <= 11.4.0, 11.3.x <= 11.3.1 fail to apply view restrictions when retrieving group member IDs, which allows authenticated guest users to enumerate user IDs outside their allowed visibility scope via the group retrieval endpoint.. Mattermost Advisory ID: MMSA-2026-00594	4.3	More Details
CVE-2026-3211	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Theme Negotiation by Rules allows Cross Site Request Forgery.This issue affects Theme Negotiation by Rules: from 0.0.0 before 1.2.1.	4.3	More Details
CVE-2025-36422	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 IBM InfoSphere DataStage Flow Designer 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.	4.3	More Details
CVE-2026-4992	A flaw has been found in wandb OpenUI up to 1.0. This affects the function create_share/get_share of the file backend/openui/server.py of the component HTMLAnnotator Component. Executing a manipulation of the argument ID can lead to HTML injection. The attack may be performed from remote. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-33477	FileRise is a self-hosted web-based file manager with multi-file upload, editing, and batch operations. In versiosn 2.3.7 through 3.10.0, the file snippet endpoint `/api/file/snippet.php` allows an authenticated user with only `read_own` access to a folder to retrieve snippet content from files uploaded by other users in the same folder. This is a server-side authorization flaw in the `read_own` enforcement for hover previews. Version 3.11.0 fixes the issue.	4.3	More Details
CVE-2026-33868	Mastodon is a free, open-source social network server based on ActivityPub. Prior to versions 4.5.8, 4.4.15, and 4.3.21, an unauthenticated Open Redirect vulnerability (CWE-601) exists in the `/web/*` route due to improper handling of URL-encoded path segments. An attacker can craft a specially encoded URL that causes the application to redirect users to an arbitrary external domain, enabling phishing attacks and potential OAuth credential theft. The issue occurs because URL-encoded slashes (`%2F`) bypass Rails path normalization and are interpreted as host-relative redirects. Versions 4.5.8, 4.4.15, and 4.3.21 patch the issue.	4.3	More Details
CVE-2026-2726	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 11.10 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1 that could have allowed an authenticated user to perform unauthorized actions on merge requests in other projects due to improper access control during cross-repository operations.	4.3	More Details
CVE-2026-28871	A logic issue was addressed with improved checks. This issue is fixed in Safari 26.4, iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4. Visiting a maliciously crafted website may lead to a cross-site scripting attack.	4.3	More Details
CVE-2026-28859	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.4, iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. A malicious website may be able to process restricted web content outside the sandbox.	4.3	More Details
CVE-2026-28861	A logic issue was addressed with improved state management. This issue is fixed in Safari 26.4, iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, visionOS 26.4. A malicious website may be able to access script message handlers intended for other origins.	4.3	More Details
CVE-2025-14595	GitLab has remediated an issue in GitLab EE affecting all versions from 18.6 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1 that under certain conditions could have allowed an authenticated user with Planner role to view security category metadata and attributes in group security configuration due to improper access control	4.3	More Details
CVE-2026-26233	Mattermost versions 11.4.x <= 11.4.0, 11.3.x <= 11.3.1, 11.2.x <= 11.2.3, 10.11.x <= 10.11.11 fail to rate limit login requests which allows unauthenticated remote attackers to cause denial of service (server crash and restart) via HTTP/2 single packet attack with 100+ parallel login requests.. Mattermost Advisory ID: MMSA-2025-00566	4.3	More Details
CVE-	A vulnerability was identified in dloebl CGIF up to 0.5.2. This vulnerability affects the function cgif_addframe of the file src/cgif.c of the		More

2026-4985	component GIF Image Handler. The manipulation of the argument width/height leads to integer overflow. The attack may be initiated remotely. The identifier of the patch is b0ba830093f4317a5d1f345715d2fa3cd2dab474. It is suggested to install a patch to address this issue.	4.3	Details
CVE-2026-33578	OpenClaw before 2026.3.28 contains a sender policy bypass vulnerability in the Google Chat and Zalouser extensions where route-level group allowlist policies silently downgrade to open policy. Attackers can exploit this policy resolution flaw to bypass sender restrictions and interact with bots despite configured allowlist restrictions.	4.3	More Details
CVE-2026-20719	Mattermost versions 11.4.x <= 11.4.0, 11.3.x <= 11.3.1, 11.2.x <= 11.2.3, 10.11.x <= 10.11.11 fail to prevent rendering of external SVGs on link embeds which allows unauthenticated users to crash the Mattermost webapp and desktop app via creating an issue or PR on GitHub.. Mattermost Advisory ID: MMSA-2026-00595	4.3	More Details
CVE-2026-5215	A vulnerability was identified in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205. The impacted element is the function cgi_get_ipv6 of the file /cgi-bin/network_mgr.cgi. Such manipulation leads to improper access controls. The exploit is publicly available and might be used.	4.3	More Details
CVE-2026-27857	Sending "NOOP (((...)))" command with 4000 parenthesis open+close results in ~1MB extra memory usage. Longer commands will result in client disconnection. This 1 MB can be left allocated for longer time periods by not sending the command ending LF. So attacker could connect possibly from even a single IP and create 1000 connections to allocate 1 GB of memory, which would likely result in reaching VSZ limit and killing the process and its other proxied connections. Attacker could connect possibly from even a single IP and create 1000 connections to allocate 1 GB of memory, which would likely result in reaching VSZ limit and killing the process and its other proxied connections. Install fixed version, there is no other remediation. No publicly available exploits are known.	4.3	More Details
CVE-2026-4971	A weakness has been identified in SourceCodester Note Taking App up to 1.0. This impacts an unknown function. This manipulation causes cross-site request forgery. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	4.3	More Details
CVE-2026-4799	In Search Guard FLX up to version 4.0.1, it is possible to use specially crafted requests to redirect the user to an untrusted URL.	4.3	More Details
CVE-2026-33884	Statamic is a Laravel and Git powered content management system (CMS). Prior to versions 5.73.16 and 6.7.2, an authenticated Control Panel user with access to live preview could use a live preview token to access restricted content that the token was not intended for. This has been fixed in 5.73.16 and 6.7.2.	4.3	More Details
CVE-2026-1032	The Conditional Menus plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.6. This is due to missing nonce validation on the 'save_options' function. This makes it possible for unauthenticated attackers to modify conditional menu assignments 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-2026-2272	A flaw was found in GIMP. An integer overflow vulnerability exists when processing ICO image files, specifically in the `ico_read_info` and `ico_read_icon` functions. This issue arises because a size calculation for image buffers can wrap around due to a 32-bit integer evaluation, allowing oversized image headers to bypass security checks. A remote attacker could exploit this by providing a specially crafted ICO file, leading to a buffer overflow and memory corruption, which may result in an application level denial of service.	4.3	More Details
CVE-2026-28786	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to version 0.8.6, an unsanitized filename field in the speech-to-text transcription endpoint allows any authenticated non-admin user to trigger a `FileNotFoundError` whose message — including the server's absolute `DATA_DIR` path — is returned verbatim in the HTTP 400 response body, confirming information disclosure on all default deployments. Version 0.8.6 patches the issue.	4.3	More Details
CVE-2026-4847	A vulnerability was found in dameng100 muucmf 1.9.5.20260309. The impacted element is an unknown function of the file /admin/config/list.html. Performing a manipulation of the argument Name results in cross site scripting. The attack can be initiated 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.	4.3	More Details
CVE-2025-40841	Ericsson Indoor Connect 8855 versions prior to 2025.Q3 contains a Cross-Site Request Forgery (CSRF) vulnerability which, if exploited, can lead to unauthorized modification of certain information.	4.3	More Details
CVE-2026-33532	`yaml` is a YAML parser and serialiser for JavaScript. Parsing a YAML document with a version of `yaml` on the 1.x branch prior to 1.10.3 or on the 2.x branch prior to 2.8.3 may throw a RangeError due to a stack overflow. The node resolution/composition phase uses recursive function calls without a depth bound. An attacker who can supply YAML for parsing can trigger a `RangeError: Maximum call stack size exceeded` with a small payload (~2–10 KB). The `RangeError` is not a `YAMLParseError`, so applications that only catch YAML-specific errors will encounter an unexpected exception type. Depending on the host application's exception handling, this can fail requests or terminate the Node.js process. Flow sequences allow deep nesting with minimal bytes (2 bytes per level: one `[` and one `]`). On the default Node.js stack, approximately 1,000–5,000 levels of nesting (2–10 KB input) exhaust the call stack. The exact threshold is environment-dependent (Node.js version, stack size, call stack depth at invocation). Note: the library's `Parser` (CST phase) uses a stack-based iterative approach and is not affected. Only the compose/resolve phase uses actual call-stack recursion. All three public parsing APIs are affected: `YAML.parse()`, `YAML.parseDocument()`, and `YAML.parseAllDocuments()`. Versions 1.10.3 and 2.8.3 contain a patch.	4.3	More Details
CVE-2025-55273	HCL Aftermarket DPC is affected by Cross Domain Script Include vulnerability where an attacker using external scripts can tamper with the DOM, altering the content or behavior of the application. Malicious scripts can steal cookies or session tokens, leading to session hijacking.	4.3	More Details
CVE-2026-1917	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal Login Disable allows Functionality Bypass.This issue affects Login Disable: from 0.0.0 before 2.1.3.	4.3	More Details
CVE-2026-2484	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is affected by an information exposure vulnerability caused by overly verbose error messages	4.3	More Details
CVE-2026-1262	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is affected by an information disclosure vulnerability.	4.3	More Details
CVE-2026-4968	A vulnerability was determined in SourceCodester Diary App 1.0. The affected element is an unknown function of the file diary.php. Executing a manipulation can lead to cross-site request forgery. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	4.3	More Details

CVE-2026-26072	EVerest is an EV charging software stack. Versions prior to 2026.02.0 have a data race leading to `std::map<std::optional>` concurrent access (container/optional corruption possible). The trigger is EV SoC update with powermeter periodic update and unplugging/SessionFinished status. Version 2026.02.0 patches the issue.	4.2	More Details
CVE-2026-32187	Microsoft Edge (Chromium-based) Defense in Depth Vulnerability	4.2	More Details
CVE-2026-26071	EVerest is an EV charging software stack. Versions prior to 2026.02.0 have a data race leading to `std::string` concurrent access. with heap-use-after-free possible. This is triggered by EVCCID update (EV/ISO15118) and OCPP session/authorization events. Version 2026.02.0 contains a patch.	4.2	More Details
CVE-2026-33720	n8n is an open source workflow automation platform. Prior to version 2.8.0, when the `N8N_SKIP_AUTH_ON_OAUTH_CALLBACK` environment variable is set to `true`, the OAuth callback handler skips ownership verification of the OAuth state parameter. This allows an attacker to trick a victim into completing an OAuth flow against a credential object the attacker controls, causing the victim's OAuth tokens to be stored in the attacker's credential. The attacker can then use those tokens to execute workflows in their name. This issue only affects instances where `N8N_SKIP_AUTH_ON_OAUTH_CALLBACK=true` is explicitly configured (non-default). The issue has been fixed in n8n version 2.8.0. Users should upgrade to this version or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations: Avoid enabling `N8N_SKIP_AUTH_ON_OAUTH_CALLBACK=true` unless strictly required, and/ or restrict access to the n8n instance to fully trusted users only. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.	4.2	More Details
CVE-2025-55269	HCL Aftermarket DPC is affected by Weak Password Policy vulnerability, which makes it easier for attackers to guess weak passwords or use brute-force techniques to gain unauthorized access to user accounts.	4.2	More Details
CVE-2026-3532	Improper Handling of Case Sensitivity vulnerability in Drupal OpenID Connect / OAuth client allows Privilege Escalation.This issue affects OpenID Connect / OAuth client: from 0.0.0 before 1.5.0.	4.2	More Details
CVE-2026-27814	EVerest is an EV charging software stack. Versions prior to 2026.02.0 have a data race (C++ UB) triggered by an A 1-phase ↔ 3-phase switch request (`ac_switch_three_phases_while_charging`) during charging/waiting executes concurrently with the state machine loop. Version 2026.02.0 contains a patch.	4.2	More Details
CVE-2026-5107	A vulnerability has been found in FRRouting FRR up to 10.5.1. This affects the function process_type2_route of the file bgpd/bgp_evpn.c of the component EVPN Type-2 Route Handler. The manipulation leads to improper access controls. The attack can be initiated remotely. The attack is considered to have high complexity. The exploitability is reported as difficult. The identifier of the patch is 7676cad65114aa23adde583d91d9d29e2debd045. To fix this issue, it is recommended to deploy a patch.	4.2	More Details
CVE-2026-33248	NATS-Server is a High-Performance server for NATS.io, a cloud and edge native messaging system. Prior to versions 2.11.15 and 2.12.6, when using mTLS for client identity, with `verify_and_map` to derive a NATS identity from the client certificate's Subject DN, certain patterns of RDN would not be correctly enforced, allowing for authentication bypass. This does require a valid certificate from a CA already trusted for client certificates, and `DN` naming patterns which the NATS maintainers consider highly unlikely. So this is an unlikely attack. Nonetheless, administrators who have been very sophisticated in their `DN` construction patterns might conceivably be impacted. Versions 2.11.15 and 2.12.6 contain a fix. As a workaround, developers should review their CA issuing practices.	4.2	More Details
CVE-2026-33619	PinchTab is a standalone HTTP server that gives AI agents direct control over a Chrome browser. PinchTab v0.8.3 contains a server-side request forgery issue in the optional scheduler's webhook delivery path. When a task is submitted to `POST /tasks` with a user-controlled `callbackUrl`, the v0.8.3 scheduler sends an outbound HTTP `POST` to that URL when the task reaches a terminal state. In that release, the webhook path validated only the URL scheme and did not reject loopback, private, link-local, or other non-public destinations. Because the v0.8.3 implementation also used the default HTTP client behavior, redirects were followed and the destination was not pinned to validated IPs. This allowed blind SSRF from the PinchTab server to attacker-chosen HTTP(S) targets reachable from the server. This issue is narrower than a general unauthenticated internet-facing SSRF. The scheduler is optional and off by default, and in token-protected deployments the attacker must already be able to submit tasks using the server's master API token. In PinchTab's intended deployment model, that token represents administrative control rather than a low-privilege role. Tokenless deployments lower the barrier further, but that is a separate insecure configuration state rather than impact created by the webhook bug itself. PinchTab's default deployment model is local-first and user-controlled, with loopback bind and token-based access in the recommended setup. That lowers practical risk in default use, even though it does not remove the underlying webhook issue when the scheduler is enabled and reachable. This was addressed in v0.8.4 by validating callback targets before dispatch, rejecting non-public IP ranges, pinning delivery to validated IPs, disabling redirect following, and validating `callbackUrl` during task submission.	4.1	More Details
CVE-2026-28826	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Tahoe 26.4. A malicious app may be able to break out of its sandbox.	4.0	More Details
CVE-2025-14684	IBM Maximo Application Suite - Monitor Component 9.1, 9.0, 8.11, and 8.10 could allow an unauthorized user to inject data into log messages due to improper neutralization of special elements when written to log files.	4.0	More Details
CVE-2026-20607	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access protected user data.	4.0	More Details
CVE-2026-34553	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Prior to version 2.3.1.6, there is a defect in LUT dump/iteration logic affecting CIccCLUT::Iterate() and output produced by CIccMBB::Describe() (via CLUT dumping). This issue has been patched in version 2.3.1.6.	4.0	More Details
CVE-2026-28882	This issue was addressed with improved checks. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An app may be able to enumerate a user's installed apps.	4.0	More Details
CVE-2026-33535	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-18 and 6.9.13-43, an out-of-bounds write of a zero byte exists in the X11 `display` interaction path that could lead to a crash. Versions 7.1.2-18 and 6.9.13-43 patch the issue.	4.0	More Details
CVE-2026-	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS	4.0	More

28816	Tahoe 26.4. An app may be able to delete files for which it does not have permission.		Details
CVE-2026-31804	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. Prior to version 2.17.0, the /pms_image_proxy endpoint accepts a user-supplied img parameter and forwards it to Plex Media Server's /photo/:/ transcode transcoder without authentication and without restricting the scheme or host. The endpoint is intentionally excluded from all authentication checks in webstart.py, any value of img beginning with http is passed directly to Plex, this causes the Plex Media Server process, which typically runs on the same host or internal network as Tautulli, with access to RFC-1918 address space, to issue an outbound HTTP request to any attacker-specified URL. This issue has been patched in version 2.17.0.	4.0	More Details
CVE-2025-66037	OpenSC is an open source smart card tools and middleware. Prior to version 0.27.0, feeding a crafted input to the fuzz_pkcs15_reader harness causes OpenSC to perform an out-of-bounds heap read in the X.509/SPKI handling path. Specifically, sc_pkcs15_pubkey_from_spki_fields() allocates a zero-length buffer and then reads one byte past the end of that allocation. This issue has been patched in version 0.27.0.	3.9	More Details
CVE-2025-66038	OpenSC is an open source smart card tools and middleware. Prior to version 0.27.0, sc_compacttlv_find_tag searches a compact-TLV buffer for a given tag. In compact-TLV, a single byte encodes the tag (high nibble) and value length (low nibble). With a 1-byte buffer {0x0A}, the encoded element claims tag=0 and length=10 but no value bytes follow. Calling sc_compacttlv_find_tag with search tag 0x00 returns a pointer equal to buf+1 and outlen=10 without verifying that the claimed value length fits within the remaining buffer. In cases where the sc_compacttlv_find_tag is provided untrusted data (such as being read from cards/files), attackers may be able to influence it to return out-of-bounds pointers leading to downstream memory corruption when subsequent code tries to dereference the pointer. This issue has been patched in version 0.27.0.	3.9	More Details
CVE-2025-66215	OpenSC is an open source smart card tools and middleware. Prior to version 0.27.0, an attacker with physical access to the computer at the time user or administrator uses a token can cause a stack-buffer-overflow WRITE in card-oberthur. The attack requires crafted USB device or smart card that would present the system with specially crafted responses to the APDUs. This issue has been patched in version 0.27.0.	3.8	More Details
CVE-2025-49010	OpenSC is an open source smart card tools and middleware. Prior to version 0.27.0, an attacker with physical access to the computer at the time user or administrator uses a token can cause a stack-buffer-overflow write in GET RESPONSE. The attack requires crafted USB device or smart card that would present the system with specially crafted responses to the APDUs. This issue has been patched in version 0.27.0.	3.8	More Details
CVE-2026-3470	A vulnerability exists in the SonicWall Email Security appliance due to improper input sanitization that may lead to data corruption, allowing a remote authenticated attacker as admin user could exploit this issue by providing crafted input that corrupts application database.	3.8	More Details
CVE-2026-5124	A security vulnerability has been detected in osrg GoBGP up to 4.3.0. Affected is the function BGPHeader.DecodeFromBytes of the file pkg/packet/bgp/bgp.go of the component BGP Header Handler. The manipulation leads to improper access controls. Remote exploitation of the attack is possible. The attack is considered to have high complexity. The exploitability is told to be difficult. The identifier of the patch is f0f24a2a901cbf159260698211ab15c583ced131. To fix this issue, it is recommended to deploy a patch.	3.7	More Details
CVE-2026-5123	A weakness has been identified in osrg GoBGP up to 4.3.0. This impacts the function DecodeFromBytes of the file pkg/packet/bgp/bgp.go. Executing a manipulation of the argument data[1] can lead to off-by-one. The attack may be launched remotely. Attacks of this nature are highly complex. The exploitability is said to be difficult. This patch is called 67c059413470df64bc20801c46f64058e88f800f. A patch should be applied to remediate this issue.	3.7	More Details
CVE-2026-5122	A security flaw has been discovered in osrg GoBGP up to 4.3.0. This affects the function DecodeFromBytes of the file pkg/packet/bgp/bgp.go of the component BGP OPEN Message Handler. Performing a manipulation of the argument domainNameLen results in improper access controls. The attack may be initiated remotely. A high degree of complexity is needed for the attack. The exploitability is reported as difficult. The patch is named 2b09db390a3d455808363c53e409afe6b1b86d2d. It is suggested to install a patch to address this issue.	3.7	More Details
CVE-2025-55275	HCL Aftermarket DPC is affected by Admin Session Concurrency vulnerability using which an attacker can exploit concurrent sessions to hijack or impersonate an admin user.	3.7	More Details
CVE-2026-4831	A security flaw has been discovered in kalcaddle kodbox 1.64. Impacted is the function can of the file /workspace/source-code/app/controller/explorer/auth.class.php of the component Password-protected Share Handler. Performing a manipulation results in improper authentication. The attack is possible to be carried out remotely. The complexity of an attack is rather high. The exploitability is considered 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.	3.7	More Details
CVE-2026-4363	GitLab has remediated an issue in GitLab EE affecting all versions from 18.1 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1 that under certain conditions could have allowed an authenticated user to gain unauthorized access to resources due to improper caching of authorization decisions.	3.7	More Details
CVE-2026-27860	If auth_username_chars is empty, it is possible to inject arbitrary LDAP filter to Dovecot's LDAP authentication. This leads to potentially bypassing restrictions and allows probing of LDAP structure. Do not clear out auth_username_chars, or install fixed version. No publicly available exploits are known.	3.7	More Details
CVE-2026-4988	A security flaw has been discovered in Open5GS 2.7.6. This issue affects the function smf_gx_cca_cb/smf_gy_cca_cb/smf_s6b of the component CCA Message Handler. The manipulation results in denial of service. The attack may be launched remotely. Attacks of this nature are highly complex. The exploitability is assessed as difficult. The exploit has been released to the public and may be used for attacks.	3.7	More Details
CVE-2026-33490	H3 is a minimal H(TTP) framework. In versions 2.0.0-0 through 2.0.1-rc.16, the `mount()` method in h3 uses a simple `startsWith()` check to determine whether incoming requests fall under a mounted sub-application's path prefix. Because this check does not verify a path segment boundary (i.e., that the next character after the base is `/` or end-of-string), middleware registered on a mount like `/admin` will also execute for unrelated routes such as `/admin-public`, `/administrator`, or `/adminstuff`. This allows an attacker to trigger context-setting middleware on paths it was never intended to cover, potentially polluting request context with unintended privilege flags. Version 2.0.2-rc.17 contains a patch.	3.7	More Details
CVE-2026-4835	A security vulnerability has been detected in code-projects Accounting System 1.0. Impacted is an unknown function of the file /my_account/add_costumer.php of the component Web Application Interface. Such manipulation of the argument costumer_name leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	3.5	More Details
CVE-2026-28527	BlueKitchen BTstack versions prior to 1.8.1 contain an out-of-bounds read vulnerability in the AVRCP Controller GET_PLAYER_APPLICATION_SETTING_ATTRIBUTE_TEXT and GET_PLAYER_APPLICATION_SETTING_VALUE_TEXT handlers that allows nearby attackers to read beyond packet boundaries. Attackers can establish a paired Bluetooth Classic connection and send specially crafted VENDOR_DEPENDENT responses to trigger out-of-bounds reads, causing information disclosure and potential crashes on affected devices.	3.5	More Details
	A vulnerability was found in wandb OpenUI up to 1.0/3.5-turb. Affected is the function generic_exception_handler of the file		

CVE-2026-4994	backend/openui/server.py of the component APIStatusError Handler. The manipulation of the argument key results in information exposure through error message. Access to the local network is required for this attack. 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.	3.5	More Details
CVE-2026-4995	A vulnerability was determined in wandb OpenUI up to 1.0. Affected by this vulnerability is an unknown functionality of the file frontend/public/annotator/index.html of the component Window Message Event Handler. This manipulation causes cross site scripting. 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.	3.5	More Details
CVE-2026-32984	Wazuh authd contains a heap-buffer overflow vulnerability that allows attackers to cause memory corruption and malformed heap data by sending specially crafted input. Attackers can exploit this vulnerability to trigger a denial of service condition, resulting in low availability impact to the authentication daemon.	3.5	More Details
CVE-2026-28526	BlueKitchen BTstack versions prior to 1.8.1 contain an out-of-bounds read vulnerability in the AVRCP Controller LIST_PLAYER_APPLICATION_SETTING_ATTRIBUTES and LIST_PLAYER_APPLICATION_SETTING_VALUES handlers that allows attackers to read beyond buffer boundaries. A nearby attacker with a paired Bluetooth Classic connection can send a specially crafted VENDOR_DEPENDENT response with an attacker-controlled count value to trigger an out-of-bounds read from the L2CAP receive buffer, potentially causing a crash on resource-constrained devices.	3.5	More Details
CVE-2025-55270	HCL Aftermarket DPC is affected by Improper Input Validation which allows an attacker to inject executable code and can carry out attacks such as XSS, SQL Injection, Command Injection etc.	3.5	More Details
CVE-2023-7340	Wazuh authd contains a heap-buffer overflow vulnerability that allows attackers to cause memory corruption and malformed heap data by sending specially crafted input. Attackers can exploit this vulnerability to trigger a denial of service condition, resulting in low availability impact to the authentication daemon.	3.5	More Details
CVE-2026-4973	A vulnerability was detected in SourceCodester Online Quiz System up to 1.0. Affected by this vulnerability is an unknown functionality of the file endpoint/add-question.php. Performing a manipulation of the argument quiz_question results in cross site scripting. It is possible to initiate the attack remotely. The exploit is now public and may be used.	3.5	More Details
CVE-2026-4969	A vulnerability was identified in code-projects Social Networking Site 1.0. The impacted element is an unknown function of the file /home.php of the component Alert Handler. The manipulation of the argument content leads to cross site scripting. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	3.5	More Details
CVE-2026-4991	A vulnerability was detected in QDOCS Smart School Management System up to 7.2. The impacted element is an unknown function of the file /admin/enquiry of the component Admission Enquiry Module. Performing a manipulation of the argument Note results in cross site scripting. The attack is possible to be carried out remotely.	3.5	More Details
CVE-2026-5037	A vulnerability was determined in mxml up to 4.0.4. This issue affects the function index_sort of the file mxml-index.c of the component mxmlIndexNew. Executing a manipulation of the argument tempr can lead to stack-based buffer overflow. The attack is restricted to local execution. The exploit has been publicly disclosed and may be utilized. This patch is called 6e27354466092a1ac65601e01ce6708710bb9fa5. A patch should be applied to remediate this issue.	3.3	More Details
CVE-2026-20684	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26.4. An app may bypass Gatekeeper checks.	3.3	More Details
CVE-2026-33529	Zoraxy is a general purpose HTTP reverse proxy and forwarding tool. Prior to version 3.3.2, an authenticated path traversal vulnerability in the configuration import endpoint allows an authenticated user to write arbitrary files outside the config directory, which can lead to RCE by creating a plugin. Version 3.3.2 patches the issue.	3.3	More Details
CVE-2026-4993	A vulnerability has been found in wandb OpenUI up to 0.0.0.0/1.0. This impacts an unknown function of the file backend/openui/config.py. The manipulation of the argument LITELLM_MASTER_KEY leads to hard-coded credentials. An attack has to be approached locally. 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.	3.3	More Details
CVE-2026-4833	A weakness has been identified in Orc discount up to 3.0.1.2. This issue affects the function compile of the file markdown.c of the component Markdown Handler. This manipulation causes uncontrolled recursion. The attack is restricted to local execution. The exploit has been made available to the public and could be used for attacks. The project maintainer confirms: "[I]f you feed it an infinitely deep blockquote input it will crash. (...) [T]his is a duplicate of an old bug that I've been working on."	3.3	More Details
CVE-2026-28893	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Tahoe 26.4. A document may be written to a temporary file when using print preview.	3.3	More Details
CVE-2026-28864	This issue was addressed with improved permissions checking. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, visionOS 26.4, watchOS 26.4. A local attacker may gain access to user's Keychain items.	3.3	More Details
CVE-2026-2271	A flaw was found in GIMP's PSP (Paint Shop Pro) file parser. A remote attacker could exploit an integer overflow vulnerability in the read_creator_block() function by providing a specially crafted PSP image file. This vulnerability occurs when a 32-bit length value from the file is used for memory allocation without proper validation, leading to a heap overflow and an out-of-bounds write. Successful exploitation could result in an application level denial of service.	3.3	More Details
CVE-2026-4874	A flaw was found in Keycloak. An authenticated attacker can perform Server-Side Request Forgery (SSRF) by manipulating the `client_session_host` parameter during refresh token requests. This occurs when a Keycloak client is configured to use the `backchannel.logout.url` with the `application.session.host` placeholder. Successful exploitation allows the attacker to make HTTP requests from the Keycloak server's network context, potentially probing internal networks or internal APIs, leading to information disclosure.	3.1	More Details
CVE-2026-4958	A vulnerability has been found in OpenBMB XAgent 1.0.0. This affects the function ReplayServer.on_connect/ReplayServer.send_data of the file XAgentServer/application/websockets/replayer.py of the component WebSocket Endpoint. Such manipulation of the argument interaction_id leads to authorization bypass. The attack may be launched remotely. Attacks of this nature are highly complex. The exploitability is reported as difficult. 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.	3.1	More Details
CVE-2026-29071	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to version 0.8.6, any authenticated user can read other users' private memories via `/api/v1/retrieval/query/collection`. Version 0.8.6 patches the issue.	3.1	More Details

CVE-2026-0396	An attacker might be able to inject HTML content into the internal web dashboard by sending crafted DNS queries to a DNSdist instance where domain-based dynamic rules have been enabled via either DynBlockRulesGroup:setSuffixMatchRule or DynBlockRulesGroup:setSuffixMatchRuleFFI.	3.1	More Details
CVE-2025-55276	HCL Aftermarket DPC is affected by Internal IP Disclosure vulnerability will give attackers a clearer map of the organization’s network layout.	3.1	More Details
CVE-2025-14808	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 could allow an attacker to obtain sensitive information from the query string of an HTTP GET method to process a request which could be obtained using man in the middle techniques.	3.1	More Details
CVE-2026-0397	When the internal webserver is enabled (default is disabled), an attacker might be able to trick an administrator logged to the dashboard into visiting a malicious website and extract information about the running configuration from the dashboard. The root cause of the issue is a misconfiguration of the Cross-Origin Resource Sharing (CORS) policy.	3.1	More Details
CVE-2026-32696	NanoMQ MQTT Broker (NanoMQ) is an all-around Edge Messaging Platform. In NanoMQ version 0.24.6, after enabling auth.http_auth (HTTP authentication), when a client connects to the broker using MQTT CONNECT without providing username/password, and the configuration params uses the placeholders %u / %P (e.g., username="%u", password="%P"), the HTTP request construction phase enters auth_http.c:set_data(). This results in calling strlen() on a NULL pointer, causing a SIGSEGV crash. This crash can be triggered remotely, resulting in a denial of service. This issue has been patched in version 0.24.7.	3.1	More Details
CVE-2025-55271	HCL Aftermarket DPC is affected by HTTP Response Splitting vulnerability where in depending on how the web application handles the split response, an attacker may be able to execute arbitrary commands or inject harmful content into the response..	3.1	More Details
CVE-2025-55272	HCL Aftermarket DPC is affected by Banner Disclosure vulnerability where attackers gain insights into the system’s software and version details which would allow them to craft software specific attacks.	3.1	More Details
CVE-2026-33762	go-git is an extensible git implementation library written in pure Go. Prior to version 5.17.1, go-git’s index decoder for format version 4 fails to validate the path name prefix length before applying it to the previously decoded path name. A maliciously crafted index file can trigger an out-of-bounds slice operation, resulting in a runtime panic during normal index parsing. This issue only affects Git index format version 4. Earlier formats (go-git supports only v2 and v3) are not vulnerable to this issue. This issue has been patched in version 5.17.1.	2.8	More Details
CVE-2026-2239	A flaw was found in GIMP. Heap-buffer-overflow vulnerability exists in the fread_pascal_string function when processing a specially crafted PSD (Photoshop Document) file. This occurs because the buffer allocated for a Pascal string is not properly null-terminated, leading to an out-of-bounds read when strlen() is subsequently called. Successfully exploiting this vulnerability can cause the application to crash, resulting in an application level Denial of Service.	2.8	More Details
CVE-2026-3469	A denial-of-service (DoS) vulnerability exists due to improper input validation in the SonicWall Email Security appliance, allowing a remote authenticated attacker as admin user to cause the application to become unresponsive.	2.7	More Details
CVE-2026-4957	A flaw has been found in OpenBMB XAgent 1.0.0. The impacted element is the function FunctionHandler.handle_tool_call of the file XAgent/function_handler.py of the component API Key Handler. This manipulation of the argument api_key causes sensitive information in log files. 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.	2.7	More Details
CVE-2026-34203	Nautobot is a Network Source of Truth and Network Automation Platform. Prior to versions 2.4.30 and 3.0.10, user creation and editing via the REST API fails to apply the password validation rules defined by Django's AUTH_PASSWORD_VALIDATORS setting (which defaults to an empty list, i.e., no specific rules, but can be configured in Nautobot's nautobot_config.py to apply various rules if desired). This can potentially allow for the creation or modification of users to have passwords that are weak or otherwise do not comply with configured standards. This issue has been patched in versions 2.4.30 and 3.0.10.	2.7	More Details
CVE-2025-55277	HCL Aftermarket DPC is affected by Use of Vulnerable/Outdated Versions vulnerability using which an attacker may make use of the exploits available across the internet and craft attacks against the application.	2.6	More Details
CVE-2025-55274	HCL Aftermarket DPC is affected by Cross-Origin Resource Sharing vulnerability. CORS misconfigurations includes the exposure of sensitive user information to attackers, unauthorized access to APIs, and possible data manipulation or leakage. If an attacker to exploit CORS misconfiguration, they could steal sensitive data, perform actions on behalf of a legitimate user.	2.6	More Details
CVE-2026-4823	A flaw has been found in Enter Software Iperius Backup up to 8.7.3. Affected by this vulnerability is an unknown functionality of the component NTLM2 Handler. Executing a manipulation can lead to information disclosure. The attack is restricted to local execution. Attacks of this nature are highly complex. The exploitation appears to be difficult. The exploit has been published and may be used. Upgrading to version 8.7.4 addresses this issue. Upgrading the affected component is advised. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	2.5	More Details
CVE-2026-32970	OpenClaw before 2026.3.11 contains a credential fallback vulnerability where unavailable local gateway.auth.token and gateway.auth.password SecretRefs are treated as unset, allowing fallback to remote credentials in local mode. Attackers can exploit misconfigured local auth references to cause CLI and helper paths to select incorrect credential sources, potentially bypassing intended local authentication boundaries.	2.5	More Details
CVE-2026-4972	A security vulnerability has been detected in code-projects Online Reviewer System up to 1.0. Affected is an unknown function of the file /system/system/students/assessments/databank/btn_functions.php. Such manipulation of the argument Description leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	2.4	More Details
CVE-2026-5106	A flaw has been found in code-projects Exam Form Submission 1.0. The impacted element is an unknown function of the file /admin/update_fst.php. Executing a manipulation of the argument sname can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been published and may be used.	2.4	More Details
CVE-2026-5209	A security vulnerability has been detected in SourceCodester Leave Application System 1.0. Affected by this issue is some unknown functionality of the component User Management Handler. Such manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	2.4	More Details
CVE-	A security flaw has been discovered in code-projects Online Food Ordering System 1.0. Affected by this issue is some unknown functionality of		

2026-4899	the file /dbfood/food.php. The manipulation of the argument cuisines results in cross site scripting. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	2.4	More Details
CVE-2026-4909	A weakness has been identified in code-projects Exam Form Submission 1.0. This impacts an unknown function of the file /admin/update_s7.php. This manipulation of the argument sname causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	2.4	More Details
CVE-2026-3109	Mattermost Plugins versions <=11.4 10.11.11.0 fail to validate webhook request timestamps which allows an attacker to corrupt Zoom meeting state in Mattermost via replayed webhook requests. Mattermost Advisory ID: MMSA-2026-00584	2.2	More Details
CVE-2026-33674	PrestaShop is an open source e-commerce web application. Versions prior to 8.2.5 and 9.1.0 improperly use the validation framework. Versions 8.2.5 and 9.1.0 contain a fix. No known workarounds are available.	2.0	More Details
CVE-2026-33343	etcd is a distributed key-value store for the data of a distributed system. Prior to versions 3.4.42, 3.5.28, and 3.6.9, an authenticated user with RBAC restricted permissions on key ranges can use nested transactions to bypass all key-level authorization. This allows any authenticated user with direct access to etcd to effectively ignore all key range restrictions, accessing the entire etcd data store. Kubernetes does not rely on etcd's built-in authentication and authorization. Instead, the API server handles authentication and authorization itself, so typical Kubernetes deployments are not affected. Versions 3.4.42, 3.5.28, and 3.6.9 contain a patch. If upgrading is not immediately possible, reduce exposure by treating the affected RPCs as unauthenticated in practice. Restrict network access to etcd server ports so only trusted components can connect and require strong client identity at the transport layer, such as mTLS with tightly scoped client certificate distribution.	0.0	More Details
CVE-2026-30892	crun is an open source OCI Container Runtime fully written in C. In versions 1.19 through 1.26, the `crun exec` option `-u` (`--user`) is incorrectly parsed. The value `1` is interpreted as UID 0 and GID 0 when it should have been UID 1 and GID 0. The process thus runs with higher privileges than expected. Version 1.27 patches the issue.	0.0	More Details
CVE-2026-32678	Authentication bypass issue exists in BUFFALO Wi-Fi router products, which may allow an attacker to alter critical configuration settings without authentication.	N/A	More Details
CVE-2026-33890	MyTube is a self-hosted downloader and player for several video websites Prior to version 1.8.71, an unauthenticated attacker can register an arbitrary passkey and subsequently authenticate with it to obtain a full admin session. The application exposes passkey registration endpoints without requiring prior authentication. Any successfully authenticated passkey is automatically granted an administrator token, allowing full administrative access to the application. This enables a complete compromise of the application without requiring any existing credentials. Version 1.8.71 fixes the issue.	N/A	More Details
CVE-2026-3106	Blind Cross-Site Scripting (XSS) in Teampass, versions prior to 3.1.5.16, within the password manager login functionality in the 'contraseña' parameter of the login form 'redacted/index.php'. During failed authentication attempts, the application does not properly clean or encode the information entered by the user in the username field. As a result, arbitrary JavaScript code is automatically executed in the administrator's browser when viewing failed login entries, resulting in a blind XSS condition.	N/A	More Details
CVE-2026-23396	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix NULL deref in mesh_matches_local() mesh_matches_local() unconditionally dereferences ie->mesh_config to compare mesh configuration parameters. When called from mesh_rx_csa_frame(), the parsed action-frame elements may not contain a Mesh Configuration IE, leaving ie->mesh_config NULL and triggering a kernel NULL pointer dereference. The other two callers are already safe: - ieee80211_mesh_rx_bcn_presp() checks !elems->mesh_config before calling mesh_matches_local() - mesh_plink_get_event() is only reached through mesh_process_plink_frame(), which checks !elems->mesh_config, too mesh_rx_csa_frame() is the only caller that passes raw parsed elements to mesh_matches_local() without guarding mesh_config. An adjacent attacker can exploit this by sending a crafted CSA action frame that includes a valid Mesh ID IE but omits the Mesh Configuration IE, crashing the kernel. The captured crash log: Oops: general protection fault, probably for non-canonical address ... KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] Workqueue: events_unbound cfg80211_wiphy_work [...] Call Trace: <TASK> ? __pfx_mesh_matches_local (net/mac80211/mesh.c:65) ieee80211_mesh_rx_queued_mgmt (net/mac80211/mesh.c:1686) [...] ieee80211_iface_work (net/mac80211/iface.c:1754 net/mac80211/iface.c:1802) [...] cfg80211_wiphy_work (net/wireless/core.c:426) process_one_work (net/kernel/workqueue.c:3280) ? assign_work (net/kernel/workqueue.c:1219) worker_thread (net/kernel/workqueue.c:3352) ? __pfx_worker_thread (net/kernel/workqueue.c:3385) kthread (net/kernel/kthread.c:436) [...] ret_from_fork_asm (net/arch/x86/entry/entry_64.S:255) </TASK> This patch adds a NULL check for ie->mesh_config at the top of mesh_matches_local() to return false early when the Mesh Configuration IE is absent.	N/A	More Details
CVE-2026-23279	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix NULL pointer dereference in mesh_rx_csa_frame() In mesh_rx_csa_frame(), elems->mesh_chansw_params_ie is dereferenced at lines 1638 and 1642 without a prior NULL check: ifmsh->chsw_ttl = elems->mesh_chansw_params_ie->mesh_ttl; ... pre_value = le16_to_cpu(elems->mesh_chansw_params_ie->mesh_pre_value); The mesh_matches_local() check above only validates the Mesh ID, Mesh Configuration, and Supported Rates IEs. It does not verify the presence of the Mesh Channel Switch Parameters IE (element ID 118). When a received CSA action frame omits that IE, ieee802_11_parse_elems() leaves elems->mesh_chansw_params_ie as NULL, and the unconditional dereference causes a kernel NULL pointer dereference. A remote mesh peer with an established peer link (PLINK_ESTAB) can trigger this by sending a crafted SPECTRUM_MGMT/CHL_SWITCH action frame that includes a matching Mesh ID and Mesh Configuration IE but omits the Mesh Channel Switch Parameters IE. No authentication beyond the default open mesh peering is required. Crash confirmed on kernel 6.17.0-5-generic via mac80211_hwsim: BUG: kernel NULL pointer dereference, address: 0000000000000000 Oops: Oops: 0000 [#1] SMP NOPTI RIP: 0010:ieee80211_mesh_rx_queued_mgmt+0x143/0x2a0 [mac80211] CR2: 0000000000000000 Fix by adding a NULL check for mesh_chansw_params_ie after mesh_matches_local() returns, consistent with how other optional IEs are guarded throughout the mesh code. The bug has been present since v3.13 (released 2014-01-19).	N/A	More Details
CVE-2026-33559	WordPress Plugin "OpenStreetMap" provided by MiKa contains a cross-site scripting vulnerability. On the site with the affected version of the plugin enabled, a logged-in user with a page-creating/editing privilege can embed some malicious script with a crafted HTTP request. When a victim user accesses this page, the script may be executed in the user's web browser.	N/A	More Details
CVE-2026-32326	SHARP routers do not perform authentication for some web APIs. The device information may be retrieved without authentication. If the administrative password of the device is left as the initial one, the device may be taken over.	N/A	More Details
CVE-2025-41357	Reflected Cross-Site Scripting (XSS) vulnerability in Anon Proxy Server v0.104. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by sending him/her a malicious URL. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user. It affects 'host' parameter in '/diagdns.php' endpoint.	N/A	More Details
CVE-2025-14213	Cato Networks' Socket versions prior to 25 contain a command injection vulnerability that allows an authenticated attacker with access to the Socket web interface (UI) to execute arbitrary operating system commands as the root user on the Socket's internal system.	N/A	More Details

CVE-2026-26306	The installer for OM Workspace (Windows Edition) Ver 2.4 and earlier insecurely loads Dynamic Link Libraries (DLLs), which could allow an attacker to execute arbitrary code with the privileges of the user invoking the installer.	N/A	More Details
CVE-2026-34172	Giskard is an open-source Python library for testing and evaluating agentic systems. Prior to versions 0.3.4 and 1.0.2b1, ChatWorkflow.chat(message) passes its string argument directly as a Jinja2 template source to a non-sandboxed Environment. A developer who passes user input to this method enables full remote code execution via Jinja2 class traversal. The method name chat and parameter name message naturally invite passing user input directly, but the string is silently parsed as a Jinja2 template, not treated as plain text. This issue has been patched in versions 0.3.4 and 1.0.2b1.	N/A	More Details
CVE-2026-34200	Nhost is an open source Firebase alternative with GraphQL. Prior to version 1.41.0, The Nhost CLI MCP server, when explicitly configured to listen on a network port, applies no inbound authentication and does not enforce strict CORS. This allows a malicious website visited on the same machine to issue cross-origin requests to the MCP server and invoke privileged tools using the developer's locally configured credentials. This vulnerability requires two explicit, non-default configuration steps to be exploitable. The default nhost mcp start configuration is not affected. This issue has been patched in version 1.41.0.	N/A	More Details
CVE-2026-33253	SANUPS SOFTWARE provided by SANYO DENKI CO., LTD. registers Windows services with unquoted file paths. A user with the write permission on the root directory of the system drive may execute arbitrary code with SYSTEM privilege.	N/A	More Details
CVE-2026-34202	ZEBRA is a Zcash node written entirely in Rust. Prior to zebrad version 4.3.0 and zebra-chain version 6.0.1, a vulnerability in Zebra's transaction processing logic allows a remote, unauthenticated attacker to cause a Zebra node to panic (crash). This is triggered by sending a specially crafted V5 transaction that passes initial deserialization but fails during transaction ID calculation. This issue has been patched in zebrad version 4.3.0 and zebra-chain version 6.0.1.	N/A	More Details
CVE-2025-41356	Reflected Cross-Site Scripting (XSS) vulnerability in Anon Proxy Server v0.104. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by sending him/her a malicious URL. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user. It affects 'host' parameter in '/diagconnect.php' endpoint.	N/A	More Details
CVE-2026-34210	mppx is a TypeScript interface for machine payments protocol. Prior to version 0.4.11, the stripe/charge payment method did not check Stripe's Idempotent-Replayed response header when creating PaymentIntents. An attacker could replay a valid credential containing the same spt token against a new challenge, and the server would accept the replayed Stripe PaymentIntent as a new successful payment without actually charging the customer again. This allowed an attacker to pay once and consume unlimited resources by replaying the credential. This issue has been patched in version 0.4.11.	N/A	More Details
CVE-2026-33366	Missing authentication for critical function vulnerability in BUFFALO Wi-Fi router products may allow an attacker to forcibly reboot the product without authentication.	N/A	More Details
CVE-2026-23397	In the Linux kernel, the following vulnerability has been resolved: nfnetlink_osf: validate individual option lengths in fingerprints nfnl_osf_add_callback() validates opt_num bounds and string NUL-termination but does not check individual option length fields. A zero-length option causes nf_osf_match_one() to enter the option matching loop even when foptsize sums to zero, which matches packets with no TCP options where ctx->optp is NULL: Oops: general protection fault KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] RIP: 0010:nf_osf_match_one (net/netfilter/nfnetlink_osf.c:98) Call Trace: nf_osf_match (net/netfilter/nfnetlink_osf.c:227) xt_osf_match_packet (net/netfilter/xt_osf.c:32) ipt_do_table (net/ipv4/netfilter/ip_tables.c:293) nf_hook_slow (net/netfilter/core.c:623) ip_local_deliver (net/ipv4/ip_input.c:262) ip_rcv (net/ipv4/ip_input.c:573) Additionally, an MSS option (kind=2) with length < 4 causes out-of-bounds reads when nf_osf_match_one() unconditionally accesses optp[2] and optp[3] for MSS value extraction. While RFC 9293 section 3.2 specifies that the MSS option is always exactly 4 bytes (Kind=2, Length=4), the check uses "< 4" rather than "!= 4" because lengths greater than 4 do not cause memory safety issues -- the buffer is guaranteed to be at least foptsize bytes by the ctx->optsize == foptsize check. Reject fingerprints where any option has zero length, or where an MSS option has length less than 4, at add time rather than trusting these values in the packet matching hot path.	N/A	More Details
CVE-2026-23283	In the Linux kernel, the following vulnerability has been resolved: regulator: fp9931: Fix PM runtime reference leak in fp9931_hwmon_read() In fp9931_hwmon_read(), if regmap_read() failed, the function returned the error code without calling pm_runtime_put_autosuspend(), causing a PM reference leak.	N/A	More Details
CVE-2026-23280	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Prevent ubuf size overflow The ubuf size calculation may overflow, resulting in an undersized allocation and possible memory corruption. Use check_add_overflow() helpers to validate the size calculation before allocation.	N/A	More Details
CVE-2026-4399	Prompt injection vulnerability in 1millionbot Millie chatbot that occurs when a user manages to evade chat restrictions using Boolean prompt injection techniques (formulating a question in such a way that, upon receiving an affirmative response ('true'), the model executes the injected instruction), causing it to return prohibited information and information outside its intended context. Successful exploitation of this vulnerability could allow a malicious remote attacker to abuse the service for purposes other than those originally intended, or even execute out-of-context tasks using 1millionbot's resources and/or OpenAI's API key. This allows the attacker to evade the containment mechanisms implemented during LLM model training and obtain responses or chat behaviors that were originally restricted.	N/A	More Details
CVE-2026-0596	A command injection vulnerability exists in mlflow/mlflow when serving a model with `enable_mlserver=True`. The `model_uri` is embedded directly into a shell command executed via `bash -c` without proper sanitization. If the `model_uri` contains shell metacharacters, such as `$()` or backticks, it allows for command substitution and execution of attacker-controlled commands. This vulnerability affects the latest version of mlflow/mlflow and can lead to privilege escalation if a higher-privileged service serves models from a directory writable by lower-privileged users.	N/A	More Details
CVE-2026-3308	An integer overflow vulnerability in 'pdf-image.c' in Artifex's MuPDF version 1.27.0 allows an attacker to maliciously craft a PDF that can trigger an integer overflow within the 'pdf_load_image_imp' function. This allows a heap out-of-bounds write that could be exploited for arbitrary code execution.	N/A	More Details
CVE-2026-34155	RAUC controls the update process on embedded Linux systems. Prior to version 1.15.2, RAUC bundles using the 'plain' format exceeding a payload size of 2 GiB cause an integer overflow which results in a signature which covers only the first few bytes of the payload. Given such a bundle with a legitimate signature, an attacker can modify the part of the payload which is not covered by the signature. This issue has been patched in version 1.15.2.	N/A	More Details
CVE-2026-23282	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix oops due to uninitialised var in smb2_unlink() If SMB2_open_init() or SMB2_close_init() fails (e.g. reconnect), the iovs set @rqst will be left uninitialised, hence calling SMB2_open_free(), SMB2_close_free() or smb2_set_related() on them will oops. Fix this by initialising @close_iov and @open_iov before setting them in @rqst.	N/A	More Details
	In its design for automatic terminal command execution, Sixth offers two options: Execute safe commands and Execute all commands. The		

CVE-2026-30310	description for the former states that commands determined by the model to be safe will be automatically executed, whereas if the model judges a command to be potentially destructive, it still requires user approval. However, this design is highly susceptible to prompt injection attacks. An attacker can employ a generic template to wrap any malicious command and mislead the model into misclassifying it as a 'safe' command, thereby bypassing the user approval requirement and resulting in arbitrary command execution.	N/A	More Details
CVE-2026-33935	MyTube is a self-hosted downloader and player for several video websites Prior to version 1.8.72, an unauthenticated attacker can lock out administrator and visitor accounts from password-based authentication by triggering failed login attempts. The application exposes three password verification endpoints, all of which are publicly accessible. All three endpoints share a single file-backed login attempt state stored in `login-attempts.json`. When any endpoint records a failed authentication attempt via `recordFailedAttempt()`, the shared login attempt state is updated, increasing the `failedAttempts` counter and adjusting the associated timestamps and cooldown values. Before verifying a password, each endpoint calls `canAttemptLogin()`. This function checks the shared JSON file to determine whether a cooldown period is active. If the cooldown has not expired, the request is rejected before the password is validated. Because the failed attempt counter and cooldown timer are globally shared, failed authentication attempts against any endpoint affect all other endpoints. An attacker can exploit this by repeatedly sending invalid authentication requests to any of these endpoints, incrementing the shared counter and waiting for the cooldown period between attempts. By doing so, the attacker can progressively increase the lockout duration until it reaches 24 hours, effectively preventing legitimate users from authenticating. Once the maximum lockout is reached, the attacker can maintain the denial of service indefinitely by waiting for the cooldown to expire and sending another failed attempt, which immediately triggers another 24-hour lockout if no successful login occurred in the meantime. Version 1.8.72 fixes the vulnerability.	N/A	More Details
CVE-2026-30311	Ridvay Code's command auto-approval module contains a critical OS command injection vulnerability that renders its whitelist security mechanism completely ineffective. The system relies on fragile regular expressions to parse command structures; while it attempts to intercept dangerous operations, it fails to account for standard Shell command substitution Ridvay Code (specifically$(...)and backticks ...). An attacker can construct a command such as git log --grep="$(malicious_command)", forcing Syntx to misidentify it as a safe git operation and automatically approve it. The underlying Shell prioritizes the execution of the malicious code injected within the arguments, resulting in Remote Code Execution without any user interaction.	N/A	More Details
CVE-2026-23284	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: mtk_eth_soc: Reset prog ptr to old_prog in case of error in mtk_xdp_setup() Reset eBPF program pointer to old_prog and do not decrease its ref-count if mtk_open routine in mtk_xdp_setup() fails.	N/A	More Details
CVE-2026-30312	DSAI-Cline's command auto-approval module contains a critical OS command injection vulnerability that renders its whitelist security mechanism completely ineffective. The system relies on string-based parsing to validate commands; while it intercepts dangerous operators such as ;, &&, ||, |, and command substitution patterns, it fails to account for raw newline characters embedded within the input. An attacker can construct a payload by embedding a literal newline between a whitelisted command and malicious code (e.g., git log malicious_command), forcing DSAI-Cline to misidentify it as a safe operation and automatically approve it. The underlying PowerShell interpreter treats the newline as a command separator, executing both commands sequentially, resulting in Remote Code Execution without any user interaction.	N/A	More Details
CVE-2026-20915	Stored cross-site scripting (XSS) in Checkmk version 2.5.0 (beta) before 2.5.0b2 allows authenticated users with permission to create pending changes to inject malicious JavaScript into the Pending Changes sidebar, which will execute in the browsers of other users viewing the sidebar.	N/A	More Details
CVE-2026-23285	In the Linux kernel, the following vulnerability has been resolved: drbd: fix null-pointer dereference on local read error In drbd_request_endio(), READ_COMPLETED_WITH_ERROR is passed to __req_mod() with a NULL peer_device: __req_mod(req, what, NULL, &m); The READ_COMPLETED_WITH_ERROR handler then unconditionally passes this NULL peer_device to drbd_set_out_of_sync(), which dereferences it, causing a null-pointer dereference. Fix this by obtaining the peer_device via first_peer_device(device), matching how drbd_req_destroy() handles the same situation.	N/A	More Details
CVE-2026-4400	Insecure Direct Object Reference (IDOR) vulnerability in 1millionbot Millie chat that allows private conversations of other users being viewed by simply changing the conversation ID. The vulnerability is present in the endpoint 'api.1millionbot.com/api/public/conversations/' and, if exploited, could allow a remote attacker to access other users private chatbot conversations, revealing sensitive or confidential data without requiring credentials or impersonating users. In order for the vulnerability to be exploited, the attacker must have the user's conversation ID.	N/A	More Details
CVE-2026-30314	Ridvay Code's command auto-approval module contains a critical OS command injection vulnerability that renders its whitelist security mechanism completely ineffective. The system relies on fragile regular expressions to parse command structures; while it attempts to intercept dangerous operations, it fails to account for standard Shell command substitution Ridvay Code (specifically$(...)and backticks ...). An attacker can construct a command such as git log --grep="$(malicious_command)", forcing Syntx to misidentify it as a safe git operation and automatically approve it. The underlying Shell prioritizes the execution of the malicious code injected within the arguments, resulting in Remote Code Execution without any user interaction.	N/A	More Details
CVE-2026-23281	In the Linux kernel, the following vulnerability has been resolved: wifi: libertas: fix use-after-free in lbs_free_adapter() The lbs_free_adapter() function uses timer_delete() (non-synchronous) for both command_timer and tx_lockup_timer before the structure is freed. This is incorrect because timer_delete() does not wait for any running timer callback to complete. If a timer callback is executing when lbs_free_adapter() is called, the callback will access freed memory since lbs_cfg_free() frees the containing structure immediately after lbs_free_adapter() returns. Both timer callbacks (lbs_cmd_timeout_handler and lbs_tx_lockup_handler) access priv->driver_lock, priv->cur_cmd, priv->dev, and other fields, which would all be use-after-free violations. Use timer_delete_sync() instead to ensure any running timer callback has completed before returning. This bug was introduced in commit 8f641d93c38a ("libertas: detect TX lockups and reset hardware") where del_timer() was used instead of del_timer_sync() in the cleanup path. The command_timer has had the same issue since the driver was first written.	N/A	More Details
CVE-2026-23286	In the Linux kernel, the following vulnerability has been resolved: atm: lec: fix null-ptr-deref in lec_arp_clear_vccs syzkaller reported a null-ptr-deref in lec_arp_clear_vccs(). This issue can be easily reproduced using the syzkaller reproducer. In the ATM LANE (LAN Emulation) module, the same atm_vcc can be shared by multiple lec_arp_table entries (e.g., via entry->vcc or entry->recv_vcc). When the underlying VCC is closed, lec_vcc_close() iterates over all ARP entries and calls lec_arp_clear_vccs() for each matched entry. For example, when lec_vcc_close() iterates through the hlists in priv->lec_arp_empty_ones or other ARP tables: 1. In the first iteration, for the first matched ARP entry sharing the VCC, lec_arp_clear_vccs() frees the associated vpriv (which is vcc->user_back) and sets vcc->user_back to NULL. 2. In the second iteration, for the next matched ARP entry sharing the same VCC, lec_arp_clear_vccs() is called again. It obtains a NULL vpriv from vcc->user_back (via LEC_VCC_PRIV(vcc)) and then attempts to dereference it via `vcc->pop = vpriv->old_pop`, leading to a null-ptr-deref crash. Fix this by adding a null check for vpriv before dereferencing it. If vpriv is already NULL, it means the VCC has been cleared by a previous call, so we can safely skip the cleanup and just clear the entry's vcc/recv_vcc pointers. The entire cleanup block (including vcc_release_async()) is placed inside the vpriv guard because a NULL vpriv indicates the VCC has already been fully released by a prior iteration — repeating the teardown would redundantly set flags and trigger callbacks on an already-closing socket. The Fixes tag points to the initial commit because the entry->vcc path has been vulnerable since the original code. The entry->recv_vcc path was later added by commit 8d9f73c0ad2f ("atm: fix a memory leak of vcc->user_back") with the same pattern, and both paths are fixed here.	N/A	More Details
CVE-2026-	Stored Cross-Site Scripting (XSS) in Teampass versions prior to 3.1.5.16, affecting the password manager's password import functionality at the endpoint 'redacted/index.php?page=items'. The application fails to properly sanitize and encode user-input data during the import process, allowing malicious JavaScript payloads to be persistently stored in the database. When other users view the imported passwords, the payload is	N/A	More

3107	automatically executed in their browsers, resulting in a stored XSS condition at the endpoint 'redacted/index.php?page=items'. Exploiting this vulnerability allows an attacker to execute arbitrary JavaScript code in the context of multiple users and the administrator, which can lead to session hijacking, credential theft, privilege abuse, and compromise of application integrity.		Details
CVE-2026-23398	In the Linux kernel, the following vulnerability has been resolved: icmp: fix NULL pointer dereference in icmp_tag_validation() icmp_tag_validation() unconditionally dereferences the result of rcu_dereference(inet_protos[proto]) without checking for NULL. The inet_protos[] array is sparse -- only about 15 of 256 protocol numbers have registered handlers. When ip_no_pmtu_disc is set to 3 (hardened PMTU mode) and the kernel receives an ICMP Fragmentation Needed error with a quoted inner IP header containing an unregistered protocol number, the NULL dereference causes a kernel panic in softirq context. Oops: general protection fault, probably for non-canonical address 0xdffffc0000000002: 0000 [#1] SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] RIP: 0010:icmp_unreach (net/ipv4/icmp.c:1085 net/ipv4/icmp.c:1143) Call Trace: <IRQ> icmp_rcv (net/ipv4/icmp.c:1527) ip_protocol_deliver_rcu (net/ipv4/ip_input.c:207) ip_local_deliver_finish (net/ipv4/ip_input.c:242) ip_local_deliver (net/ipv4/ip_input.c:262) ip_rcv (net/ipv4/ip_input.c:573) __netif_receive_skb_one_core (net/core/dev.c:6164) process_backlog (net/core/dev.c:6628) handle_softirqs (kernel/softirq.c:561) </IRQ> Add a NULL check before accessing icmp_strict_tag_validation. If the protocol has no registered handler, return false since it cannot perform strict tag validation.	N/A	More Details
CVE-2026-33276	Stored cross-site scripting (XSS) in Checkmk 2.5.0 (beta) before 2.5.0b2 allows authenticated users with permission to create hosts or services to execute arbitrary JavaScript in the browsers of other users performing searches in the Unified Search feature.	N/A	More Details
CVE-2026-4317	SQL inyection (SQLi) vulnerability in Umami Software web application through an improperly sanitized parameter, which could allow an authenticated attacker to execute arbitrary SQL commands in the database.Specifically, they could manipulate the value of the 'timezone' request parameter by including malicious characters and SQL payload. The application would interpolate these values directly into the SQL query without first performing proper filtering or sanitization (e.g., using functions such as 'prisma.rawQuery', 'prisma.$queryRawUnsafe' or raw queries with 'ClickHouse'). The successful explotation of this vulnerability could allow an authenticated attacker to compromiso the data of the database and execute dangerous functions.	N/A	More Details
CVE-2026-33881	Windmill is an open-source developer platform for internal code: APIs, background jobs, workflows and UIs. Workspace environment variable values are interpolated into JavaScript string literals without escaping single quotes in the NativeTS executor. A workspace admin who sets a custom environment variable with a value containing `'` can inject arbitrary JavaScript that executes inside every NativeTS script in that workspace. This is a code injection bug in `worker.rs`, not related to the sandbox/NSJAIL topic. Version 1.664.0 patches the issue.	N/A	More Details
CVE-2026-34224	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.64 and 9.7.0-alpha.8, an attacker who possesses a valid authentication provider token and a single MFA recovery code or SMS one-time password can create multiple authenticated sessions by sending concurrent login requests via the authData login endpoint. This defeats the single-use guarantee of MFA recovery codes and SMS one-time passwords, allowing session persistence even after the legitimate user revokes detected sessions. This issue has been patched in versions 8.6.64 and 9.7.0-alpha.8.	N/A	More Details
CVE-2026-34400	Alerta is a monitoring tool. Prior to version 9.1.0, the Query string search API (q=) was vulnerable to SQL injection via the Postgres query parser, which built WHERE clauses by interpolating user-supplied search terms directly into SQL strings via f-strings. This issue has been patched in version 9.1.0.	N/A	More Details
CVE-2026-0748	In the Drupal 7 Internationalization (i18n) module, the i18n_node submodule allows a user with both "Translate content" and "Administer content translations" permissions to view and attach unpublished nodes via the translation UI and its autocomplete widget. This bypasses intended access controls and discloses unpublished node titles and IDs. Exploit affects versions 7.x-1.0 up to and including 7.x-1.35.	N/A	More Details
CVE-2026-1556	Information disclosure in the file URI processing of File (Field) Paths in Drupal File (Field) Paths 7.x prior to 7.1.3 on Drupal 7.x allows authenticated users to disclose other users' private files via filename-collision uploads. This can cause hook_node_insert() consumers (for example, email attachment modules) to receive the wrong file URI, bypassing normal access controls on private files.	N/A	More Details
CVE-2026-34372	Sulu is an open-source PHP content management system based on the Symfony framework. From versions 1.0.0 to before 2.6.22, and 3.0.0 to before 3.0.5, a user which has permission for the Sulu Admin via at least one role could have access to the sub-entities of contacts via the admin API without even have permission for contacts. This issue has been patched in versions 2.6.22 and 3.0.5.	N/A	More Details
CVE-2026-33658	Active Storage allows users to attach cloud and local files in Rails applications. Prior to versions 8.1.2.1, 8.0.4.1, and 7.2.3.1 Active Storage's proxy controller does not limit the number of byte ranges in an HTTP Range header. A request with thousands of small ranges causes disproportionate CPU usage compared to a normal request for the same file, possibly resulting in a DoS vulnerability. Versions 8.1.2.1, 8.0.4.1, and 7.2.3.1 contain a patch.	N/A	More Details
CVE-2026-34784	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.71 and 9.7.1-alpha.1, file downloads via HTTP Range requests bypass the afterFind(Parse.File) trigger and its validators on storage adapters that support streaming (e.g. the default GridFS adapter). This allows access to files that should be protected by afterFind trigger authorization logic or built-in validators such as requireUser. This issue has been patched in versions 8.6.71 and 9.7.1-alpha.1.	N/A	More Details
CVE-2026-34215	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.63 and 9.7.0-alpha.7, the verify password endpoint returns unsanitized authentication data, including MFA TOTP secrets, recovery codes, and OAuth access tokens. An attacker who knows a user's password can extract the MFA secret to generate valid MFA codes, defeating multi-factor authentication protection. This issue has been patched in versions 8.6.63 and 9.7.0-alpha.7.	N/A	More Details
CVE-2026-34204	MinIO is a high-performance object storage system. Prior to version RELEASE.2026-03-26T21-24-40Z, a flaw in extractMetadataFromMime() allows any authenticated user with s3:PutObject permission to inject internal server-side encryption metadata into objects by sending crafted X-Minio-Replication-* headers on a normal PutObject request. This issue has been patched in version RELEASE.2026-03-26T21-24-40Z.	N/A	More Details
CVE-2026-30290	An arbitrary file overwrite vulnerability in InTouch Contacts & Caller ID APP v6.38.1 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.	N/A	More Details
CVE-2026-30285	An arbitrary file overwrite vulnerability in Zora: Post, Trade, Earn Crypto v2.60.0 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.	N/A	More Details
CVE-2026-30280	An arbitrary file overwrite vulnerability in RAREPROB SOLUTIONS PRIVATE LIMITED Video player Play All Videos v1.0.135 allows attackers to overwrite critical internal files via the file import process, leading to arbtrary code execution or information exposure.	N/A	More Details
CVE-2026-	The MS27102A Remote Spectrum Monitor is vulnerable to an authentication bypass that allows unauthorized users to access and manipulate its management interface. Because the device provides no mechanism to enable or configure authentication, the issue is inherent to its design	N/A	More Details

3356	rather than a deployment error.		
CVE-2026-30521	A Business Logic vulnerability exists in SourceCodester Loan Management System v1.0 due to improper server-side validation. The application allows administrators to create "Loan Plans" with specific interest rates. While the frontend interface prevents users from entering negative numbers, this constraint is not enforced on the backend. An authenticated attacker can bypass the client-side restriction by manipulating the HTTP POST request to submit a negative value for the interest_percentage. This results in the creation of loan plans with negative interest rates.	N/A	More Details
CVE-2026-33415	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, an authenticated moderator-level user could retrieve post content, topic titles, and usernames from categories they were not authorized to view. Insufficient access controls on a sentiment analytics endpoint allowed category permission boundaries to be bypassed. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.	N/A	More Details
CVE-2026-33300	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, an authorization bypass in the Category Chatables Controller show action allowed moderators to get information on hidden groups names and user count. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.	N/A	More Details
CVE-2026-33185	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, the group email settings test endpoint could be used to make the server initiate outbound connections to arbitrary hosts and ports. This could allow probing of internal network infrastructure. The endpoint was accessible to non-staff group owners. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.	N/A	More Details
CVE-2026-33397	The Angular SSR is a server-rise rendering tool for Angular applications. Versions on the 22.x branch prior to 22.0.0-next.2, the 21.x branch prior to 21.2.3, and the 20.x branch prior to 20.3.21 have an Open Redirect vulnerability in `@angular/ssr` due to an incomplete fix for CVE-2026-27738. While the original fix successfully blocked multiple leading slashes (e.g., `///`), the internal validation logic fails to account for a single backslash (`\`) bypass. When an Angular SSR application is deployed behind a proxy that passes the `X-Forwarded-Prefix` header, an attacker provides a value starting with a single backslash, the internal validation failed to flag the single backslash as invalid, the application prepends a leading forward slash, resulting in a `Location` header containing the URL, and modern browsers interpret the `/\` sequence as `//`, treating it as a protocol-relative URL and redirecting the user to the attacker-controlled domain. Furthermore, the response lacks the `Vary: X-Forwarded-Prefix` header, allowing the malicious redirect to be stored in intermediate caches (Web Cache Poisoning). Versions 22.0.0-next.2, 21.2.3, and 20.3.21 contain a patch. Until the patch is applied, developers should sanitize the `X-Forwarded-Prefix` header in their `server.ts` before the Angular engine processes the request.	N/A	More Details
CVE-2026-34404	Nuxt OG Image generates OG Images with Vue templates in Nuxt. Prior to version 6.2.5, the image-generation component by the URI: /_og/d/ (and, in older versions, /og-image/) contains a Denial of Service (DoS) vulnerability. The issue arises because there is no restriction on the width and height parameters of the generated image. The vulnerability was reproduced using the standard configuration and the default templates. This issue has been patched in version 6.2.5.	N/A	More Details
CVE-2026-33073	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, the discourse-subscriptions plugin leaks stripe API keys across sites in a multisite cluster resulting in the potential for stripe related information to be leaked across sites within the same multisite cluster. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.	N/A	More Details
CVE-2026-34406	APTRS (Automated Penetration Testing Reporting System) is a Python and Django-based automated reporting tool designed for penetration testers and security organizations. Prior to version 2.0.1, the edit_user endpoint (POST /api/auth/edituser/<pk>) allows Any user who can reach that endpoint and submit crafted permission to escalate their own account (or any other account) to superuser by including "is_superuser": true in the request body. The root cause is that CustomUserSerializer explicitly includes is_superuser in its fields list but omits it from read_only_fields, making it a writable field. The edit_user view performs no additional validation to prevent non-superusers from modifying this field. Once is_superuser is set to true, gaining unrestricted access to all application functionality without requiring re-authentication. This issue has been patched in version 2.0.1.	N/A	More Details
CVE-2026-26213	thingino-firmware versions up to the firmware-2026-03-16 release contains an unauthenticated os command injection vulnerability in the WiFi captive portal CGI script that allows remote attackers to execute arbitrary commands as root by injecting malicious code through unsanitized HTTP parameter names. Attackers can exploit the eval function in parse_query() and parse_post() functions to achieve remote code execution and perform privileged configuration changes including root password reset and SSH authorized_keys modification, resulting in full persistent device compromise.	N/A	More Details
CVE-2026-33525	Authelia is an open-source authentication and authorization server providing two-factor authentication and single sign-on (SSO) for applications via a web portal. In version 4.39.15, an attacker may potentially be able to inject javascript into the Authelia login page if several conditions are met simultaneously. Unless both the `script-src` and `connect-src` directives have been modified it's almost impossible for this to have a meaningful impact. However if both of these are and they are done so without consideration to their potential impact; there is a are situations where this vulnerability could be exploited. This is caused to the lack of neutralization of the `langauge` cookie value when rendering the HTML template. This vulnerability is likely difficult to discover though fingerprinting due to the way Authelia is designed but it should not be considered impossible. The additional requirement to identify the secondary application is however likely to be significantly harder to identify along side this, but also likely easier to fingerprint. Users should upgrade to 4.39.16 or downgrade to 4.39.14 to mitigate the issue. The overwhelming majority of installations will not be affected and no workarounds are necessary. The default value for the Content Security Policy makes exploiting this weakness completely impossible. It's only possible via the deliberate removal of the Content Security Policy or deliberate inclusion of clearly noted unsafe policies.	N/A	More Details
CVE-2026-33531	InvenTree is an Open Source Inventory Management System. Prior to version 1.2.6, a path traversal vulnerability in the report template engine allows a staff-level user to read arbitrary files from the server filesystem via crafted template tags. Affected functions: `encode_svg_image()`, `asset()`, and `uploaded_image()` in `src/backend/InvenTree/report/templatetags/report.py`. This requires staff access (to upload / edit templates with maliciously crafted tags). If the InvenTree installation is configured with high access privileges on the host system, this path traversal may allow file access outside of the InvenTree source directory. This issue is patched in version 1.2.6, and 1.3.0 (or above). Users should update to the patched versions. No known workarounds are available.	N/A	More Details
CVE-2026-34605	SiYuan is a personal knowledge management system. From version 3.6.0 to before version 3.6.2, the SanitizeSVG function introduced in version 3.6.0 to fix XSS in the unauthenticated /api/icon/getDynamicIcon endpoint can be bypassed by using namespace-prefixed element names such as <x:script xmlns:x="http://www.w3.org/2000/svg">. The Go HTML5 parser records the element's tag as "x:script" rather than "script", so the tag check passes it through. The SVG is served with Content-Type: image/svg+xml and no Content Security Policy; when a browser opens the response directly, its XML parser resolves the prefix to the SVG namespace and executes the embedded script. This issue has been patched in version 3.6.2.	N/A	More Details
CVE-2026-33632	ClearanceKit intercepts file-system access events on macOS and enforces per-process access policies. Prior to version 4.2.4, two file operation event types — ES_EVENT_TYPE_AUTH_EXCHANGEDATA and ES_EVENT_TYPE_AUTH_CLONE — were not intercepted by ClearanceKit's opfilter system extension, allowing local processes to bypass file access policies. Commit 6181c4a patches the vulnerability by subscribing to both event types and routing them through the existing policy evaluator. Users must upgrade to v4.2.4 or later and reactivate the system extension.	N/A	More Details

CVE-2026-0964	A malicious SCP server can send unexpected paths that could make the client application override local files outside of working directory. This could be misused to create malicious executable or configuration files and make the user execute them under specific consequences. This is the same issue as in OpenSSH, tracked as CVE-2019-6111.	N/A	More Details
CVE-2026-0965	A flaw was found in libssh where it can attempt to open arbitrary files during configuration parsing. A local attacker can exploit this by providing a malicious configuration file or when the system is misconfigured. This vulnerability could lead to a Denial of Service (DoS) by causing the system to try and access dangerous files, such as block devices or large system files, which can disrupt normal operations.	N/A	More Details
CVE-2026-0966	The API function `ssh_get_hexa()` is vulnerable, when 0-lenght input is provided to this function. This function is used internally in `ssh_get_fingerprint_hash()` and `ssh_print_hexa()` (deprecated), which is vulnerable to the same input (length is provided by the calling application). The function is also used internally in the gssapi code for logging the OIDs received by the server during GSSAPI authentication. This could be triggered remotely, when the server allows GSSAPI authentication and logging verbosity is set at least to SSH_LOG_PACKET (3). This could cause self-DoS of the per-connection daemon process.	N/A	More Details
CVE-2026-0967	A flaw was found in libssh. A remote attacker, by controlling client configuration files or known_hosts files, could craft specific hostnames that when processed by the `match_pattern()` function can lead to inefficient regular expression backtracking. This can cause timeouts and resource exhaustion, resulting in a Denial of Service (DoS) for the client.	N/A	More Details
CVE-2026-0968	A flaw was found in libssh in which a malicious SFTP (SSH File Transfer Protocol) server can exploit this by sending a malformed 'longname' field within an `SSH_FXP_NAME` message during a file listing operation. This missing null check can lead to reading beyond allocated memory on the heap. This can cause unexpected behavior or lead to a denial of service (DoS) due to application crashes.	N/A	More Details
CVE-2026-33537	Lychee is a free, open-source photo-management tool. The patch introduced for GHSA-cpgw-wgf3-xc6v (SSRF via `Photo::fromUrl`) contains an incomplete IP validation check that fails to block loopback addresses and link-local addresses. Prior to version 7.5.1, an authenticated user can still reach internal services using direct IP addresses, bypassing all four protection configuration settings even when they are set to their secure defaults. Version 7.5.1 contains a fix for the issue.	N/A	More Details
CVE-2026-34452	The Claude SDK for Python provides access to the Claude API from Python applications. From version 0.86.0 to before version 0.87.0, the async local filesystem memory tool in the Anthropic Python SDK validated that model-supplied paths resolved inside the sandboxed memory directory, but then returned the unresolved path for subsequent file operations. A local attacker able to write to the memory directory could retarget a symlink between validation and use, causing reads or writes to escape the sandbox. The synchronous memory tool implementation was not affected. This issue has been patched in version 0.87.0.	N/A	More Details
CVE-2026-34451	Claude SDK for TypeScript provides access to the Claude API from server-side TypeScript or JavaScript applications. From version 0.79.0 to before version 0.81.0, the local filesystem memory tool in the Anthropic TypeScript SDK validated model-supplied paths using a string prefix check that did not append a trailing path separator. A model steered by prompt injection could supply a crafted path that resolved to a sibling directory sharing the memory root's name as a prefix, allowing reads and writes outside the sandboxed memory directory. This issue has been patched in version 0.81.0.	N/A	More Details
CVE-2026-34450	The Claude SDK for Python provides access to the Claude API from Python applications. From version 0.86.0 to before version 0.87.0, the local filesystem memory tool in the Anthropic Python SDK created memory files with mode 0o666, leaving them world-readable on systems with a standard umask and world-writable in environments with a permissive umask such as many Docker base images. A local attacker on a shared host could read persisted agent state, and in containerized deployments could modify memory files to influence subsequent model behavior. Both the synchronous and asynchronous memory tool implementations were affected. This issue has been patched in version 0.87.0.	N/A	More Details
CVE-2026-34443	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Prior to version 1.8.211, checkIpByMask() in app/Misc/Helper.php checks whether the input IP contains a / character. Plain IP addresses never contain /, so the function always returns false without checking any CIDR ranges. The entire 10.0.0.0/8 and 172.16.0.0/12 private ranges are unprotected. This issue has been patched in version 1.8.211.	N/A	More Details
CVE-2026-33074	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, a user may be able to purchase a lower tier subscription but grant themselves the benefits that comes along with a higher tier subscription. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.	N/A	More Details
CVE-2026-23287	In the Linux kernel, the following vulnerability has been resolved: irqchip/sifive-plic: Fix frozen interrupt due to affinity setting PLIC ignores interrupt completion message for disabled interrupt, explained by the specification: The PLIC signals it has completed executing an interrupt handler by writing the interrupt ID it received from the claim to the claim/complete register. The PLIC does not check whether the completion ID is the same as the last claim ID for that target. If the completion ID does not match an interrupt source that is currently enabled for the target, the completion is silently ignored. This caused problems in the past, because an interrupt can be disabled while still being handled and plic_irq_eoi() had no effect. That was fixed by checking if the interrupt is disabled, and if so enable it, before sending the completion message. That check is done with irqd_irq_disabled(). However, that is not sufficient because the enable bit for the handling hart can be zero despite irqd_irq_disabled(d) being false. This can happen when affinity setting is changed while a hart is still handling the interrupt. This problem is easily reproducible by dumping a large file to uart (which generates lots of interrupts) and at the same time keep changing the uart interrupt's affinity setting. The uart port becomes frozen almost instantaneously. Fix this by checking PLIC's enable bit instead of irqd_irq_disabled().	N/A	More Details
CVE-2026-34363	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.65 and 9.7.0-alpha.9, when multiple clients subscribe to the same class via LiveQuery, the event handlers process each subscriber concurrently using shared mutable objects. The sensitive data filter modifies these shared objects in-place, so when one subscriber's filter removes a protected field, subsequent subscribers may receive the already-filtered object. This can cause protected fields and authentication data to leak to clients that should not see them, or cause clients that should see the data to receive an incomplete object. Additionally, when an afterEvent Cloud Code trigger is registered, one subscriber's trigger modifications can leak to other subscribers through the same shared mutable state. Any Parse Server deployment using LiveQuery with protected fields or afterEvent triggers is affected when multiple clients subscribe to the same class. This issue has been patched in versions 8.6.65 and 9.7.0-alpha.9.	N/A	More Details
CVE-2026-34574	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.69 and 9.7.0-alpha.14, an authenticated user can bypass the immutability guard on session fields (expiresAt, createdWith) by sending a null value in a PUT request to the session update endpoint. This allows nullifying the session expiry, making the session valid indefinitely and bypassing configured session length policies. This issue has been patched in versions 8.6.69 and 9.7.0-alpha.14.	N/A	More Details
CVE-2026-34235	PJSIP is a free and open source multimedia communication library written in C. Prior to version 2.17, a heap out-of-bounds read vulnerability exists in PJSIP's VP9 RTP unpacketizer that occurs when parsing crafted VP9 Scalability Structure (SS) data. Insufficient bounds checking on the payload descriptor length may cause reads beyond the allocated RTP payload buffer. This issue has been patched in version 2.17. A workaround for this issue involves disabling VP9 codec if not needed.	N/A	More Details
CVE-2026-	Sliver is a command and control framework that uses a custom Wireguard netstack. Prior to version 1.7.4, a single click on a malicious link gives an unauthenticated attacker immediate, silent control over every active C2 session or beacon, capable of exfiltrating all collected target	N/A	More

34227	data (e.g. SSH keys, ntds.dit) or destroying the entire compromised infrastructure, entirely through the operator's own browser. This issue has been patched in version 1.7.4.		Details
CVE-2026-34221	MikroORM is a TypeScript ORM for Node.js based on Data Mapper, Unit of Work and Identity Map patterns. Prior to versions 6.6.10 and 7.0.6, a prototype pollution vulnerability exists in the Utils.merge helper used internally by MikroORM when merging object structures. The function did not prevent special keys such as __proto__, constructor, or prototype, allowing attacker-controlled input to modify the JavaScript object prototype when merged. This issue has been patched in versions 6.6.10 and 7.0.6.	N/A	More Details
CVE-2026-34220	MikroORM is a TypeScript ORM for Node.js based on Data Mapper, Unit of Work and Identity Map patterns. Prior to versions 6.6.10 and 7.0.6, there is a SQL injection vulnerability when specially crafted objects are interpreted as raw SQL query fragments. This issue has been patched in versions 6.6.10 and 7.0.6.	N/A	More Details
CVE-2026-34219	libp2p-rust is the official rust language Implementation of the libp2p networking stack. Prior to version 0.49.4, the Rust libp2p Gossipsub implementation contains a remotely reachable panic in backoff expiry handling. After a peer sends a crafted PRUNE control message with an attacker-controlled, near-maximum backoff value, the value is accepted and stored as an Instant near the representable upper bound. On a later heartbeat, the implementation performs unchecked Instant + Duration arithmetic (backoff_time + slack), which can overflow and panic with: overflow when adding duration to instant. This issue is reachable from any Gossipsub peer over normal TCP + Noise + mplex/yamux connectivity and requires no further authentication beyond becoming a protocol peer. This issue has been patched in version 0.49.4.	N/A	More Details
CVE-2026-34218	ClearanceKit intercepts file-system access events on macOS and enforces per-process access policies. Prior to version 4.2.14, two related startup defects created a window during which only the single compile-time baseline rule was enforced by opfilter. All managed (MDM-delivered) and user-defined file-access rules were not applied until the user interacted with policies through the GUI, triggering a policy mutation over XPC. This issue has been patched in version 4.2.14.	N/A	More Details
CVE-2026-30284	An arbitrary file overwrite vulnerability in UXGROUP LLC Voice Recorder v10.0 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.	N/A	More Details
CVE-2026-30281	An arbitrary file overwrite vulnerability in MaruNuri LLC v2.0.23 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.	N/A	More Details
CVE-2026-30276	An arbitrary file overwrite vulnerability in DeftPDF Document Translator v54.0 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.	N/A	More Details
CVE-2026-33728	dd-trace-java is a Datadog APM client for Java. In versions of dd-trace-java 0.40.0 through prior to 1.60.2, the RMI instrumentation registered a custom endpoint that deserialized incoming data without applying serialization filters. On JDK version 16 and earlier, an attacker with network access to a JMX or RMI port on an instrumented JVM could exploit this to potentially achieve remote code execution. All three of the following conditions must be true to exploit this vulnerability: First, dd-trace-java is attached as a Java agent (`-javaagent`) on Java 16 or earlier. Second, a JMX/RMI port has been explicitly configured via `-Dcom.sun.management.jmxremote.port` and is network-reachable, Third, a gadget-chain-compatible library is present on the classpath. For JDK >= 17, no action is required, but upgrading is strongly encouraged. For JDK >= 8u121 < JDK 17, upgrade to dd-trace-java version 1.60.3 or later. For JDK < 8u121 and earlier where serialization filters are not available, apply the workaround. The workaround is to set the following environment variable to disable the RMI integration: `DD_INTEGRATION_RMI_ENABLED=false`.	N/A	More Details
CVE-2026-22561	Uncontrolled search path elements in Anthropic Claude for Windows installer (Claude Setup.exe) versions prior to 1.1.3363 allow local privilege escalation via DLL search-order hijacking. The installer loads DLLs (e.g., profapi.dll) from its own directory after UAC elevation, enabling arbitrary code execution if a malicious DLL is planted alongside the installer.	N/A	More Details
CVE-2026-34532	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.67 and 9.7.0-alpha.11, an attacker can bypass Cloud Function validator access controls by appending "prototype.constructor" to the function name in the URL. When a Cloud Function handler is declared using the function keyword and its validator is a plain object or arrow function, the trigger store traversal resolves the handler through its own prototype chain while the validator store fails to mirror this traversal, causing all access control enforcement to be skipped. This allows unauthenticated callers to invoke Cloud Functions that are meant to be protected by validators such as requireUser, requireMaster, or custom validation logic. This issue has been patched in versions 8.6.67 and 9.7.0-alpha.11.	N/A	More Details
CVE-2026-33729	OpenFGA is a high-performance and flexible authorization/permission engine built for developers and inspired by Google Zanzibar. In versions prior to 1.13.1, under specific conditions, models using conditions with caching enabled can result in two different check requests producing the same cache key. This can result in OpenFGA reusing an earlier cached result for a different request. Users are affected if the model has relations which rely on condition evaluation andncaching is enabled. OpenFGA v1.13.1 contains a patch.	N/A	More Details
CVE-2026-34377	ZEBRA is a Zcash node written entirely in Rust. Prior to zebrad version 4.3.0 and zebra-consensus version 5.0.1, a logic error in Zebra's transaction verification cache could allow a malicious miner to induce a consensus split. By matching a valid transaction's txid while providing invalid authorization data, a miner could cause vulnerable Zebra nodes to accept an invalid block, leading to a consensus split from the rest of the Zcash network. This would not allow invalid transactions to be accepted but could result in a consensus split between vulnerable Zebra nodes and invulnerable Zebra and Zcashd nodes. This issue has been patched in zebrad version 4.3.0 and zebra-consensus version 5.0.1.	N/A	More Details
CVE-2026-34373	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.66 and 9.7.0-alpha.10, the GraphQL API endpoint does not respect the allowOrigin server option and unconditionally allows cross-origin requests from any website. This bypasses origin restrictions that operators configure to control which websites can interact with the Parse Server API. The REST API correctly enforces the configured allowOrigin restriction. This issue has been patched in versions 8.6.66 and 9.7.0-alpha.10.	N/A	More Details
CVE-2026-34573	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.68 and 9.7.0-alpha.12, the GraphQL query complexity validator can be exploited to cause a denial-of-service by sending a crafted query with binary fan-out fragment spreads. A single unauthenticated request can block the Node.js event loop for seconds, denying service to all concurrent users. This only affects deployments that have enabled the requestComplexity.graphQLDepth or requestComplexity.graphQLFields configuration options. This issue has been patched in versions 8.6.68 and 9.7.0-alpha.12.	N/A	More Details
CVE-2026-34595	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.70 and 9.7.0-alpha.18, an authenticated user with find class-level permission can bypass the protectedFields class-level permission setting on LiveQuery subscriptions. By sending a subscription with a $or, $and, or $nor operator value as a plain object with numeric keys and a length property (an "array-like" object) instead of an array, the protected-field guard is bypassed. The subscription event firing acts as a binary oracle, allowing the attacker to infer whether a protected field matches a given test value. This issue has been patched in versions 8.6.70 and 9.7.0-alpha.18.	N/A	More Details
CVE-2026-	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, non-staff users could access read receipt information for staff-only posts they weren't supposed to see. No post content was exposed, only metadata about who read the post and when. This issue has been patched in versions 2026.1.3, 2026.2.2, and	N/A	More Details

32620	2026.3.0.		
CVE-2026-5087	PAGI::Middleware::Session::Store::Cookie versions through 0.001003 for Perl generates random bytes insecurely. PAGI::Middleware::Session::Store::Cookie attempts to read bytes from the /dev/urandom device directly. If that fails (for example, on systems without the device, such as Windows), then it will emit a warning that recommends the user install Crypt::URandom, and then return a string of random bytes generated by the built-in rand function, which is unsuitable for cryptographic applications. This modules does not use the Crypt::URandom module, and installing it will not fix the problem. The random bytes are used for generating an initialisation vector (IV) to encrypt the cookie. A predictable IV may make it easier for malicious users to decrypt and tamper with the session data that is stored in the cookie.	N/A	More Details
CVE-2026-32619	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, users who lost access to a topic (e.g., removed from a private category group) could still interact with polls in that topic, including voting and toggling poll status. No content was exposed, but users could modify poll state in topics they should no longer have access to. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.	N/A	More Details
CVE-2026-32615	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, category group moderators could perform privileged actions on topics inside private categories they did not have read access to. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.	N/A	More Details
CVE-2026-32607	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, when the hidden prioritize_full_name_in_ux site setting is enabled (defaults to false, requires console access to change), user and group display names are rendered without HTML escaping in several assignment-related UI paths. This allows users with assign permission to inject arbitrary HTML/JavaScript that executes in the browser of any user viewing an affected topic. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.	N/A	More Details
CVE-2026-32243	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, an attacker with the ability to create shared AI conversations could inject arbitrary HTML and JavaScript via crafted conversation titles. This payload would execute in the browser of any user viewing the onebox preview, potentially allowing session hijacking or unauthorized actions on behalf of the victim. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.	N/A	More Details
CVE-2026-32143	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, moderators could export CSV data for admin-restricted reports, bypassing the report visibility restrictions. This could expose sensitive operational data intended only for admins. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.	N/A	More Details
CVE-2026-32113	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to before 2026.2.2, and 2026.3.0-latest to before 2026.3.0, the enter action in StaticController reads the sso_destination_url cookie and redirects to it with allow_other_host: true without validating the destination URL. While this cookie is normally set during legitimate DiscourseConnect Provider flows with cryptographically validated SSO payloads, cookies are client-controlled and can be set by attackers. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.	N/A	More Details
CVE-2026-30286	An arbitrary file overwrite vulnerability in Funambol, Inc. Zefiro Cloud v32.0.2026011614 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.	N/A	More Details
CVE-2026-30283	An arbitrary file overwrite vulnerability in PEAKSEL D.O.O. NIS Animal Sounds and Ringtones v1.3.0 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.	N/A	More Details
CVE-2026-30279	An arbitrary file overwrite vulnerability in Squareapps LLC My Location Travel Timeline v11.80 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.	N/A	More Details
CVE-2026-30278	An arbitrary file overwrite vulnerability in FLY is FUN Aviation Navigation v35.33 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.	N/A	More Details
CVE-2026-30277	An arbitrary file overwrite vulnerability in PDF Reader App : TA/UTAX Mobile Print v3.7.2.251001 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.	N/A	More Details
CVE-2026-2123	A security audit identified a privilege escalation vulnerability in Operations Agent(<=OA 12.29) on Windows. Under specific conditions Operations Agent may run executables from specific writeable locations.Thanks to Manuel Rickli & Philippe Leiser of Oneconsult AG for reporting this vulnerability	N/A	More Details
CVE-2025-62184	Pega Platform versions 8.1.0 through 25.1.0 are affected by a Stored Cross-site Scripting vulnerability in a user interface component. Requires an administrative user and given extensive access rights, impact to Confidentiality is low and Integrity is none.	N/A	More Details
CVE-2026-33699	pypdf is a free and open-source pure-python PDF library. Versions prior to 6.9.2 have a vulnerability in which an attacker can craft a PDF which leads to an infinite loop. This requires reading a file in non-strict mode. This has been fixed in pypdf 6.9.2. If users cannot upgrade yet, consider applying the changes from the patch manually.	N/A	More Details
CVE-2026-33701	OpenTelemetry Java Instrumentation provides OpenTelemetry auto-instrumentation and instrumentation libraries for Java. In versions prior to 2.26.1, the RMI instrumentation registered a custom endpoint that deserialized incoming data without applying serialization filters. On JDK version 16 and earlier, an attacker with network access to a JMX or RMI port on an instrumented JVM could exploit this to potentially achieve remote code execution. All three of the following conditions must be true to exploit this vulnerability: First, OpenTelemetry Java instrumentation is attached as a Java agent (`-javaagent`) on Java 16 or earlier. Second, JMX/RMI port has been explicitly configured via `-Dcom.sun.management.jmxremote.port` and is network-reachable. Third, gadget-chain-compatible library is present on the classpath. This results in arbitrary remote code execution with the privileges of the user running the instrumented JVM. For JDK >= 17, no action is required, but upgrading is strongly encouraged. For JDK < 17, upgrade to version 2.26.1 or later. As a workaround, set the system property `-Dotel.instrumentation.rmi.enabled=false` to disable the RMI integration.	N/A	More Details
CVE-2025-41355	Reflected Cross-Site Scripting (XSS) vulnerability in Anon Proxy Server v0.104. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by sending him/her a malicious URL. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user. It affects 'port' and 'proxyPort' parameters in '/anon.php' endpoint.	N/A	More Details

CVE-2026-23317	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Return the correct value in vmw_translate_ptr functions Before the referenced fixes these functions used a lookup function that returned a pointer. This was changed to another lookup function that returned an error code with the pointer becoming an out parameter. The error path when the lookup failed was not changed to reflect this change and the code continued to return the PTR_ERR of the now uninitialized pointer. This could cause the vmw_translate_ptr functions to return success when they actually failed causing further uninitialized and OOB accesses.	N/A	More Details
CVE-2026-23288	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Fix out-of-bounds memset in command slot handling The remaining space in a command slot may be smaller than the size of the command header. Clearing the command header with memset() before verifying the available slot space can result in an out-of-bounds write and memory corruption. Fix this by moving the memset() call after the size validation.	N/A	More Details
CVE-2026-23352	In the Linux kernel, the following vulnerability has been resolved: x86/efi: defer freeing of boot services memory efi_free_boot_services() frees memory occupied by EFI_BOOT_SERVICES_CODE and EFI_BOOT_SERVICES_DATA using memblock_free_late(). There are two issue with that: memblock_free_late() should be used for memory allocated with memblock_alloc() while the memory reserved with memblock_reserve() should be freed with free_reserved_area(). More acutely, with CONFIG_DEFERRED_STRUCT_PAGE_INIT=y efi_free_boot_services() is called before deferred initialization of the memory map is complete. Benjamin Herrenschmidt reports that this causes a leak of ~140MB of RAM on EC2 t3a.nano instances which only have 512MB or RAM. If the freed memory resides in the areas that memory map for them is still uninitialized, they won't be actually freed because memblock_free_late() calls memblock_free_pages() and the latter skips uninitialized pages. Using free_reserved_area() at this point is also problematic because __free_page() accesses the buddy of the freed page and that again might end up in uninitialized part of the memory map. Delaying the entire efi_free_boot_services() could be problematic because in addition to freeing boot services memory it updates efi.memmap without any synchronization and that's undesirable late in boot when there is concurrency. More robust approach is to only defer freeing of the EFI boot services memory. Split efi_free_boot_services() in two. First efi_unmap_boot_services() collects ranges that should be freed into an array then efi_free_boot_services() later frees them after deferred init is complete.	N/A	More Details
CVE-2025-15036	A path traversal vulnerability exists in the `extract_archive_to_dir` function within the `mlflow/pyfunc/dbconnect_artifact_cache.py` file of the mlflow/mlflow repository. This vulnerability, present in versions before v3.7.0, arises due to the lack of validation of tar member paths during extraction. An attacker with control over the tar.gz file can exploit this issue to overwrite arbitrary files or gain elevated privileges, potentially escaping the sandbox directory in multi-tenant or shared cluster environments.	N/A	More Details
CVE-2026-23354	In the Linux kernel, the following vulnerability has been resolved: x86/fred: Correct speculative safety in fred_extint() array_index_nospec() is no use if the result gets spilled to the stack, as it makes the believed safe-under-speculation value subject to memory predictions. For all practical purposes, this means array_index_nospec() must be used in the expression that accesses the array. As the code currently stands, it's the wrong side of irqentry_enter(), and 'index' is put into %ebp across the function call. Remove the index variable and reposition array_index_nospec(), so it's calculated immediately before the array access.	N/A	More Details
CVE-2026-23355	In the Linux kernel, the following vulnerability has been resolved: ata: libata: cancel pending work after clearing deferred_qc Syzbot reported a WARN_ON() in ata_scsi_deferred_qc_work(), caused by ap->ops->qc_defer() returning non-zero before issuing the deferred qc. ata_scsi_schedule_deferred_qc() is called during each command completion. This function will check if there is a deferred QC, and if ap->ops->qc_defer() returns zero, meaning that it is possible to queue the deferred qc at this time (without being deferred), then it will queue the work which will issue the deferred qc. Once the work get to run, which can potentially be a very long time after the work was scheduled, there is a WARN_ON() if ap->ops->qc_defer() returns non-zero. While we hold the ap->lock both when assigning and clearing deferred_qc, and the work itself holds the ap->lock, the code currently does not cancel the work after clearing the deferred qc. This means that the following scenario can happen: 1) One or several NCQ commands are queued. 2) A non-NCQ command is queued, gets stored in ap->deferred_qc. 3) Last NCQ command gets completed, work is queued to issue the deferred qc. 4) Timeout or error happens, ap->deferred_qc is cleared. The queued work is currently NOT canceled. 5) Port is reset. 6) One or several NCQ commands are queued. 7) A non-NCQ command is queued, gets stored in ap->deferred_qc. 8) Work is finally run. Yet at this time, there is still NCQ commands in flight. The work in 8) really belongs to the non-NCQ command in 2), not to the non-NCQ command in 7). The reason why the work is executed when it is not supposed to, is because it was never canceled when ap->deferred_qc was cleared in 4). Thus, ensure that we always cancel the work after clearing ap->deferred_qc. Another potential fix would have been to let ata_scsi_deferred_qc_work() do nothing if ap->ops->qc_defer() returns non-zero. However, canceling the work when clearing ap->deferred_qc seems slightly more logical, as we hold the ap->lock when clearing ap->deferred_qc, so we know that the work cannot be holding the lock. (The function could be waiting for the lock, but that is okay since it will do nothing if ap->deferred_qc is not set.)	N/A	More Details
CVE-2025-7741	Hardcoded Password Vulnerability have been found in CENTUM. Affected products contain a hardcoded password for the user account (PROG) used for CENTUM Authentication Mode within the system. Under the following conditions, there is a risk that an attacker could log in as the PROG user. The default permission for the PROG users is S1 permission (equivalent to OFFUSER). Therefore, for properly permission-controlled targets of operation and monitoring, even if an attacker user in as the PROG user, the risk of critical operations or configuration changes being performed is considered low. (If the PROG user's permissions have been changed for any reason, there is a risk that operations or configuration changes may be performed under the modified permissions. The CVSS values below are for the default permissions.) Additionally, exploiting this vulnerability requires an attacker to already have access to the HIS screen controls. Therefore, an attacker can already operate and monitor at that point, regardless of this vulnerability. The conditions under which this vulnerability is exploited: If all of the following conditions are met, the affected products are vulnerable to this vulnerability. -An attacker obtains the hardcoded password using a certain method. -The HIS with the affected product installed is configured in CTM authentication mode. -An attacker must have direct access to the aforementioned HIS or be able to break into it remotely using a certain method and perform screen operations. The affected products and versions are as follows: CENTUM VP R5.01.00 to R5.04.20, R6.01.00 to R6.12.00 and R7.01.00.	N/A	More Details
CVE-2026-23356	In the Linux kernel, the following vulnerability has been resolved: drbd: fix "LOGIC BUG" in drbd_al_begin_io_nonblock() Even though we check that we "should" be able to do lc_get_cumulative() while holding the device->al_lock spinlock, it may still fail, if some other code path decided to do lc_try_lock() with bad timing. If that happened, we logged "LOGIC BUG for enr=...", but still did not return an error. The rest of the code now assumed that this request has references for the relevant activity log extents. The implcations are that during an active resync, mutual exclusivity of resync versus application IO is not guaranteed. And a potential crash at this point may not realizs that these extents could have been target of in-flight IO and would need to be resynced just in case. Also, once the request completes, it will give up activity log references it does not even hold, which will trigger a BUG_ON(refcnt == 0) in lc_put(). Fix: Do not crash the kernel for a condition that is harmless during normal operation: also catch "e->refcnt == 0", not only "e == NULL" when being noisy about "al_complete_io() called on inactive extent %u\n". And do not try to be smart and "guess" whether something will work, then be surprised when it does not. Deal with the fact that it may or may not work. If it does not, remember a possible "partially in activity log" state (only possible for requests that cross extent boundaries), and return an error code from drbd_al_begin_io_nonblock(). A latter call for the same request will then resume from where we left off.	N/A	More Details
CVE-2026-23357	In the Linux kernel, the following vulnerability has been resolved: can: mcp251x: fix deadlock in error path of mcp251x_open The mcp251x_open() function call free_irq() in its error path with the mpc_lock mutex held. But if an interrupt already occurred the interrupt handler will be waiting for the mpc_lock and free_irq() will deadlock waiting for the handler to finish. This issue is similar to the one fixed in commit 7dd9c26bd6cf ("can: mcp251x: fix deadlock if an interrupt occurs during mcp251x_open") but for the error path. To solve this issue move the call to free_irq() after the lock is released. Setting `priv->force_quit = 1` beforehand ensure that the IRQ handler will exit right away once it acquired the lock.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix error handling in slot reset If the device has not recovered		

2026-23358	after slot reset is called, it goes to out label for error handling. There it could make decision based on uninitialized hive pointer and could result in accessing an uninitialized list. Initialize the list and hive properly so that it handles the error situation and also releases the reset domain lock which is acquired during error_detected callback. (cherry picked from commit bb71362182e59caa227e4192da5a612b09349696)	N/A	More Details
CVE-2026-23359	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix stack-out-of-bounds write in devmap get_upper_ifindexes() iterates over all upper devices and writes their indices into an array without checking bounds. Also the callers assume that the max number of upper devices is MAX_NEST_DEV and allocate excluded_devices[1+MAX_NEST_DEV] on the stack, but that assumption is not correct and the number of upper devices could be larger than MAX_NEST_DEV (e.g., many macvlans), causing a stack-out-of-bounds write. Add a max parameter to get_upper_ifindexes() to avoid the issue. When there are too many upper devices, return -EOVERFLOW and abort the redirect. To reproduce, create more than MAX_NEST_DEV(8) macvlans on a device with an XDP program attached using BPF_F_BROADCAST | BPF_F_EXCLUDE_INGRESS. Then send a packet to the device to trigger the XDP redirect path.	N/A	More Details
CVE-2026-23360	In the Linux kernel, the following vulnerability has been resolved: nvme: fix admin queue leak on controller reset When nvme_alloc_admin_tag_set() is called during a controller reset, a previous admin queue may still exist. Release it properly before allocating a new one to avoid orphaning the old queue. This fixes a regression introduced by commit 03b3bcd319b3 ("nvme: fix admin request_queue lifetime").	N/A	More Details
CVE-2026-23362	In the Linux kernel, the following vulnerability has been resolved: can: bcm: fix locking for bcm_op runtime updates Commit c2aba69d0c36 ("can: bcm: add locking for bcm_op runtime updates") added a locking for some variables that can be modified at runtime when updating the sending bcm_op with a new TX_SETUP command in bcm_tx_setup(). Usually the RX_SETUP only handles and filters incoming traffic with one exception: When the RX_RTR_FRAME flag is set a predefined CAN frame is sent when a specific RTR frame is received. Therefore the rx bcm_op uses bcm_can_tx() which uses the bcm_tx_lock that was only initialized in bcm_tx_setup(). Add the missing spin_lock_init() when allocating the bcm_op in bcm_rx_setup() to handle the RTR case properly.	N/A	More Details
CVE-2026-23363	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7925: Fix possible oob access in mt7925_mac_write_txwi_80211() Check frame length before accessing the mgmt fields in mt7925_mac_write_txwi_80211 in order to avoid a possible oob access.	N/A	More Details
CVE-2026-23364	In the Linux kernel, the following vulnerability has been resolved: ksmbd: Compare MACs in constant time To prevent timing attacks, MAC comparisons need to be constant-time. Replace the memcmp() with the correct function, crypto_memneq().	N/A	More Details
CVE-2026-5022	The '/api/v1/files/images/{flow_id}/{file_name}' endpoint does not enforce any authentication or authorization checks, allowing any unauthenticated user to download images belonging to any flow by knowing (or guessing) the flow ID and file name.	N/A	More Details
CVE-2026-23365	In the Linux kernel, the following vulnerability has been resolved: net: usb: kalmia: validate USB endpoints The kalmia driver should validate that the device it is probing has the proper number and types of USB endpoints it is expecting before it binds to it. If a malicious device were to not have the same urbs the driver will crash later on when it blindly accesses these endpoints.	N/A	More Details
CVE-2026-23366	In the Linux kernel, the following vulnerability has been resolved: drm/client: Do not destroy NULL modes 'modes' in drm_client_modeset_probe may fail to kcalloc. If this occurs, we jump to 'out', calling modes_destroy on it, which dereferences it. This may result in a NULL pointer dereference in the error case. Prevent that.	N/A	More Details
CVE-2026-23367	In the Linux kernel, the following vulnerability has been resolved: wifi: radiotap: reject radiotap with unknown bits The radiotap parser is currently only used with the radiotap namespace (not with vendor namespaces), but if the undefined field 18 is used, the alignment/size is unknown as well. In this case, iterator->_next_ns_data isn't initialized (it's only set for skipping vendor namespaces), and syzbot points out that we later compare against this uninitialized value. Fix this by moving the rejection of unknown radiotap fields down to after the in-namespace lookup, so it will really use iterator->_next_ns_data only for vendor namespaces, even in case undefined fields are present.	N/A	More Details
CVE-2026-23368	In the Linux kernel, the following vulnerability has been resolved: net: phy: register phy led_triggers during probe to avoid AB-BA deadlock There is an AB-BA deadlock when both LEDS_TRIGGER_NETDEV and LED_TRIGGER_PHY are enabled: [1362.049207] [<8054e4b8>] led_trigger_register+0x5c/0x1fc <-- Trying to get lock "triggers_list_lock" via down_write(&triggers_list_lock); [1362.054536] [<80662830>] phy_led_triggers_register+0xd0/0x234 [1362.060329] [<8065e200>] phy_attach_direct+0x33c/0x40c [1362.065489] [<80651fc4>] phylink_fwnode_phy_connect+0x15c/0x23c [1362.071480] [<8066ee18>] mtk_open+0x7c/0xba0 [1362.075849] [<806d714c>] __dev_open+0x280/0x2b0 [1362.080384] [<806d7668>] __dev_change_flags+0x244/0x24c [1362.085598] [<806d7698>] dev_change_flags+0x28/0x78 [1362.090528] [<807150e4>] dev_ioctl+0x4c0/0x654 <-- Hold lock "rtnl_mutex" by calling rtnl_lock(); [1362.094985] [<80694360>] sock_ioctl+0x2f4/0x4e0 [1362.099567] [<802e9c4c>] sys_ioctl+0x32c/0xd8c [1362.104022] [<80014504>] syscall_common+0x34/0x58 Here LED_TRIGGER_PHY is registering LED triggers during phy_attach while holding RTNL and then taking triggers_list_lock. [1362.191101] [<806c2640>] register_netdevice_notifier+0x60/0x168 <-- Trying to get lock "rtnl_mutex" via rtnl_lock(); [1362.197073] [<805504ac>] netdev_trig_activate+0x194/0x1e4 [1362.202490] [<8054e28c>] led_trigger_set+0x1d4/0x360 <-- Hold lock "triggers_list_lock" by down_read(&triggers_list_lock); [1362.207511] [<8054eb38>] led_trigger_write+0xd8/0x14c [1362.212566] [<80381d98>] sysfs_kf_bin_write+0x80/0xbc [1362.217688] [<8037fcd8>] kernfs_fop_write_iter+0x17c/0x28c [1362.223174] [<802cbd70>] vfs_write+0x21c/0x3c4 [1362.227712] [<802cc0c4>] ksys_write+0x78/0x12c [1362.232164] [<80014504>] syscall_common+0x34/0x58 Here LEDS_TRIGGER_NETDEV is being enabled on an LED. It first takes triggers_list_lock and then RTNL. A classical AB-BA deadlock. phy_led_triggers_registers() does not require the RTNL, it does not make any calls into the network stack which require protection. There is also no requirement the PHY has been attached to a MAC, the triggers only make use of phydev state. This allows the call to phy_led_triggers_registers() to be placed elsewhere. PHY probe() and release() don't hold RTNL, so solving the AB-BA deadlock.	N/A	More Details
CVE-2026-23369	In the Linux kernel, the following vulnerability has been resolved: i2c: i801: Revert "i2c: i801: replace acpi_lock with I2C bus lock" This reverts commit f707d6b9e7c18f669adfdb443906d46cfbaaa0c1. Under rare circumstances, multiple udev threads can collect i801 device info on boot and walk i801_acpi_io_handler somewhat concurrently. The first will note the area is reserved by acpi to prevent further touches. This ultimately causes the area to be deregistered. The second will enter i801_acpi_io_handler after the area is unregistered but before a check can be made that the area is unregistered. i2c_lock_bus relies on the now unregistered area containing lock_ops to lock the bus. The end result is a kernel panic on boot with the following backtrace; [14.971872] ioatdma 0000:09:00.2: enabling device (0100 -> 0102) [14.971873] BUG: kernel NULL pointer dereference, address: 0000000000000000 [14.971880] #PF: supervisor read access in kernel mode [14.971884] #PF: error_code(0x0000) - not-present page [14.971887] PGD 0 P4D 0 [14.971894] Oops: 0000 [#1] PREEMPT SMP PTI [14.971900] CPU: 5 PID: 956 Comm: systemd-udevd Not tainted 5.14.0-611.5.1.el9_7.x86_64 #1 [14.971905] Hardware name: XXXXXXXXXXXXXXXXXXXXXX BIOS 1.20.10.SV91 01/30/2023 [14.971908] RIP: 0010:i801_acpi_io_handler+0x2d/0xb0 [i2c_i801] [14.971929] Code: 00 00 49 8b 40 20 41 57 41 56 4d 8b b8 30 04 00 00 49 89 ce 41 55 41 89 d5 41 54 49 89 f4 be 02 00 00 00 55 4c 89 c5 53 89 fb <48> 8b 00 4c 89 c7 e8 18 61 54 e9 80 bd 80 04 00 00 00 75 09 4c 3b [14.971933] RSP: 0018:ffffbaa841483838 EFLAGS: 00010282 [14.971938] RAX: 0000000000000000 RBX: 0000000000000000 RCX: ffff9685e01ba568 [14.971941] RDX: 0000000000000008 RSI: 0000000000000002 RDI: 0000000000000000 [14.971944] RBP: ffff9685ca22f028 R08: ffff9685ca22f028 R09: ffff9685ca22f028 [14.971948] R10: 000000000000000b R11: 0000000000000580 R12: 0000000000000580 [14.971951] R13: 0000000000000008 R14: ffff9685e01ba568 R15: ffff9685c222f000 [14.971954] FS: 00007f8287c0ab40(0000) GS:ffff96a47f940000(0000) knlGS:0000000000000000 [14.971959] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [14.971963] CR2: 0000000000000000 CR3: 0000000168090001 CR4: 0000000003706f0 [14.971966] DR0:	N/A	More Details

	0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [14.971968] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [14.971972] Call Trace: [14.971977] <TASK> [14.971981] ? show_trace_log_lvl+0x1c4/0x2df [14.971994] ? show_trace_log_lvl+0x1c4/0x2df [14.972003] ? acpi_ev_address_space_dispatch+0x16e/0x3c0 [14.972014] ? __die_body.cold+0x8/0xd [14.972021] ? page_fault_oops+0x132/0x170 [14.972028] ? exc_page_fault+0x61/0x150 [14.972036] ? asm_exc_page_fault+0x22/0x30 [14.972045] ? i801_acpi_io_handler+0x2d/0xb0 [i2c_i801] [14.972061] acpi_ev_address_space_dispatch+0x16e/0x3c0 [14.972069] ? __pfx_i801_acpi_io_handler+0x10/0x10 [i2c_i801] [14.972085] acpi_ex_access_region+0x5b/0xd0 [14.972093] acpi_ex_field_datum_io+0x73/0x2e0 [14.972100] acpi_ex_read_data_from_field+0x8e/0x230 [14.972106] acpi_ex_resolve_node_to_value+0x23d/0x310 [14.972114] acpi_ds_evaluate_name_path+0xad/0x110 [14.972121] acpi_ds_exec_end_op+0x321/0x510 [14.972127] acpi_ps_parse_loop+0xf7/0x680 [14.972136] acpi_ps_parse_aml+0x17a/0x3d0 [14.972143] acpi_ps_execute_method+0x137/0x270 [14.972150] acpi_ns_evaluate+0x1f4/0x2e0 [14.972158] acpi_evaluate_object+0x134/0x2f0 [14.972164] acpi_evaluate_integer+0x50/0xe0 [14.972173] ? vsnprintf+0x24b/0x570 [14.972181] acpi_ac_get_state.part.0+0x23/0x70 [14.972189] get_ac_property+0x4e/0x60 [14.972195] power_supply_show_property+0x90/0x1f0 [14.972205] add_prop_uevent+0x29/0x90 [14.972213] power_supply_uevent+0x109/0x1d0 [14.972222] dev_uevent+0x10e/0x2f0 [14.972228] uevent_show+0x8e/0x100 [14.972236] dev_attr_show+0x19 ---truncated---		
CVE-2026-23370	In the Linux kernel, the following vulnerability has been resolved: platform/x86: dell-wmi-sysman: Don't hex dump plaintext password data set_new_password() hex dumps the entire buffer, which contains plaintext password data, including current and new passwords. Remove the hex dump to avoid leaking credentials.	N/A	More Details
CVE-2026-23371	In the Linux kernel, the following vulnerability has been resolved: sched/deadline: Fix missing ENQUEUE_REPLENISH during PI de-boosting Running stress-ng --schedpolicy 0 on an RT kernel on a big machine might lead to the following WARNINGs (edited). sched: DL de-boosted task PID 22725: REPLENISH flag missing WARNING: CPU: 93 PID: 0 at kernel/sched/deadline.c:239 dequeue_task_dl+0x15c/0x1f8 ... (running_bw underflow) Call trace: dequeue_task_dl+0x15c/0x1f8 (P) dequeue_task+0x80/0x168 deactivate_task+0x24/0x50 push_dl_task+0x264/0x2e0 dl_task_timer+0x1b0/0x228 __hrtimer_run_queues+0x188/0x378 hrtimer_interrupt+0xfc/0x260 ... The problem is that when a SCHED_DEADLINE task (lock holder) is changed to a lower priority class via sched_setscheduler(), it may fail to properly inherit the parameters of potential DEADLINE donors if it didn't already inherit them in the past (shorter deadline than donor's at that time). This might lead to bandwidth accounting corruption, as enqueue_task_dl() won't recognize the lock holder as boosted. The scenario occurs when: 1. A DEADLINE task (donor) blocks on a PI mutex held by another DEADLINE task (holder), but the holder doesn't inherit parameters (e.g., it already has a shorter deadline) 2. sched_setscheduler() changes the holder from DEADLINE to a lower class while still holding the mutex 3. The holder should now inherit DEADLINE parameters from the donor and be enqueued with ENQUEUE_REPLENISH, but this doesn't happen Fix the issue by introducing __setscheduler_dl_pi(), which detects when a DEADLINE (proper or boosted) task gets setscheduled to a lower priority class. In case, the function makes the task inherit DEADLINE parameters of the donoer (pi_se) and sets ENQUEUE_REPLENISH flag to ensure proper bandwidth accounting during the next enqueue operation.	N/A	More Details
CVE-2026-5026	The '/api/v1/files/images/{flow_id}/{file_name}' endpoint serves SVG files with the 'image/svg+xml' content type without sanitizing their content. Since SVG files can contain embedded JavaScript, an attacker can upload a malicious SVG that executes arbitrary JavaScript when viewed by other users, leading to stored cross-site scripting (XSS). This allows stealing authentication tokens stored in cookies, including JWT access and refresh tokens.	N/A	More Details
CVE-2026-23372	In the Linux kernel, the following vulnerability has been resolved: nfc: rawsock: cancel tx_work before socket teardown In rawsock_release(), cancel any pending tx_work and purge the write queue before orphaning the socket. rawsock_tx_work runs on the system workqueue and calls nfc_data_exchange which dereferences the NCI device. Without synchronization, tx_work can race with socket and device teardown when a process is killed (e.g. by SIGKILL), leading to use-after-free or leaked references. Set SEND_SHUTDOWN first so that if tx_work is already running it will see the flag and skip transmitting, then use cancel_work_sync to wait for any in-progress execution to finish, and finally purge any remaining queued skbs.	N/A	More Details
CVE-2026-23373	In the Linux kernel, the following vulnerability has been resolved: wifi: rsi: Don't default to -EOPNOTSUPP in rsi_mac80211_config This triggers a WARN_ON in ieee80211_hw_conf_init and isn't the expected behavior from the driver - other drivers default to 0 too.	N/A	More Details
CVE-2026-23353	In the Linux kernel, the following vulnerability has been resolved: ice: fix crash in ethtool offline loopback test Since the conversion of ice to page pool, the ethtool loopback test crashes: BUG: kernel NULL pointer dereference, address: 000000000000000c #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 1100f1067 P4D 0 Oops: Oops: 0002 [#1] SMP NOPTI CPU: 23 UID: 0 PID: 5904 Comm: ethtool Kdump: loaded Not tainted 6.19.0-0.rc7.260128g1f97d9dcf5364.49.eln154.x86_64 #1 PREEMPT(lazy) Hardware name: [...] RIP: 0010:ice_alloc_rx_bufs+0x1cd/0x310 [ice] Code: 83 6c 24 30 01 66 41 89 47 08 0f 84 c0 00 00 00 41 0f b7 dc 48 8b 44 24 18 48 c1 e3 04 41 bb 00 10 00 00 48 8d 2c 18 8b 04 24 <89> 45 0c 41 8b 4d 00 49 d3 e3 44 3b 5c 24 24 0f 83 ac fe ff ff 44 RSP: 0018:ff7894738aa1f768 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000700 RDI: 0000000000000000 RBP: 0000000000000000 R08: ff16dcae79880200 R09: 0000000000000019 R10: 0000000000000001 R11: 0000000000001000 R12: 0000000000000000 R13: 0000000000000000 R14: 0000000000000000 R15: ff16dcae6c670000 FS: 00007fcf428850c0(0000) GS:ff16dcb149710000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000000000000c CR3: 0000000121227005 CR4: 0000000000773ef0 PKRU: 55555554 Call Trace: <TASK> ice_vsi_cfg_rxq+0xca/0x460 [ice] ice_vsi_cfg_rxqs+0x54/0x70 [ice] ice_loopback_test+0xa9/0x520 [ice] ice_self_test+0x1b9/0x280 [ice] ethtool_self_test+0xe5/0x200 __dev_ethtool+0x1106/0x1a90 dev_ethtool+0xbe/0x1a0 dev_ioctl+0x258/0x4c0 sock_do_ioctl+0xe3/0x130 __x64_sys_ioctl+0xb9/0x100 do_syscall_64+0x7c/0x700 entry_SYSCALL_64_after_hwframe+0x76/0x7e [...] It crashes because we have not initialized libeth for the rx ring. Fix it by treating ICE_VSI_LB VSIs slightly more like normal PF VSIs and letting them have a q_vector. It's just a dummy, because the loopback test does not use interrupts, but it contains a napi struct that can be passed to libeth_rx_fq_create() called from ice_vsi_cfg_rxq() -> ice_rxq_pp_create().	N/A	More Details
CVE-2026-23351	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_set_pipapo: split gc into unlink and reclaim phase Yiming Qian reports Use-after-free in the pipapo set type: Under a large number of expired elements, commit-time GC can run for a very long time in a non-preemptible context, triggering soft lockup warnings and RCU stall reports (local denial of service). We must split GC in an unlink and a reclaim phase. We cannot queue elements for freeing until pointers have been swapped. Expired elements are still exposed to both the packet path and userspace dumpers via the live copy of the data structure. call_rcu() does not protect us: dump operations or element lookups starting after call_rcu has fired can still observe the free'd element, unless the commit phase has made enough progress to swap the clone and live pointers before any new reader has picked up the old version. This a similar approach as done recently for the rbtree backend in commit 35f83a75529a ("netfilter: nft_set_rbtree: don't gc elements on insert").	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: xdp: produce a warning when calculated tailroom is negative Many ethernet drivers report xdp Rx queue frag size as being the same as DMA write size. However, the only user of this field, namely bpf_xdp_frags_increase_tail(), clearly expects a truesize. Such difference leads to unspecific memory corruption issues under certain circumstances, e.g. in ixgbevf maximum DMA write size is 3 KB, so when running xskxceiver's XDP_ADJUST_TAIL_GROW_MULTI_BUFF, 6K packet fully uses all DMA-writable space in 2 buffers. This would be fine, if only rxq->frag_size was properly set to 4K, but value of 3K results in a negative tailroom, because there is a non-zero page offset. We are supposed to return -EINVAL and be done with it in such case, but due to tailroom being stored as an unsigned int, it is reported to be somewhere near UINT_MAX, resulting in a tail being grown, even if the requested offset is too much (it is around 2K in the abovementioned test). This later leads to all kinds of unspecific calltraces. [7340.337579] xskxceiver[1440]: segfault at 1da718 ip 00007f4161aeac9d sp 00007f41615a6a00 error 6 [7340.338040] xskxceiver[1441]: segfault at		

CVE-2026-23343	7f410000000b ip 00000000004042b5 sp 00007f415bffecf0 error 4 [7340.338179] in libc.so.6[61c9d,7f4161aaf000+160000] [7340.339230] in xskxceiver[42b5,400000+69000] [7340.340300] likely on CPU 6 (core 0, socket 6) [7340.340302] Code: ff ff 01 e9 f4 fe ff ff 0f 1f 44 00 00 4c 39 f0 74 73 31 c0 ba 01 00 00 00 f0 0f b1 17 0f 85 ba 00 00 00 49 8b 87 88 00 00 00 <4c> 89 70 08 eb cc 0f 1f 44 00 00 48 8d bd f0 fe ff ff 89 85 ec fe [7340.340888] likely on CPU 3 (core 0, socket 3) [7340.345088] Code: 00 00 00 ba 00 00 00 00 be 00 00 00 00 89 c7 e8 31 ca ff ff 89 45 ec 8b 45 ec 85 c0 78 07 b8 00 00 00 00 eb 46 e8 0b c8 ff ff <8b> 00 83 f8 69 74 24 e8 ff c7 ff ff 8b 00 83 f8 0b 74 18 e8 f3 c7 [7340.404334] Oops: general protection fault, probably for non-canonical address 0x6d255010bdffc: 0000 [#1] SMP NOPTI [7340.405972] CPU: 7 UID: 0 PID: 1439 Comm: xskxceiver Not tainted 6.19.0-rc1+ #21 PREEMPT(lazy) [7340.408006] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.17.0-5.fc42 04/01/2014 [7340.409716] RIP: 0010:lookup_swap_cgroup_id+0x44/0x80 [7340.410455] Code: 83 f8 1c 73 39 48 ba ff ff ff ff ff ff ff 03 48 8b 04 c5 20 55 fa bd 48 21 d1 48 89 ca 83 e1 01 48 d1 ea c1 e1 04 48 8d 04 90 <8b> 00 48 83 c4 10 d3 e8 c3 cc cc cc cc 31 c0 e9 98 b7 dd 00 48 89 [7340.412787] RSP: 0018:ffffcc5c04f7f6d0 EFLAGS: 00010202 [7340.413494] RAX: 0006d255010bdffc RBX: ffff891f477895a8 RCX: 0000000000000010 [7340.414431] RDX: 0001c17e3fffffff RSI: 00fa070000000000 RDI: 000382fc7fffffff [7340.415354] RBP: 00fa070000000000 R08: ffffcc5c04f7f8f8 R09: ffffcc5c04f7f7d0 [7340.416283] R10: ffff891f4c1a7000 R11: ffffcc5c04f7f9c8 R12: ffffcc5c04f7f7d0 [7340.417218] R13: 03ffffffffffffff R14: 00fa06fffffffe00 R15: ffff891f47789500 [7340.418229] FS: 0000000000000000(0000) GS:ffff891ffdfaa000(0000) knlGS:0000000000000000 [7340.419489] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [7340.420286] CR2: 00007f415bfffd58 CR3: 0000000103f03002 CR4: 0000000000772ef0 [7340.421237] PKRU: 55555554 [7340.421623] Call Trace: [7340.421987] <TASK> [7340.422309] ? softleaf_from_pte+0x77/0xa0 [7340.422855] swap_pte_batch+0xa7/0x290 [7340.423363] zap_nonpresent_ptes.constprop.0.isra.0+0xd1/0x270 [7340.424102] zap_pte_range+0x281/0x580 [7340.424607] zap_pmd_range.isra.0+0xc9/0x240 [7340.425177] unmap_page_range+0x24d/0x420 [7340.425714] unmap_vmas+0xa1/0x180 [7340.426185] exit_mmap+0xe1/0x3b0 [7340.426644] __mmput+0x41/0x150 [7340.427098] exit_mm+0xb1/0x110 [7340.427539] do_exit+0x1b2/0x460 [7340.427992] do_group_exit+0x2d/0xc0 [7340.428477] get_signal+0x79d/0x7e0 [7340.428957] arch_do_signal_or_restart+0x34/0x100 [7340.429571] exit_to_user_mode_loop+0x8e/0x4c0 [7340.430159] do_syscall_64+0x188/ ---truncated---	N/A	More Details
CVE-2026-23350	In the Linux kernel, the following vulnerability has been resolved: drm/xe/queue: Call fini on exec queue creation fail Every call to queue init should have a corresponding fini call. Skipping this would mean skipping removal of the queue from GuC list (which is part of guc_id allocation). A damaged queue stored in exec_queue_lookup list would lead to invalid memory reference, sooner or later. Call fini to free guc_id. This must be done before any internal LRCs are freed. Since the finalization with this extra call became very similar to __xe_exec_queue_fini(), reuse that. To make this reuse possible, alter xe_lrc_put() so it can survive NULL parameters, like other similar functions. v2: Reuse _xe_exec_queue_fini(). Make xe_lrc_put() aware of NULLs. (cherry picked from commit 393e5fea6f7d7054abc2c3d97a4cfe8306cd6079)	N/A	More Details
CVE-2026-33373	An issue was discovered in Zimbra Collaboration (ZCS) 10.0 and 10.1. A Cross-Site Request Forgery (CSRF) vulnerability exists in Zimbra Web Client due to the issuance of authentication tokens without CSRF protection during certain account state transitions. Specifically, tokens generated after operations such as enabling two-factor authentication or changing a password may lack CSRF enforcement. While such a token is active, authenticated SOAP requests that trigger token generation or state changes can be performed without CSRF validation. An attacker could exploit this by inducing a victim to submit crafted requests, potentially allowing sensitive account actions such as disabling two-factor authentication. The issue is mitigated by ensuring CSRF protection is consistently enforced for all issued authentication tokens.	N/A	More Details
CVE-2026-1496	Vulnerable versions of Coverity Connect lack an error handler in the authentication logic for command line tooling that makes it vulnerable to an authentication bypass. A malicious actor with access to the /token API endpoint that either knows or guesses a valid username, can use this in a specially crafted HTTP request to bypass authentication. Successful exploitation allows the malicious actor to assume all roles and privileges granted to the valid user's Coverity Connect account.	N/A	More Details
CVE-2026-28760	The installer of RATOC RAID Monitoring Manager for Windows searches the current directory to load certain DLLs. If a user is directed to place a crafted DLL with the installer, an arbitrary code may be executed with the administrator privilege.	N/A	More Details
CVE-2026-3321	A vulnerability of authorization bypass through user-controlled key in the 'console-survey/api/v1/answer/{EVENTID}/{TIMESTAMP}/' endpoint. Exploiting this vulnerability would allow an unauthenticated attacker to enumerate event IDs and obtain the complete Q&A history. This publicly exposed data may include IDs, private URLs, private messages, internal references, or other sensitive information that should only be exposed to authenticated users. In addition, the leaked content could be exploited to facilitate other malicious activities, such as reconnaissance for lateral movement, exploitation of related systems, or unauthorised access to internal applications referenced in the content of chat messages.	N/A	More Details
CVE-2026-4315	A Cross-Site Request Forgery (CSRF) vulnerability in the WatchGuard Fireware OS WebUI could allow a remote attacker to trigger a denial-of-service (DoS) condition in the Fireware Web UI by convincing an authenticated administrator into visiting a malicious web page.This issue affects Fireware OS: 11.8 through 11.12.4+541730, 12.0 through 12.11.8, and 2025.1 through 2026.1.2.	N/A	More Details
CVE-2026-4266	An Insecure Deserialization vulnerability in WatchGuard Fireware OS allows an attacker that has obtained write access to the local filesystem through another vulnerability to execute arbitrary code in the context of the portald user.This issue affects Fireware OS: 12.1 through 12.11.8 and 2025.1 through 2026.1.2. Note, this vulnerability does not affect Firebox platforms that do not support the Access Portal feature, including the T-15 and T-35.	N/A	More Details
CVE-2026-4425	Rejected reason: Reserved for EastLink case, but no need for CVE anymore	N/A	More Details
CVE-2026-30407	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-2026-23345	In the Linux kernel, the following vulnerability has been resolved: arm64: gcs: Do not set PTE_SHARED on GCS mappings if FEAT_LPA2 is enabled When FEAT_LPA2 is enabled, bits 8-9 of the PTE replace the shareability attribute with bits 50-51 of the output address. The _PAGE_GCS{,_RO} definitions include the PTE_SHARED bits as 0b11 (this matches the other _PAGE_* definitions) but using this macro directly leads to the following panic when enabling GCS on a system/model with LPA2: Unable to handle kernel paging request at virtual address fffff1ffc32d8008 Mem abort info: ESR = 0x0000000096000004 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 swapper pgtable: 4k pages, 52-bit VAs, pgdp=0000000060f4d000 [fffff1ffc32d8008] pgd=100000006184b003, p4d=0000000000000000 Internal error: Oops: 0000000096000004 [#1] SMP CPU: 0 UID: 0 PID: 513 Comm: gcs_write_fault Tainted: G M 7.0.0-rc1 #1 PREEMPT Tainted: [M]=MACHINE_CHECK Hardware name: QEMU QEMU Virtual Machine, BIOS 2025.02-8+deb13u1 11/08/2025 pstate: 03402005 (nzcv daif +PAN -UAO +TCO +DIT -SSBS BTYPE=--) pc : zap_huge_pmd+0x168/0x468 lr : zap_huge_pmd+0x2c/0x468 sp : ffff800080beb660 x29: ffff800080beb660 x28: fff00000c2058180 x27: ffff800080beb898 x26: fff00000c2058180 x25: ffff800080beb820 x24: 00c800010b600f41 x23: ffffc1ffc30af1a8 x22: fff00000c2058180 x21: 0000ffff8dc00000 x20: fff00000c2bc6370 x19: ffff800080beb898 x18: ffff800080bebb60 x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000007 x14: 000000000000000a x13: 0000aaaacbbbffff x12: 0000000000000000 x11: 0000ffff8ddfffff x10: 00000000000001fe x9 : 0000ffff8ddfffff x8 : 0000ffff8de00000 x7 : 0000ffff8da00000 x6 : fff00000c2bc6370 x5 : 0000ffff8da00000 x4 : 000000010b600000 x3 : ffffc1ffc0000000 x2 : fff00000c2058180 x1 : fffff1ffc32d8000 x0 : 000000c00010b600 Call trace: zap_huge_pmd+0x168/0x468 (P) unmap_page_range+0xd70/0x1560 unmap_single_vma+0x48/0x80 unmap_vmas+0x90/0x180 unmap_region+0x88/0xe4	N/A	More Details

	vms_complete_munmap_vmas+0xf8/0x1e0 do_vmi_align_munmap+0x158/0x180 do_vmi_munmap+0xac/0x160 __vm_munmap+0xb0/0x138 vm_munmap+0x14/0x20 gcs_free+0x70/0x80 mm_release+0x1c/0xc8 exit_mm_release+0x28/0x38 do_exit+0x190/0x8ec do_group_exit+0x34/0x90 get_signal+0x794/0x858 arch_do_signal_or_restart+0x11c/0x3e0 exit_to_user_mode_loop+0x10c/0x17c el0_da+0x8c/0x9c el0t_64_sync_handler+0xd0/0xf0 el0t_64_sync+0x198/0x19c Code: aa1603e2 d34cfc00 cb813001 8b011861 (f9400420) Similarly to how the kernel handles protection_map[], use a gcs_page_prot variable to store the protection bits and clear PTE_SHARED if LPA2 is enabled. Also remove the unused PAGE_GCS{,_RO} macros.		
CVE-2026-33284	GlobaLeaks is free and open-source whistleblowing software. Prior to version 5.0.89, the /api/support endpoint of GlobaLeaks performs minimal validation on user-submitted support requests. As a result, arbitrary URLs can be included in support emails sent to administrators. Version 5.0.89 patches the issue.	N/A	More Details
CVE-2026-33433	Traefik is an HTTP reverse proxy and load balancer. Prior to versions 2.11.42, 3.6.11, and 3.7.0-ea.3, when `headerField` is configured with a non-canonical HTTP header name (e.g., `x-auth-user` instead of `X-Auth-User`), an authenticated attacker can inject their own canonical version of that header to impersonate any identity to the backend. The backend receives two header entries — the attacker-injected canonical one is read first, overriding Traefik's non-canonical write. Versions 2.11.42, 3.6.11, and 3.7.0-ea.3 patch the issue.	N/A	More Details
CVE-2026-33748	BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. Prior to version 0.28.1, insufficient validation of Git URL fragment subdir components may allow access to files outside the checked-out Git repository root. Possible access is limited to files on the same mounted filesystem. The issue has been fixed in version v0.28.1 The issue affects only builds that use Git URLs with a subpath component. As a workaround, avoid building Dockerfiles from untrusted sources or using the subdir component from an untrusted Git repository where the subdir component could point to a symlink.	N/A	More Details
CVE-2026-33201	Digital Photo Frame GH-WDF10A provided by GREEN HOUSE CO., LTD. contains an active debug code vulnerability. If this vulnerability is exploited, files or configurations on the affected device may be read or written, or arbitrary files may be executed with root privileges.	N/A	More Details
CVE-2026-1612	AL-KO Robolinho Update Software has hard-coded AWS Access and Secret keys that allow anyone to access AL-KO's AWS bucket. Using the keys directly might give the attacker greater access than the app itself. Key grants AT LEAST read access to some of the objects in bucket. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only versions 8.0.21.0610 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2026-5128	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-23346	In the Linux kernel, the following vulnerability has been resolved: arm64: io: Extract user memory type in ioremap_prot() The only caller of ioremap_prot() outside of the generic ioremap() implementation is generic_access_phys(), which passes a 'pgprot_t' value determined from the user mapping of the target 'pfn' being accessed by the kernel. On arm64, the 'pgprot_t' contains all of the non-address bits from the pte, including the permission controls, and so we end up returning a new user mapping from ioremap_prot() which faults when accessed from the kernel on systems with PAN: | Unable to handle kernel read from unreadable memory at virtual address ffff80008ea89000 | ... | Call trace: | __memcpy_fromio+0x80/0xf8 | generic_access_phys+0x20c/0x2b8 | __access_remote_vm+0x46c/0x5b8 | access_remote_vm+0x18/0x30 | environ_read+0x238/0x3e8 | vfs_read+0xe4/0x2b0 | ksys_read+0xcc/0x178 | __arm64_sys_read+0x4c/0x68 Extract only the memory type from the user 'pgprot_t' in ioremap_prot() and assert that we're being passed a user mapping, to protect us against any changes in future that may require additional handling. To avoid falsely flagging users of ioremap(), provide our own ioremap() macro which simply wraps __ioremap_prot().	N/A	More Details
CVE-2026-23347	In the Linux kernel, the following vulnerability has been resolved: can: usb: f81604: correctly anchor the urb in the read bulk callback When submitting an urb, that is using the anchor pattern, it needs to be anchored before submitting it otherwise it could be leaked if usb_kill_anchored_urbs() is called. This logic is correctly done elsewhere in the driver, except in the read bulk callback so do that here also.	N/A	More Details
CVE-2026-23348	In the Linux kernel, the following vulnerability has been resolved: cxl: Fix race of nvdimm_bus object when creating nvdimm objects Found issue during running of cxl-translate.sh unit test. Adding a 3s sleep right before the test seems to make the issue reproduce fairly consistently. The cxl_translate module has dependency on cxl_acpi and causes orphaned nvdimm objects to reprobe after cxl_acpi is removed. The nvdimm_bus object is registered by the cxl_nvb object when cxl_acpi_probe() is called. With the nvdimm_bus object missing, __nd_device_register() will trigger NULL pointer dereference when accessing the dev->parent that points to &nvdimm_bus->dev. [192.884510] BUG: kernel NULL pointer dereference, address: 000000000000006c [192.895383] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS edk2-20250812-19.fc42 08/12/2025 [192.897721] Workqueue: cxl_port cxl_bus_rescan_queue [cxl_core] [192.899459] RIP: 0010:kobject_get+0xc/0x90 [192.924871] Call Trace: [192.925959] <TASK> [192.926976] ? pm_runtime_init+0xb9/0xe0 [192.929712] __nd_device_register.part.0+0x4d/0xc0 [libnvdimm] [192.933314] __nvdimm_create+0x206/0x290 [libnvdimm] [192.936662] cxl_nvdimm_probe+0x119/0x1d0 [cxl_pmem] [192.940245] cxl_bus_probe+0x1a/0x60 [cxl_core] [192.943349] really_probe+0xde/0x380 This patch also relies on the previous change where devm_cxl_add_nvdimm_bridge() is called from drivers/cxl/pmem.c instead of drivers/cxl/core.c to ensure the dependency of cxl_acpi on cxl_pmem. 1. Set probe_type of cxl_nvb to PROBE_FORCE_SYNCHRONOUS to ensure the driver is probed synchronously when add_device() is called. 2. Add a check in __devm_cxl_add_nvdimm_bridge() to ensure that the cxl_nvb driver is attached during cxl_acpi_probe(). 3. Take the cxl_root uport_dev lock and the cxl_nvb->dev lock in devm_cxl_add_nvdimm() before checking nvdimm_bus is valid. 4. Set cxl_nvdimm flag to CXL_NVD_F_INVALIDATED so cxl_nvdimm_probe() will exit with -EBUSY. The removal of cxl_nvdimm devices should prevent any orphaned devices from probing once the nvdimm_bus is gone. [dj: Fixed 0-day reported kdoc issue.] [dj: Fix cxl_nvb reference leak on error. Gregory (kreview-0811365)]	N/A	More Details
CVE-2026-23349	In the Linux kernel, the following vulnerability has been resolved: HID: pidff: Fix condition effect bit clearing As reported by MPDarkGuy on discord, NULL pointer dereferences were happening because not all the conditional effects bits were cleared. Properly clear all conditional effect bits from ffbit	N/A	More Details
CVE-2026-25704	A Privilege Dropping / Lowering Errors/Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in cosmic-greeter can allow an attacker to regain privileges that should have been dropped and abuse them in the racy checking logic. This issue affects cosmic-greeter before https://github.Com/pop-os/cosmic-greeter/pull/426.	N/A	More Details
CVE-2025-3716	User enumeration in ESET Protect (on-prem) via Response Timing.	N/A	More Details
CVE-2025-15379	A command injection vulnerability exists in MLflow's model serving container initialization code, specifically in the `_install_model_dependencies_to_env()` function. When deploying a model with `env_manager=LOCAL`, MLflow reads dependency specifications from the model artifact's `python_env.yaml` file and directly interpolates them into a shell command without sanitization. This allows an attacker to supply a malicious model artifact and achieve arbitrary command execution on systems that deploy the model. The vulnerability affects versions 3.8.0 and is fixed in version 3.8.2.	N/A	More Details

CVE-2026-5010	A reflected Cross-Site Scripting (XSS) vulnerability has been discovered in Clickedu. This vulnerability allows an attacker to execute JavaScript code in the victim’s browser by sending them a malicious URL using the endpoint “/user.php/”. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on the user’s behalf.	N/A	More Details
CVE-2026-23374	In the Linux kernel, the following vulnerability has been resolved: blktrace: fix __this_cpu_read/write in preemptible context tracing_record_cmdline() internally uses __this_cpu_read() and __this_cpu_write() on the per-CPU variable trace_cmdline_save, and trace_save_cmdline() explicitly asserts preemption is disabled via lockdep_assert_preemption_disabled(). These operations are only safe when preemption is off, as they were designed to be called from the scheduler context (probe_wakeup_sched_switch() / probe_wakeup()). __blk_add_trace() was calling tracing_record_cmdline(current) early in the blk_tracer path, before ring buffer reservation, from process context where preemption is fully enabled. This triggers the following using blktests/blktrace/002: blktrace/002 (blktrace ftrace corruption with sysfs trace) [failed] runtime 0.367s ... 0.437s something found in dmesg: [81.211018] run blktests blktrace/002 at 2026-02-25 22:24:33 [81.239580] null_blk: disk nullb1 created [81.357294] BUG: using __this_cpu_read() in preemptible [00000000] code: dd/2516 [81.362842] caller is tracing_record_cmdline+0x10/0x40 [81.362872] CPU: 16 UID: 0 PID: 2516 Comm: dd Tainted: G N 7.0.0-rc1lblk+ #84 PREEMPT(full) [81.362877] Tainted: [N]=TEST [81.362878] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.17.0-0-gb52ca86e094d-prebuilt.qemu.org 04/01/2014 [81.362881] Call Trace: [81.362884] <TASK> [81.362886] dump_stack_lvl+0x8d/0xb0 ... (See '/mnt/sda/blktests/results/nodev/blktrace/002.dmesg' for the entire message) [81.211018] run blktests blktrace/002 at 2026-02-25 22:24:33 [81.239580] null_blk: disk nullb1 created [81.357294] BUG: using __this_cpu_read() in preemptible [00000000] code: dd/2516 [81.362842] caller is tracing_record_cmdline+0x10/0x40 [81.362872] CPU: 16 UID: 0 PID: 2516 Comm: dd Tainted: G N 7.0.0-rc1lblk+ #84 PREEMPT(full) [81.362877] Tainted: [N]=TEST [81.362878] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.17.0-0-gb52ca86e094d-prebuilt.qemu.org 04/01/2014 [81.362881] Call Trace: [81.362884] <TASK> [81.362886] dump_stack_lvl+0x8d/0xb0 [81.362895] check_preemption_disabled+0xce/0xe0 [81.362902] tracing_record_cmdline+0x10/0x40 [81.362923] __blk_add_trace+0x307/0x5d0 [81.362934] ? lock_acquire+0xe0/0x300 [81.362940] ? iov_iter_extract_pages+0x101/0xa30 [81.362959] blk_add_trace_bio+0x106/0x1e0 [81.362968] submit_bio_noacct_nocheck+0x24b/0x3a0 [81.362979] ? lockdep_init_map_type+0x58/0x260 [81.362988] submit_bio_wait+0x56/0x90 [81.363009] __blkdev_direct_IO_simple+0x16c/0x250 [81.363026] ? __pfx_submit_bio_wait_endio+0x10/0x10 [81.363038] ? rcu_read_lock_any_held+0x73/0xa0 [81.363051] blkdev_read_iter+0xc1/0x140 [81.363059] vfs_read+0x20b/0x330 [81.363083] ksys_read+0x67/0xe0 [81.363090] do_syscall_64+0xbf/0xf00 [81.363102] entry_SYSCALL_64_after_hwframe+0x76/0x7e [81.363106] RIP: 0033:0x7f281906029d [81.363111] Code: 31 c0 e9 c6 fe ff ff 50 48 8d 3d 66 63 0a 00 e8 59 ff 01 00 66 0f 1f 84 00 00 00 00 00 80 3d 41 33 0e 00 00 74 17 31 c0 0f 05 <48> 3d 00 f0 ff ff 77 5b c3 66 2e 0f 1f 84 00 00 00 00 00 48 83 ec [81.363113] RSP: 002b:00007ffca127dd48 EFLAGS: 00000246 ORIG_RAX: 0000000000000000 [81.363120] RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007f281906029d [81.363122] RDX: 0000000000001000 RSI: 0000559f8bfae000 RDI: 0000000000000000 [81.363123] RBP: 0000000000001000 R08: 0000002863a10a81 R09: 00007f281915f000 [81.363124] R10: 00007f2818f77b60 R11: 0000000000000246 R12: 0000559f8bfae000 [81.363126] R13: 0000000000000000 R14: 0000000000000000 R15: 000000000000000a [81.363142] </TASK> The same BUG fires from blk_add_trace_plug(), blk_add_trace_unplug(), and blk_add_trace_rq() paths as well. The purpose of tracin ---truncated---	N/A	More Details
CVE-2026-23400	In the Linux kernel, the following vulnerability has been resolved: rust_binder: call set_notification_done() without proc lock Consider the following sequence of events on a death listener: 1. The remote process dies and sends a BR_DEAD_BINDER message. 2. The local process invokes the BC_CLEAR_DEATH_NOTIFICATION command. 3. The local process then invokes the BC_DEAD_BINDER_DONE. Then, the kernel will reply to the BC_DEAD_BINDER_DONE command with a BR_CLEAR_DEATH_NOTIFICATION_DONE reply using push_work_if_looper(). However, this can result in a deadlock if the current thread is not a looper. This is because dead_binder_done() still holds the proc lock during set_notification_done(), which called push_work_if_looper(). Normally, push_work_if_looper() takes the thread lock, which is fine to take under the proc lock. But if the current thread is not a looper, then it falls back to delivering the reply to the process work queue, which involves taking the proc lock. Since the proc lock is already held, this is a deadlock. Fix this by releasing the proc lock during set_notification_done(). It was not intentional that it was held during that function to begin with. I don't think this ever happens in Android because BC_DEAD_BINDER_DONE is only invoked in response to BR_DEAD_BINDER messages, and the kernel always delivers BR_DEAD_BINDER to a looper. So there's no scenario where Android userspace will call BC_DEAD_BINDER_DONE on a non-looper thread.	N/A	More Details
CVE-2026-23375	In the Linux kernel, the following vulnerability has been resolved: mm: thp: deny THP for files on anonymous inodes file_thp_enabled() incorrectly allows THP for files on anonymous inodes (e.g. guest_memfd and secretmem). These files are created via alloc_file_pseudo(), which does not call get_write_access() and leaves inode->i_writecount at 0. Combined with S_ISREG(inode->i_mode) being true, they appear as read-only regular files when CONFIG_READ_ONLY_THP_FOR_FS is enabled, making them eligible for THP collapse. Anonymous inodes can never pass the inode_is_open_for_write() check since their i_writecount is never incremented through the normal VFS open path. The right thing to do is to exclude them from THP eligibility altogether, since CONFIG_READ_ONLY_THP_FOR_FS was designed for real filesystem files (e.g. shared libraries), not for pseudo-filesystem inodes. For guest_memfd, this allows khugepaged and MADV_COLLAPSE to create large folios in the page cache via the collapse path, but the guest_memfd fault handler does not support large folios. This triggers WARN_ON_ONCE(folio_test_large(folio)) in kvm_gmem_fault_user_mapping(). For secretmem, collapse_file() tries to copy page contents through the direct map, but secretmem pages are removed from the direct map. This can result in a kernel crash: BUG: unable to handle page fault for address: ffff88810284d000 RIP: 0010:memcpy_orig+0x16/0x130 Call Trace: collapse_file hpage_collapse_scan_file madvise_collapse Secretmem is not affected by the crash on upstream as the memory failure recovery handles the failed copy gracefully, but it still triggers confusing false memory failure reports: Memory failure: 0x106d96f: recovery action for clean unevictable LRU page: Recovered Check IS_ANON_FILE(inode) in file_thp_enabled() to deny THP for all anonymous inode files.	N/A	More Details
CVE-2026-23376	In the Linux kernel, the following vulnerability has been resolved: nvmet-fcloop: Check remoteport port_state before calling done callback In nvme_fc_handle_ls_rqst_work, the lsrsp->done callback is only set when remoteport->port_state is FC_OBJSTATE_ONLINE. Otherwise, the nvme_fc_xmt_ls_rsp's LLDD call to lport->ops->xmt_ls_rsp is expected to fail and the nvme-fc transport layer itself will directly call nvme_fc_xmt_ls_rsp_free instead of relying on LLDD's done callback to free the lsrsp resources. Update the fcloop_t2h_xmt_ls_rsp routine to check remoteport->port_state. If online, then lsrsp->done callback will free the lsrsp. Else, return -ENODEV to signal the nvme-fc transport to handle freeing lsrsp.	N/A	More Details
CVE-2025-9497	Use of Hard-coded Credentials vulnerability in Microchip Time Provider 4100 allows Malicious Manual Software Update.This issue affects Time Provider 4100: before 2.5.0.	N/A	More Details
CVE-2026-23399	In the Linux kernel, the following vulnerability has been resolved: nf_tables: nft_dynset: fix possible stateful expression memleak in error path If cloning the second stateful expression in the element via GFP_ATOMIC fails, then the first stateful expression remains in place without being released. unreferenced object (percpu) 0x607b97e9cab8 (size 16): comm "softirq", pid 0, jiffies 4294931867 hex dump (first 16 bytes on cpu 3): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 backtrace (crc 0): pcpu_alloc_noprof+0x453/0xd80 nft_counter_clone+0x9c/0x190 [nf_tables] nft_expr_clone+0x8f/0x1b0 [nf_tables] nft_dynset_new+0x2cb/0x5f0 [nf_tables] nft_rhash_update+0x236/0x11c0 [nf_tables] nft_dynset_eval+0x11f/0x670 [nf_tables] nft_do_chain+0x253/0x1700 [nf_tables] nft_do_chain_ipv4+0x18d/0x270 [nf_tables] nf_hook_slow+0xaa/0x1e0 ip_local_deliver+0x209/0x330	N/A	More Details
CVE-2026-34385	Fleet is open source device management software. Prior to 4.81.0, a second-order SQL injection vulnerability in Fleet's Apple MDM profile delivery pipeline could allow an attacker with a valid MDM enrollment certificate to exfiltrate or modify the contents of the Fleet database, including user credentials, API tokens, and device enrollment secrets. Version 4.81.0 patches the issue.	N/A	More Details
CVE-2026-	Fleet is open source device management software. Prior to 4.81.0, a SQL injection vulnerability in Fleet's MDM bootstrap package configuration allows an authenticated user with Team Admin or Global Admin privileges to modify arbitrary team configurations, exfiltrate sensitive data from	N/A	More

34386	the Fleet database, and inject arbitrary content into team configs via direct API calls. Version 4.81.0 patches the issue.		Details
CVE-2026-33994	Locutus brings stdlibs of other programming languages to JavaScript for educational purposes. Starting in version 2.0.39 and prior to version 3.0.25, a prototype pollution vulnerability exists in the `parse_str` function of the npm package locutus. An attacker can pollute `Object.prototype` by overriding `RegExp.prototype.test` and then passing a crafted query string to `parse_str`, bypassing the prototype pollution guard. This vulnerability stems from an incomplete fix for CVE-2026-25521. The CVE-2026-25521 patch replaced the `String.prototype.includes()`-based guard with a `RegExp.prototype.test()`-based guard. However, `RegExp.prototype.test` is itself a writable prototype method that can be overridden, making the new guard bypassable in the same way as the original — trading one hijackable built-in for another. Version 3.0.25 contains an updated fix.	N/A	More Details
CVE-2026-33993	Locutus brings stdlibs of other programming languages to JavaScript for educational purposes. Prior to version 3.0.25, the `unserialize()` function in `locutus/php/var/unserialize` assigns deserialized keys to plain objects via bracket notation without filtering the `__proto__` key. When a PHP serialized payload contains `__proto__` as an array or object key, JavaScript's `__proto__` setter is invoked, replacing the deserialized object's prototype with attacker-controlled content. This enables property injection, for...in propagation of injected properties, and denial of service via built-in method override. This is distinct from the previously reported prototype pollution in `parse_str` (GHSA-f98m-q3hr-p5wq, GHSA-rxrv-835q-v5mh) — `unserialize` is a different function with no mitigation applied. Version 3.0.25 patches the issue.	N/A	More Details
CVE-2026-34387	Fleet is open source device management software. Prior to 4.81.1, a command injection vulnerability in Fleet's software installer pipeline allows an attacker to achieve arbitrary code execution as root (macOS/Linux) or SYSTEM (Windows) on managed hosts when an uninstall is triggered for a crafted software package. Version 4.81.1 patches the issue.	N/A	More Details
CVE-2026-1712	Incorrect privilege assignment vulnerability in HYPR Server allows Privilege Escalation.This issue affects HYPR Server: from 10.5.1 before 10.7.	N/A	More Details
CVE-2026-33981	changedetection.io is a free open source web page change detection tool. Prior to 0.54.7, the `jq:` and `jqraw:` include filter expressions allow use of the jq `env` builtin, which reads all process environment variables and stores them as the watch snapshot. An authenticated user (or unauthenticated user when no password is set, the default) can leak sensitive environment variables including `SALTED_PASS`, `PLAYWRIGHT_DRIVER_URL`, `HTTP_PROXY`, and any secrets passed as env vars to the container. Version 0.54.7 patches the issue.	N/A	More Details
CVE-2026-23971	Deserialization of Untrusted Data vulnerability in xtemos WoodMart woodmart allows Object Injection.This issue affects WoodMart: from n/a through <= 8.3.8.	N/A	More Details
CVE-2026-25371	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in King-Theme Lumise Product Designer lumise allows Blind SQL Injection.This issue affects Lumise Product Designer: from n/a through < 2.0.9.	N/A	More Details
CVE-2026-33654	nanobot is a personal AI assistant. Prior to version 0.1.6, an indirect prompt injection vulnerability exists in the email channel processing module (`nanobot/channels/email.py`), allowing a remote, unauthenticated attacker to execute arbitrary LLM instructions (and subsequently, system tools) without any interaction from the bot owner. By sending an email containing malicious prompts to the bot's monitored email address, the bot automatically polls, ingests, and processes the email content as highly trusted input, fully bypassing channel isolation and resulting in a stealthy, zero-click attack. Version 0.1.6 patches the issue.	N/A	More Details
CVE-2026-33946	MCP Ruby SDK is the official Ruby SDK for Model Context Protocol servers and clients. Prior to version 0.9.2, the Ruby SDK's streamable_http_transport.rb implementation contains a session hijacking vulnerability. An attacker who obtains a valid session ID can completely hijack the victim's Server-Sent Events (SSE) stream and intercept all real-time data. Version 0.9.2 contains a patch.	N/A	More Details
CVE-2026-33765	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. Versions prior to 6.0 have a critical OS Command Injection vulnerability in the savesettings.php file. The application takes the user-controlled $_POST['webtheme'] parameter and concatenates it directly into a system command executed via PHP's exec() function. Since the input is neither sanitized nor validated before being passed to the shell, an attacker can append arbitrary system commands to the intended pihole command. Furthermore, because the command is executed with sudo privileges, the injected commands will run with elevated (likely root) privileges. Version 6.0 patches the issue.	N/A	More Details
CVE-2026-2414	Authorization bypass through User-Controlled key vulnerability in HYPR Server allows Privilege Escalation.This issue affects Server: from 9.5.2 before 10.7.2.	N/A	More Details
CVE-2026-34046	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to version 1.5.1, the `_read_flow` helper in `src/backend/base/langflow/api/v1/flows.py` branched on the `AUTO_LOGIN` setting to decide whether to filter by `user_id`. When `AUTO_LOGIN` was `False` (i.e., authentication was enabled), neither branch enforced an ownership check — the query returned any flow matching the given UUID regardless of who owned it. This allowed any authenticated user to read any other user's flow, including embedded plaintext API keys; modify the logic of another user's AI agents, and/or delete flows belonging to other users. The vulnerability was introduced by the conditional logic that was meant to accommodate public/example flows (those with `user_id = NULL`) under auto-login mode, but inadvertently left the authenticated path without an ownership filter. The fix in version 1.5.1 removes the `AUTO_LOGIN` conditional entirely and unconditionally scopes the query to the requesting user.	N/A	More Details
CVE-2026-32493	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eyecix JobSearch wp-jobsearch allows Reflected XSS.This issue affects JobSearch: from n/a through <= 3.2.0.	N/A	More Details
CVE-2026-33872	elixir-nodejs provides an Elixir API for calling Node.js functions. A vulnerability in versions prior to 3.1.4 results in Cross-User Data Leakage or Information Disclosure due to a race condition in the worker protocol. The lack of request-response correlation creates a "stale response" vulnerability. Because the worker does not verify which request a response belongs to, it may return the next available data in the buffer to an unrelated caller. In high-throughput environments where the library processes sensitive user data (e.g., PII, authentication tokens, or private records), a timeout or high concurrent load can cause Data A (belonging to User A) to be returned to User B. This may lead to unauthorized information disclosure that is difficult to trace, as the application may not throw an error but instead provide "valid-looking" yet entirely incorrect and private data to the wrong session. The issue is fixed in v3.1.4.	N/A	More Details
CVE-2026-34388	Fleet is open source device management software. Prior to 4.81.0, a denial-of-service vulnerability in Fleet's gRPC Launcher endpoint allows an authenticated host to crash the entire Fleet server process by sending an unexpected log type value. The server terminates immediately, disrupting all connected hosts, MDM enrollments, and API consumers. Version 4.81.0 patches the issue.	N/A	More Details
CVE-2026-34389	Fleet is open source device management software. Prior to 4.81.0, Fleet contained an issue in the user invitation flow where the email address provided during invite acceptance was not validated against the email address associated with the invite. An attacker who obtained a valid invite token could create an account under an arbitrary email address while inheriting the role granted by the invite, including global admin.	N/A	More Details

	Version 4.81.0 patches the issue.		
CVE-2026-34391	Fleet is open source device management software. Prior to 4.81.1, a vulnerability in Fleet's Windows MDM command processing allows a malicious enrolled device to access MDM commands intended for other devices, potentially exposing sensitive configuration data such as WiFi credentials, VPN secrets, and certificate payloads across the entire Windows fleet. Version 4.81.1 patches the issue.	N/A	More Details
CVE-2026-33873	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to version 1.9.0, the Agentic Assistant feature in Langflow executes LLM-generated Python code during its validation phase. Although this phase appears intended to validate generated component code, the implementation reaches dynamic execution sinks and instantiates the generated class server-side. In deployments where an attacker can access the Agentic Assistant feature and influence the model output, this can result in arbitrary server-side Python execution. Version 1.9.0 fixes the issue.	N/A	More Details
CVE-2026-33879	Federated Learning and Interoperability Platform (FLIP) is an open-source platform for federated training and evaluation of medical imaging AI models across healthcare institutions. The FLIP login page in versions 0.1.1 and prior has no rate limiting or CAPTCHA, enabling brute-force and credential-stuffing attacks. FLIP users are external to the organization, increasing credential reuse risk. As of time of publication, it is unclear if a patch is available.	N/A	More Details
CVE-2026-3126	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-28529	cryptodev-linux version 1.14 and prior contain a page reference handling flaw in the get_userbuf function of the /dev/crypto device driver that allows local users to trigger use-after-free conditions. Attackers with access to the /dev/crypto interface can repeatedly decrement reference counts of controlled pages to achieve local privilege escalation.	N/A	More Details
CVE-2026-4761	When a certificate and its private key are installed in the Windows machine certificate store using Network and Security tool, access rights to the private key are unnecessarily granted to the operator group. * Installations based on Panorama Suite 2025 (25.00.004) are vulnerable unless update PS-2500-00-0357 (or higher) is installed * Installations based on Panorama Suite 2025 Updated Dec. 25 (25.10.007) are not vulnerable Please refer to security bulletin BS-036, available on the Panorama CSIRT website: https://my.codra.net/en-gb/csirt.	N/A	More Details
CVE-2026-23387	In the Linux kernel, the following vulnerability has been resolved: pinctrl: cirrus: cs42l43: Fix double-put in cs42l43_pin_probe() devm_add_action_or_reset() already invokes the action on failure, so the explicit put causes a double-put.	N/A	More Details
CVE-2026-23377	In the Linux kernel, the following vulnerability has been resolved: ice: change XDP RxQ frag_size from DMA write length to xdp.frame_sz The only user of frag_size field in XDP RxQ info is bpf_xdp_frags_increase_tail(). It clearly expects whole buff size instead of DMA write size. Different assumptions in ice driver configuration lead to negative tailroom. This allows to trigger kernel panic, when using XDP_ADJUST_TAIL_GROW_MULTI_BUFF xskxceiver test and changing packet size to 6912 and the requested offset to a huge value, e.g. XSK_UMEM__MAX_FRAME_SIZE * 100. Due to other quirks of the ZC configuration in ice, panic is not observed in ZC mode, but tailroom growing still fails when it should not. Use fill queue buffer truesize instead of DMA write size in XDP RxQ info. Fix ZC mode too by using the new helper.	N/A	More Details
CVE-2026-23378	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_ife: Fix metalist update behavior Whenever an ife action replace changes the metalist, instead of replacing the old data on the metalist, the current ife code is appending the new metadata. Aside from being innapropriate behavior, this may lead to an unbounded addition of metadata to the metalist which might cause an out of bounds error when running the encode op: [138.423369][C1] == [138.424317][C1] BUG: KASAN: slab-out-of-bounds in ife_tlv_meta_encode (net/ife/ife.c:168) [138.424906][C1] Write of size 4 at addr ffff8880077f4ffe by task ife_out_out_bou/255 [138.425778][C1] CPU: 1 UID: 0 PID: 255 Comm: ife_out_out_bou Not tainted 7.0.0-rc1-00169-gfbdfa8da05b6 #624 PREEMPT(full) [138.425795][C1] Hardware name: Bochs Bochs, BIOS Bochs 01/01/2011 [138.425800][C1] Call Trace: [138.425804][C1] <IRQ> [138.425808][C1] dump_stack_lvl (lib/dump_stack.c:122) [138.425828][C1] print_report (mm/kasan/report.c:379 mm/kasan/report.c:482) [138.425839][C1] ? srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) [138.425844][C1] ? __virt_addr_valid (./arch/x86/include/asm/preempt.h:95 (discriminator 1) ./include/linux/rcupdate.h:975 (discriminator 1) ./include/linux/mmzone.h:2207 (discriminator 1) arch/x86/mm/physaddr.c:54 (discriminator 1)) [138.425853][C1] ? ife_tlv_meta_encode (net/ife/ife.c:168) [138.425859][C1] kasan_report (mm/kasan/report.c:221 mm/kasan/report.c:597) [138.425868][C1] ? ife_tlv_meta_encode (net/ife/ife.c:168) [138.425878][C1] kasan_check_range (mm/kasan/generic.c:186 (discriminator 1) mm/kasan/generic.c:200 (discriminator 1)) [138.425884][C1] __asan_memset (mm/kasan/shadow.c:84 (discriminator 2)) [138.425889][C1] ife_tlv_meta_encode (net/ife/ife.c:168) [138.425893][C1] ? ife_tlv_meta_encode (net/ife/ife.c:171) [138.425898][C1] ? srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) [138.425903][C1] ife_encode_meta_u16 (net/sched/act_ife.c:57) [138.425910][C1] ? __pfx_do_raw_spin_lock (kernel/locking/spinlock_debug.c:114) [138.425916][C1] ? __asan_memcpy (mm/kasan/shadow.c:105 (discriminator 3)) [138.425921][C1] ? __pfx_ife_encode_meta_u16 (net/sched/act_ife.c:45) [138.425927][C1] ? srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) [138.425931][C1] tcf_ife_act (net/sched/act_ife.c:847 net/sched/act_ife.c:879) To solve this issue, fix the replace behavior by adding the metalist to the ife rcu data structure.	N/A	More Details
CVE-2026-23379	In the Linux kernel, the following vulnerability has been resolved: net/sched: ets: fix divide by zero in the offload path Offloading ETS requires computing each class' WRR weight: this is done by averaging over the sums of quanta as 'q_sum' and 'q_psum'. Using unsigned int, the same integer size as the individual DRR quanta, can overflow and even cause division by zero, like it happened in the following splat: Oops: divide error: 0000 [#1] SMP PTI CPU: 13 UID: 0 PID: 487 Comm: tc Tainted: G E 6.19.0-virtme #45 PREEMPT(full) Tainted: [E]=UNSIGNED_MODULE Hardware name: Bochs Bochs, BIOS Bochs 01/01/2011 RIP: 0010:ets_offload_change+0x11f/0x290 [sch_ets] Code: e4 45 31 ff eb 03 41 89 c7 41 89 cb 89 ce 83 f9 0f 0f 87 b7 00 00 00 45 8b 08 31 c0 45 01 cc 45 85 c9 74 09 41 6b c4 64 31 d2 <41> f7 f2 89 c2 44 29 fa 45 89 df 41 83 fb 0f 0f 87 c7 00 00 00 44 RSP: 0018:ffffd0a180d77588 EFLAGS: 00010246 RAX: 00000000ffffff38 RBX: ffff8d3d482ca000 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: ffffd0a180d77660 RBP: ffffd0a180d77690 R08: ffff8d3d482ca2d8 R09: 00000000fffffffe R10: 0000000000000000 R11: 0000000000000000 R12: 00000000ffffffe R13: ffff8d3d472f2000 R14: 0000000000000003 R15: 0000000000000000 FS: 00007f440b6c2740(0000) GS:ffff8d3dc9803000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000003cdd2000 CR3: 0000000007b58002 CR4: 0000000000172ef0 Call Trace: <TASK> ets_qdisc_change+0x870/0xf40 [sch_ets] qdisc_create+0x12b/0x540 tc_modify_qdisc+0x6d7/0xbd0 rtnetlink_rcv_msg+0x168/0x6b0 netlink_rcv_skb+0x5c/0x110 netlink_unicast+0x1d6/0x2b0 netlink_sendmsg+0x22e/0x470 ____sys_sendmsg+0x38a/0x3c0 ___sys_sendmsg+0x99/0xe0 __sys_sendmsg+0x8a/0xf0 do_syscall_64+0x111/0xf80 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f440b81c77e Code: 4d 89 d8 e8 d4 bc 00 00 4c 8b 5d f8 41 8b 93 08 03 00 00 59 5e 48 83 f8 fc 74 11 c9 c3 0f 1f 80 00 00 00 00 48 8b 45 10 0f 05 <c9> c3 83 e2 39 83 fa 08 75 e7 e8 13 ff ff ff 0f 1f 00 f3 0f 1e fa RSP: 002b:00007fff951e4c10 EFLAGS: 00000202 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 0000000000481820 RCX: 00007f440b81c77e RDX: 0000000000000000 RSI: 00007fff951e4cd0 RDI: 0000000000000003 RBP: 00007fff951e4c20 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000202 R12: 00007fff951f4fa8 R13: 00000000699ddede R14: 00007f440bb01000 R15: 0000000000486980 </TASK> Modules linked in: sch_ets(E) netdevsim(E) ---[end trace 0000000000000000]--- RIP: 0010:ets_offload_change+0x11f/0x290 [sch_ets] Code: e4 45 31 ff eb 03 41 89 c7 41 89 cb 89 ce 83 f9 0f 0f 87 b7 00 00 00 45 8b 08 31 c0 45 01 cc 45 85 c9 74 09 41 6b c4 64 31 d2 <41> f7 f2 89 c2 44 29 fa 45 89 df 41 83 fb 0f 0f 87 c7 00 00 00 44 RSP: 0018:ffffd0a180d77588 EFLAGS: 00010246 RAX: 00000000ffffff38 RBX: ffff8d3d482ca000 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: ffffd0a180d77660 RBP: ffffd0a180d77690 R08: ffff8d3d482ca2d8	N/A	More Details

	R09: 00000000fffffffe R10: 0000000000000000 R11: 0000000000000000 R12: 00000000fffffffe R13: ffff8d3d472f2000 R14: 0000000000000003 R15: 0000000000000000 FS: 00007f440b6c2740(0000) GS:ffff8d3dc9803000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000003cdd2000 CR3: 0000000007b58002 CR4: 0000000000172ef0 Kernel panic - not syncing: Fatal exception Kernel Offset: 0x30000000 from 0xffffffff81000000 (relocation range: 0xffffffff80000000-0xffffffffbfffffff) ---[end Kernel panic - not syncing: Fatal exception]--- Fix this using 64-bit integers for 'q_sum' and 'q_psum'.		
CVE-2026-23380	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix WARN_ON in tracing_buffers_mmap_close When a process forks, the child process copies the parent's VMAs but the user_mapped reference count is not incremented. As a result, when both the parent and child processes exit, tracing_buffers_mmap_close() is called twice. On the second call, user_mapped is already 0, causing the function to return -ENODEV and triggering a WARN_ON. Normally, this isn't an issue as the memory is mapped with VM_DONTCOPY set. But this is only a hint, and the application can call madvise(MADVISE_DOFORK) which resets the VM_DONTCOPY flag. When the application does that, it can trigger this issue on fork. Fix it by incrementing the user_mapped reference count without re-mapping the pages in the VMA's open callback.	N/A	More Details
CVE-2026-23381	In the Linux kernel, the following vulnerability has been resolved: net: bridge: fix nd_tbl NULL dereference when IPv6 is disabled When booting with the 'ipv6.disable=1' parameter, the nd_tbl is never initialized because inet6_init() exits before ndisc_init() is called which initializes it. Then, if neigh_suppress is enabled and an ICMPv6 Neighbor Discovery packet reaches the bridge, br_do_suppress_nd() will dereference ipv6_stub->nd_tbl which is NULL, passing it to neigh_lookup(). This causes a kernel NULL pointer dereference. BUG: kernel NULL pointer dereference, address: 0000000000000268 Oops: 0000 [#1] PREEMPT SMP NOPTI [...] RIP: 0010:neigh_lookup+0x16/0xe0 [...] Call Trace: <IRQ> ? neigh_lookup+0x16/0xe0 br_do_suppress_nd+0x160/0x290 [bridge] br_handle_frame_finish+0x500/0x620 [bridge] br_handle_frame+0x353/0x440 [bridge] __netif_receive_skb_core.constprop.0+0x298/0x1110 __netif_receive_skb_one_core+0x3d/0xa0 process_backlog+0xa0/0x140 __napi_poll+0x2c/0x170 net_rx_action+0x2c4/0x3a0 handle_softirqs+0xd0/0x270 do_softirq+0x3f/0x60 Fix this by replacing IS_ENABLED(IPV6) call with ipv6_mod_enabled() in the callers. This is in essence disabling NS/NA suppression when IPv6 is disabled.	N/A	More Details
CVE-2026-23382	In the Linux kernel, the following vulnerability has been resolved: HID: Add HID_CLAIMED_INPUT guards in raw_event callbacks missing them In commit 2ff5baa9b527 ("HID: appleir: Fix potential NULL dereference at raw event handle"), we handle the fact that raw event callbacks can happen even for a HID device that has not been "claimed" causing a crash if a broken device were attempted to be connected to the system. Fix up the remaining in-tree HID drivers that forgot to add this same check to resolve the same issue.	N/A	More Details
CVE-2026-23383	In the Linux kernel, the following vulnerability has been resolved: bpf, arm64: Force 8-byte alignment for JIT buffer to prevent atomic tearing struct bpf_plt contains a u64 target field. Currently, the BPF JIT allocator requests an alignment of 4 bytes (sizeof(u32)) for the JIT buffer. Because the base address of the JIT buffer can be 4-byte aligned (e.g., ending in 0x4 or 0xc), the relative padding logic in build_plt() fails to ensure that target lands on an 8-byte boundary. This leads to two issues: 1. UBSAN reports misaligned-access warnings when dereferencing the structure. 2. More critically, target is updated concurrently via WRITE_ONCE() in bpf_arch_text_poke() while the JIT'd code executes ldr. On arm64, 64-bit loads/stores are only guaranteed to be single-copy atomic if they are 64-bit aligned. A misaligned target risks a torn read, causing the JIT to jump to a corrupted address. Fix this by increasing the allocation alignment requirement to 8 bytes (sizeof(u64)) in bpf_jit_binary_pack_alloc(). This anchors the base of the JIT buffer to an 8-byte boundary, allowing the relative padding math in build_plt() to correctly align the target field.	N/A	More Details
CVE-2026-23384	In the Linux kernel, the following vulnerability has been resolved: RDMA/ionic: Fix kernel stack leak in ionic_create_cq() struct ionic_cq_resp resp { __u32 cqid[2]; // offset 0 - PARTIALLY SET (see below) __u8 udma_mask; // offset 8 - SET (resp.udma_mask = vcq->udma_mask) __u8 rsvd[7]; // offset 9 - NEVER SET <- LEAK }; rsvd[7]: 7 bytes of stack memory leaked unconditionally. cqid[2]: The loop at line 1256 iterates over udma_idx but skips indices where !(vcq->udma_mask & BIT(udma_idx)). The array has 2 entries but udma_count could be 1, meaning cqid[1] might never be written via ionic_create_cq_common(). If udma_mask only has bit 0 set, cqid[1] (4 bytes) is also leaked. So potentially 11 bytes leaked.	N/A	More Details
CVE-2026-23385	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: clone set on flush only Syzbot with fault injection triggered a failing memory allocation with GFP_KERNEL which results in a WARN splat: iter.err WARNING: net/netfilter/nf_tables_api.c:845 at nft_map_deactivate+0x34e/0x3c0 net/netfilter/nf_tables_api.c:845, CPU#0: syz.0.17/5992 Modules linked in: CPU: 0 UID: 0 PID: 5992 Comm: syz.0.17 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 02/12/2026 RIP: 0010:nft_map_deactivate+0x34e/0x3c0 net/netfilter/nf_tables_api.c:845 Code: 8b 05 86 5a 4e 09 48 3b 84 24 a0 00 00 00 75 62 48 8d 65 d8 5b 41 5c 41 5d 41 5e 41 5f 5d c3 cc cc cc cc cc e8 63 6d fa f7 90 <0f> 0b 90 43 +80 7c 35 00 00 0f 85 23 fe ff ff e9 26 fe ff ff 89 d9 RSP: 0018:ffffc900045af780 EFLAGS: 00010293 RAX: ffffffff89ca45bd RBX: 00000000ffffffff4 RCX: ffff888028111e40 RDX: 0000000000000000 RSI: 00000000ffffffff4 RDI: 0000000000000000 RBP: ffffc900045af870 R08: 0000000000400dc0 R09: 00000000ffffffff R10: dffffc0000000000 R11: fffffbfff1d141db R12: ffffc900045af7e0 R13: 1ffff920008b5f24 R14: dffffc0000000000 R15: ffffc900045af920 FS: 000055557a6a5500(0000) GS:ffff888125496000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fb5ea271fc0 CR3: 000000003269e000 CR4: 00000000003526f0 Call Trace: <TASK> __nft_release_table+0xceb/0x11f0 net/netfilter/nf_tables_api.c:12115 nft_rcv_nl_event+0xc25/0xdb0 net/netfilter/nf_tables_api.c:12187 notifier_call_chain+0x19d/0x3a0 kernel/notifier.c:85 blocking_notifier_call_chain+0x6a/0x90 kernel/notifier.c:380 netlink_release+0x123b/0x1ad0 net/netlink/af_netlink.c:761 __sock_release net/socket.c:662 [inline] sock_close+0xc3/0x240 net/socket.c:1455 Restrict set clone to the flush set command in the preparation phase. Add NFT_ITER_UPDATE_CLONE and use it for this purpose, update the rbtree and pipapo backends to only clone the set when this iteration type is used. As for the existing NFT_ITER_UPDATE type, update the pipapo backend to use the existing set clone if available, otherwise use the existing set representation. After this update, there is no need to clone a set that is being deleted, this includes bound anonymous set. An alternative approach to NFT_ITER_UPDATE_CLONE is to add a .clone interface and call it from the flush set path.	N/A	More Details
CVE-2026-23386	In the Linux kernel, the following vulnerability has been resolved: gve: fix incorrect buffer cleanup in gve_tx_clean_pending_packets for QPL In DQ-QPL mode, gve_tx_clean_pending_packets() incorrectly uses the RDA buffer cleanup path. It iterates num_bufs times and attempts to unmap entries in the dma array. This leads to two issues: 1. The dma array shares storage with tx_qpl_buf_ids (union). Interpreting buffer IDs as DMA addresses results in attempting to unmap incorrect memory locations. 2. num_bufs in QPL mode (counting 2K chunks) can significantly exceed the size of the dma array, causing out-of-bounds access warnings (trace below is how we noticed this issue). UBSAN: array-index-out-of-bounds in drivers/net/ethernet/drivers/net/ethernet/google/gve/gve_tx_dqo.c:178:5 index 18 is out of range for type 'dma_addr_t[18]' (aka 'unsigned long long[18]') Workqueue: gve gve_service_task [gve] Call Trace: <TASK> dump_stack_lvl+0x33/0xa0 __ubsan_handle_out_of_bounds+0xdc/0x110 gve_tx_stop_ring_dqo+0x182/0x200 [gve] gve_close+0x1be/0x450 [gve] gve_reset+0x99/0x120 [gve] gve_service_task+0x61/0x100 [gve] process_scheduled_works+0x1e9/0x380 Fix this by properly checking for QPL mode and delegating to gve_free_tx_qpl_bufs() to reclaim the buffers.	N/A	More Details
CVE-2026-23388	In the Linux kernel, the following vulnerability has been resolved: Squashfs: check metadata block offset is within range Syzkaller reports a "general protection fault in squashfs_copy_data" This is ultimately caused by a corrupted index look-up table, which produces a negative metadata block offset. This is subsequently passed to squashfs_copy_data (via squashfs_read_metadata) where the negative offset causes an out of bounds access. The fix is to check that the offset is within range in squashfs_read_metadata. This will trap this and other cases.	N/A	More Details
CVE-2025-2535	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details

CVE-2026-23389	In the Linux kernel, the following vulnerability has been resolved: ice: Fix memory leak in ice_set_ringparam() In ice_set_ringparam, tx_rings and xdp_rings are allocated before rx_rings. If the allocation of rx_rings fails, the code jumps to the done label leaking both tx_rings and xdp_rings. Furthermore, if the setup of an individual Rx ring fails during the loop, the code jumps to the free_tx label which releases tx_rings but leaks xdp_rings. Fix this by introducing a free_xdp label and updating the error paths to ensure both xdp_rings and tx_rings are properly freed if rx_rings allocation or setup fails. Compile tested only. Issue found using a prototype static analysis tool and code review.	N/A	More Details
CVE-2026-23390	In the Linux kernel, the following vulnerability has been resolved: tracing/dma: Cap dma_map_sg tracepoint arrays to prevent buffer overflow The dma_map_sg tracepoint can trigger a perf buffer overflow when tracing large scatter-gather lists. With devices like virtio-gpu creating large DRM buffers, nents can exceed 1000 entries, resulting in: phys_addrs: 1000 * 8 bytes = 8,000 bytes dma_addrs: 1000 * 8 bytes = 8,000 bytes lengths: 1000 * 4 bytes = 4,000 bytes Total: ~20,000 bytes This exceeds PERF_MAX_TRACE_SIZE (8192 bytes), causing: WARNING: CPU: 0 PID: 5497 at kernel/trace/trace_event_perf.c:405 perf buffer not large enough, wanted 24620, have 8192 Cap all three dynamic arrays at 128 entries using min() in the array size calculation. This ensures arrays are only as large as needed (up to the cap), avoiding unnecessary memory allocation for small operations while preventing overflow for large ones. The tracepoint now records the full nents/ents counts and a truncated flag so users can see when data has been capped. Changes in v2: - Use min(nents, DMA_TRACE_MAX_ENTRIES) for dynamic array sizing instead of fixed DMA_TRACE_MAX_ENTRIES allocation (feedback from Steven Rostedt) - This allocates only what's needed up to the cap, avoiding waste for small operations Reviwed-by: Sean Anderson <sean.anderson@linux.dev>	N/A	More Details
CVE-2026-23391	In the Linux kernel, the following vulnerability has been resolved: netfilter: xt_CT: drop pending enqueued packets on template removal Templates refer to objects that can go away while packets are sitting in nfqueue refer to: - helper, this can be an issue on module removal. - timeout policy, nfnetlink_cttimeout might remove it. The use of templates with zone and event cache filter are safe, since this just copies values. Flush these enqueued packets in case the template rule gets removed.	N/A	More Details
CVE-2026-23392	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: release flowtable after rcu grace period on error Call synchronize_rcu() after unregistering the hooks from error path, since a hook that already refers to this flowtable can be already registered, exposing this flowtable to packet path and nfnetlink_hook control plane. This error path is rare, it should only happen by reaching the maximum number hooks or by failing to set up to hardware offload, just call synchronize_rcu(). There is a check for already used device hooks by different flowtable that could result in EEXIST at this late stage. The hook parser can be updated to perform this check earlier to this error path really becomes rarely exercised. Uncovered by KASAN reported as use-after-free from nfnetlink_hook path when dumping hooks.	N/A	More Details
CVE-2025-15381	In the latest version of mlflow/mlflow, when the `basic-auth` app is enabled, tracing and assessment endpoints are not protected by permission validators. This allows any authenticated user, including those with `NO_PERMISSIONS` on the experiment, to read trace information and create assessments for traces they should not have access to. This vulnerability impacts confidentiality by exposing trace metadata and integrity by allowing unauthorized creation of assessments. Deployments using `mlflow server --app-name=basic-auth` are affected.	N/A	More Details
CVE-2026-23393	In the Linux kernel, the following vulnerability has been resolved: bridge: cfm: Fix race condition in peer_mep deletion When a peer MEP is being deleted, cancel_delayed_work_sync() is called on ccm_rx_dwork before freeing. However, br_cfm_frame_rx() runs in softirq context under rcu_read_lock (without RTNL) and can re-schedule ccm_rx_dwork via ccm_rx_timer_start() between cancel_delayed_work_sync() returning and kfree_rcu() being called. The following is a simple race scenario: cpu0 cpu1 mep_delete_implementation() cancel_delayed_work_sync(ccm_rx_dwork); br_cfm_frame_rx() // peer_mep still in hlist if (peer_mep->ccm_defect) ccm_rx_timer_start() queue_delayed_work(ccm_rx_dwork) hlist_del_rcu(&peer_mep->head); kfree_rcu(peer_mep, rcu); ccm_rx_work_expired() // on freed peer_mep To prevent this, cancel_delayed_work_sync() is replaced with disable_delayed_work_sync() in both peer MEP deletion paths, so that subsequent queue_delayed_work() calls from br_cfm_frame_rx() are silently rejected. The cc_peer_disable() helper retains cancel_delayed_work_sync() because it is also used for the CC enable/disable toggle path where the work must remain re-schedulable.	N/A	More Details
CVE-2026-23394	In the Linux kernel, the following vulnerability has been resolved: af_unix: Give up GC if MSG_PEEK intervened. Igor Ushakov reported that GC purged the receive queue of an alive socket due to a race with MSG_PEEK with a nice repro. This is the exact same issue previously fixed by commit cbcf01128d0a ("af_unix: fix garbage collect vs MSG_PEEK"). After GC was replaced with the current algorithm, the cited commit removed the locking dance in unix_peek_fds() and reintroduced the same issue. The problem is that MSG_PEEK bumps a file refcount without interacting with GC. Consider an SCC containing sk-A and sk-B, where sk-A is close()d but can be recv()ed via sk-B. The bad thing happens if sk-A is recv()ed with MSG_PEEK from sk-B and sk-B is close()d while GC is checking unix_vertex_dead() for sk-A and sk-B. GC thread User thread ---------- ---------- unix_vertex_dead(sk-A) -> true <------. \ `------ recv(sk-B, MSG_PEEK) invalidate !! -> sk-A's file refcount : 1 -> 2 close(sk-B) -> sk-B's file refcount : 2 -> 1 unix_vertex_dead(sk-B) -> true Initially, sk-A's file refcount is 1 by the inflight fd in sk-B recvq. GC thinks sk-A is dead because the file refcount is the same as the number of its inflight fds. However, sk-A's file refcount is bumped silently by MSG_PEEK, which invalidates the previous evaluation. At this moment, sk-B's file refcount is 2; one by the open fd, and one by the inflight fd in sk-A. The subsequent close() releases one refcount by the former. Finally, GC incorrectly concludes that both sk-A and sk-B are dead. One option is to restore the locking dance in unix_peek_fds(), but we can resolve this more elegantly thanks to the new algorithm. The point is that the issue does not occur without the subsequent close() and we actually do not need to synchronise MSG_PEEK with the dead SCC detection. When the issue occurs, close() and GC touch the same file refcount. If GC sees the refcount being decremented by close(), it can just give up garbage-collecting the SCC. Therefore, we only need to signal the race during MSG_PEEK with a proper memory barrier to make it visible to the GC. Let's use seqcount_t to notify GC when MSG_PEEK occurs and let it defer the SCC to the next run. This way no locking is needed on the MSG_PEEK side, and we can avoid imposing a penalty on every MSG_PEEK unnecessarily. Note that we can retry within unix_scc_dead() if MSG_PEEK is detected, but we do not do so to avoid hung task splat from abusive MSG_PEEK calls.	N/A	More Details
CVE-2026-23395	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix accepting multiple L2CAP_ECRED_CONN_REQ Currently the code attempts to accept requests regardless of the command identifier which may cause multiple requests to be marked as pending (FLAG_DEFER_SETUP) which can cause more than L2CAP_ECRED_MAX_CID(5) to be allocated in l2cap_ecred_rsp_defer causing an overflow. The spec is quite clear that the same identifier shall not be used on subsequent requests: 'Within each signaling channel a different Identifier shall be used for each successive request or indication.' https://www.bluetooth.com/wp-content/uploads/Files/Specification/HTML/Core-62/out/en/host/logical-link-control-and-adaptation-protocol-specification.html#UUID-32a25a06-4aa4-c6c7-77c5-dcfe3682355d So this attempts to check if there are any channels pending with the same identifier and rejects if any are found.	N/A	More Details
CVE-2026-31788	In the Linux kernel, the following vulnerability has been resolved: xen/privcmd: restrict usage in unprivileged domU The Xen privcmd driver allows to issue arbitrary hypercalls from user space processes. This is normally no problem, as access is usually limited to root and the hypervisor will deny any hypercalls affecting other domains. In case the guest is booted using secure boot, however, the privcmd driver would be enabling a root user process to modify e.g. kernel memory contents, thus breaking the secure boot feature. The only known case where an unprivileged domU is really needing to use the privcmd driver is the case when it is acting as the device model for another guest. In this case all hypercalls issued via the privcmd driver will target that other guest. Fortunately the privcmd driver can already be locked down to allow only hypercalls targeting a specific domain, but this mode can be activated from user land only today. The target domain can be obtained from Xenstore, so when not running in dom0 restrict the privcmd driver to that target domain from the beginning, resolving the potential problem of breaking secure boot. This is XSA-482 --- V2: - defer reading from Xenstore if Xenstore isn't ready yet (Jan Beulich) - wait in open() if target domain isn't known yet - issue message in case no target domain found (Jan Beulich)	N/A	More Details
CVE-2026-	From Panorama Web HMI, an attacker can gain read access to certain Web HMI server files, if he knows their paths and if these files are accessible to the Servin process execution account. * Installations based on Panorama Suite 2022-SP1 (22.50.005) are vulnerable unless update PS-2210-02-4079 (or higher) is installed * Installations based on Panorama Suite 2023 (23.00.004) are vulnerable unless updates PS-2300-03-3078 (or higher) and PS-2300-04-3078 (or higher) and PS-2300-82-3078 (or higher) are installed * Installations based on Panorama Suite 2025	N/A	More

4760	(25.00.016) are vulnerable unless updates PS-2500-02-1078 (or higher) and PS-2500-04-1078 (or higher) are installed * Installations based on Panorama Suite 2025 Updated Dec. 25 (25.10.007) are vulnerable unless updates PS-2510-02-1077 (or higher) and PS-2510-04-1077 (or higher) are installed Please refer to security bulletin BS-035, available on the Panorama CSIRT website: https://my.codra.net/en-gb/csirt .		Details
CVE-2026-23344	In the Linux kernel, the following vulnerability has been resolved: crypto: ccp - Fix use-after-free on error path In the error path of sev_tsm_init_locked(), the code dereferences 't' after it has been freed with kfree(). The pr_err() statement attempts to access t->tio_en and t->tio_init_done after the memory has been released. Move the pr_err() call before kfree(t) to access the fields while the memory is still valid. This issue reported by Smatch static analyser	N/A	More Details
CVE-2026-21712	A flaw in Node.js URL processing causes an assertion failure in native code when `url.format()` is called with a malformed internationalized domain name (IDN) containing invalid characters, crashing the Node.js process.	N/A	More Details
CVE-2026-23289	In the Linux kernel, the following vulnerability has been resolved: IB/mthca: Add missed mthca_unmap_user_db() for mthca_create_srq() Fix a user triggerable leak on the system call failure path.	N/A	More Details
CVE-2026-23309	In the Linux kernel, the following vulnerability has been resolved: tracing: Add NULL pointer check to trigger_data_free() If trigger_data_alloc() fails and returns NULL, event_hist_trigger_parse() jumps to the out_free error path. While kfree() safely handles a NULL pointer, trigger_data_free() does not. This causes a NULL pointer dereference in trigger_data_free() when evaluating data->cmd_ops->set_filter. Fix the problem by adding a NULL pointer check to trigger_data_free(). The problem was found by an experimental code review agent based on gemini-3.1-pro while reviewing backports into v6.18.y.	N/A	More Details
CVE-2026-4794	Multiple cross-site scripting (XSS) vulnerabilities in PaperCut NG/MF before 25.0.10 allow authenticated administrator users to inject arbitrary web script or HTML code via different UI fields. This could be used to compromise other admininistrator's sessions or perform unauthorized actions via the administrator's authenticated context (e.g. requires an active login session).	N/A	More Details
CVE-2026-23310	In the Linux kernel, the following vulnerability has been resolved: bpf/bonding: reject vlan+srcmac xmit_hash_policy change when XDP is loaded bond_option_mode_set() already rejects mode changes that would make a loaded XDP program incompatible via bond_xdp_check(). However, bond_option_xmit_hash_policy_set() has no such guard. For 802.3ad and balance-xor modes, bond_xdp_check() returns false when xmit_hash_policy is vlan+srcmac, because the 802.1q payload is usually absent due to hardware offload. This means a user can: 1. Attach a native XDP program to a bond in 802.3ad/balance-xor mode with a compatible xmit_hash_policy (e.g. layer2+3). 2. Change xmit_hash_policy to vlan+srcmac while XDP remains loaded. This leaves bond->xdp_prog set but bond_xdp_check() now returning false for the same device. When the bond is later destroyed, dev_xdp_uninstall() calls bond_xdp_set(dev, NULL, NULL) to remove the program, which hits the bond_xdp_check() guard and returns -EOPNOTSUPP, triggering: WARN_ON(dev_xdp_install(dev, mode, bpf_op, NULL, 0, NULL)) Fix this by rejecting xmit_hash_policy changes to vlan+srcmac when an XDP program is loaded on a bond in 802.3ad or balance-xor mode. commit 39a0876d595b ("net, bonding: Disallow vlan+srcmac with XDP") introduced bond_xdp_check() which returns false for 802.3ad/balance-xor modes when xmit_hash_policy is vlan+srcmac. The check was wired into bond_xdp_set() to reject XDP attachment with an incompatible policy, but the symmetric path -- preventing xmit_hash_policy from being changed to an incompatible value after XDP is already loaded -- was left unguarded in bond_option_xmit_hash_policy_set(). Note: commit 094ee6017ea0 ("bonding: check xdp prog when set bond mode") later added a similar guard to bond_option_mode_set(), but bond_option_xmit_hash_policy_set() remained unprotected.	N/A	More Details
CVE-2026-23311	In the Linux kernel, the following vulnerability has been resolved: perf/core: Fix invalid wait context in ctx_sched_in() Lockdep found a bug in the event scheduling when a pinned event was failed and wakes up the threads in the ring buffer like below. It seems it should not grab a wait-queue lock under perf-context lock. Let's do it with irq_work. [39.913691] ============================== [39.914157] [BUG: Invalid wait context] [39.914623] 6.15.0-next-20250530-next-2025053 #1 Not tainted [39.915271] ----------------------------- [39.915731] repro/837 is trying to lock: [39.916191] ffff88801acfabd8 (&event->waitq){....}-{3:3}, at: __wake_up+0x26/0x60 [39.917182] other info that might help us debug this: [39.917761] context-{5:5} [39.918079] 4 locks held by repro/837: [39.918530] #0: ffffffff8725cd00 (rcu_read_lock){....}-{1:3}, at: __perf_event_task_sched_in+0xd1/0xbc0 [39.919612] #1: ffff88806ca3c6f8 (&cpuctx_lock){....}-{2:2}, at: __perf_event_task_sched_in+0x1a7/0xbc0 [39.920748] #2: ffff88800d91fc18 (&ctx->lock){....}-{2:2}, at: __perf_event_task_sched_in+0x1f9/0xbc0 [39.921819] #3: ffffffff8725cd00 (rcu_read_lock){....}-{1:3}, at: perf_event_wakeup+0x6c/0x470	N/A	More Details
CVE-2026-30880	baserCMS is a website development framework. Prior to version 5.2.3, baserCMS has an OS command injection vulnerability in the installer. This issue has been patched in version 5.2.3.	N/A	More Details
CVE-2026-30879	baserCMS is a website development framework. Prior to version 5.2.3, baserCMS has a cross-site scripting vulnerability in blog posts. This issue has been patched in version 5.2.3.	N/A	More Details
CVE-2026-27697	baserCMS is a website development framework. Prior to version 5.2.3, baserCMS has a SQL injection vulnerability in blog posts. This issue has been patched in version 5.2.3.	N/A	More Details
CVE-2026-23312	In the Linux kernel, the following vulnerability has been resolved: net: usb: kaweth: validate USB endpoints The kaweth driver should validate that the device it is probing has the proper number and types of USB endpoints it is expecting before it binds to it. If a malicious device were to not have the same urbs the driver will crash later on when it blindly accesses these endpoints.	N/A	More Details
CVE-2026-23313	In the Linux kernel, the following vulnerability has been resolved: i40e: Fix preempt count leak in napi poll tracepoint Using get_cpu() in the tracepoint assignment causes an obvious preempt count leak because nothing invokes put_cpu() to undo it: softirq: huh, entered softirq 3 NET_RX with preempt_count 00000100, exited with 00000101? This clearly has seen a lot of testing in the last 3+ years... Use smp_processor_id() instead.	N/A	More Details
CVE-2026-23314	In the Linux kernel, the following vulnerability has been resolved: regulator: bq257xx: Fix device node reference leak in bq257xx_reg_dt_parse_gpio() In bq257xx_reg_dt_parse_gpio(), if fails to get subchild, it returns without calling of_node_put(child), causing the device node reference leak.	N/A	More Details
CVE-2026-23315	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: Fix possible oob access in mt76_connac2_mac_write_txwi_80211() Check frame length before accessing the mgmt fields in mt76_connac2_mac_write_txwi_80211 in order to avoid a possible oob access. [fix check to also cover mgmt->u.action.u.addba_req.capab, correct Fixes tag]	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: net: ipv4: fix ARM64 alignment fault in multipath hash seed `struct sysctl_fib_multipath_hash_seed` contains two u32 fields (user_seed and mp_seed), making it an 8-byte structure with a 4-byte alignment requirement. In `fib_multipath_hash_from_keys()`, the code evaluates the entire struct atomically via `READ_ONCE()`: mp_seed = READ_ONCE(net->ipv4.sysctl_fib_multipath_hash_seed).mp_seed; While this silently works on GCC by falling back to unaligned regular loads which the ARM64 kernel tolerates, it causes a fatal kernel panic when compiled with Clang and LTO enabled. Commit e35123d83ee3 ("arm64: lto: Strengthen READ_ONCE() to acquire when CONFIG_LTO=y") strengthens `READ_ONCE()` to use Load-Acquire instructions (`ldar` / `ldapr`)		

2026-23316	to prevent compiler reordering bugs under Clang LTO. Since the macro evaluates the full 8-byte struct, Clang emits a 64-bit `ldar` instruction. ARM64 architecture strictly requires `ldar` to be naturally aligned, thus executing it on a 4-byte aligned address triggers a strict Alignment Fault (FSC = 0x21). Fix the read side by moving the `READ_ONCE()` directly to the `u32` member, which emits a safe 32-bit `ldar Wn`. Furthermore, Eric Dumazet pointed out that `WRITE_ONCE()` on the entire struct in `proc_fib_multipath_hash_set_seed()` is also flawed. Analysis shows that Clang splits this 8-byte write into two separate 32-bit `str` instructions. While this avoids an alignment fault, it destroys atomicity and exposes a tear-write vulnerability. Fix this by explicitly splitting the write into two 32-bit `WRITE_ONCE()` operations. Finally, add the missing `READ_ONCE()` when reading `user_seed` in `proc_fib_multipath_hash_seed()` to ensure proper pairing and concurrency safety.	N/A	More Details
CVE-2026-1001	Domoticz versions prior to 2026.1 contain a stored cross-site scripting vulnerability in the Add Hardware and rename device functionality of the web interface that allows authenticated administrators to execute arbitrary scripts by supplying crafted names containing script or HTML markup. Attackers can inject malicious code that is stored and rendered without proper output encoding, causing script execution in the browsers of users viewing the affected page and enabling unauthorized actions within their session context.	N/A	More Details
CVE-2026-25099	Bludit’s API plugin allows an authenticated attacker with a valid API token to upload files of any type and extension without restriction, which can then be executed, leading to Remote Code Execution. This issue was fixed in 3.18.4.	N/A	More Details
CVE-2026-23318	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Use correct version for UAC3 header validation The entry of the validators table for UAC3 AC header descriptor is defined with the wrong protocol version UAC_VERSION_2, while it should have been UAC_VERSION_3. This results in the validator never matching for actual UAC3 devices (protocol == UAC_VERSION_3), causing their header descriptors to bypass validation entirely. A malicious USB device presenting a truncated UAC3 header could exploit this to cause out-of-bounds reads when the driver later accesses unvalidated descriptor fields. The bug was introduced in the same commit as the recently fixed UAC3 feature unit sub-type typo, and appears to be from the same copy-paste error when the UAC3 section was created from the UAC2 section.	N/A	More Details
CVE-2026-23319	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix a UAF issue in bpf_trampoline_link_cgroup_shim The root cause of this bug is that when 'bpf_link_put' reduces the refcount of 'shim_link->link.link' to zero, the resource is considered released but may still be referenced via 'tr->progs_hlist' in 'cgroup_shim_find'. The actual cleanup of 'tr->progs_hlist' in 'bpf_shim_tramp_link_release' is deferred. During this window, another process can cause a use-after-free via 'bpf_trampoline_link_cgroup_shim'. Based on Martin KaFai Lau's suggestions, I have created a simple patch. To fix this: Add an atomic non-zero check in 'bpf_trampoline_link_cgroup_shim'. Only increment the refcount if it is not already zero. Testing: I verified the fix by adding a delay in 'bpf_shim_tramp_link_release' to make the bug easier to trigger: static void bpf_shim_tramp_link_release(struct bpf_link *link) { /* ... */ if (!shim_link->trampoline) return; + msleep(100); WARN_ON_ONCE(bpf_trampoline_unlink_prog(&shim_link->link, shim_link->trampoline, NULL)); bpf_trampoline_put(shim_link->trampoline); } Before the patch, running a PoC easily reproduced the crash(almost 100%) with a call trace similar to KaiyanM's report. After the patch, the bug no longer occurs even after millions of iterations.	N/A	More Details
CVE-2026-25100	Bludit is vulnerable to Stored Cross-Site Scripting (XSS) in its image upload functionality. An authenticated attacker with content upload privileges (such as Author, Editor, or Administrator) can upload an SVG file containing a malicious payload, which is executed when a victim visits the URL of the uploaded resource. The uploaded resource itself is accessible without authentication. The vendor was notified early about this vulnerability, but stopped responding in the middle of coordination. All versions up to 3.18.2 are considered to be vulnerable, future versions might also be vulnerable.	N/A	More Details
CVE-2026-23320	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_ncm: align net_device lifecycle with bind/unbind Currently, the net_device is allocated in ncm_alloc_inst() and freed in ncm_free_inst(). This ties the network interface's lifetime to the configuration instance rather than the USB connection (bind/unbind). This decoupling causes issues when the USB gadget is disconnected where the underlying gadget device is removed. The net_device can outlive its parent, leading to dangling sysfs links and NULL pointer dereferences when accessing the freed gadget device. Problem 1: NULL pointer dereference on disconnect Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Call trace: __pi_strlen+0x14/0x150 rtnl_fill_ifinfo+0x6b4/0x708 rtmsg_ifinfo_build_skb+0xd8/0x13c rtmsg_ifinfo+0x50/0xa0 __dev_notify_flags+0x4c/0x1f0 dev_change_flags+0x54/0x70 do_setlink+0x390/0xebc rtnl_newlink+0x7d0/0xac8 rtnetlink_rcv_msg+0x27c/0x410 netlink_rcv_skb+0x134/0x150 rtnetlink_rcv+0x18/0x28 netlink_unicast+0x254/0x3f0 netlink_sendmsg+0x2e0/0x3d4 Problem 2: Dangling sysfs symlinks console:/ # ls -l /sys/class/net/ncm0 lrwxrwxrwx ... /sys/class/net/ncm0 -> /sys/devices/platform/.../gadget.0/net/ncm0 console:/ # ls -l /sys/devices/platform/.../gadget.0/net/ncm0 ls: .../gadget.0/net/ncm0: No such file or directory Move the net_device allocation to ncm_bind() and deallocation to ncm_unbind(). This ensures the network interface exists only when the gadget function is actually bound to a configuration. To support pre-bind configuration (e.g., setting interface name or MAC address via configfs), cache user-provided options in f_ncm_opts using the gether_opts structure. Apply these cached settings to the net_device upon creation in ncm_bind(). Preserve the use-after-free fix from commit 6334b8e4553c ("usb: gadget: f_ncm: Fix UAF ncm object at re-bind after usb ep transport error"). Check opts->net in ncm_set_alt() and ncm_disable() to ensure gether_disconnect() runs only if a connection was established.	N/A	More Details
CVE-2026-23321	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: in-kernel: always mark signal+subflow endp as used Syzkaller managed to find a combination of actions that was generating this warning: msk->pm.local_addr_used == 0 WARNING: net/mptcp/pm_kernel.c:1071 at __mark_subflow_endp_available net/mptcp/pm_kernel.c:1071 [inline], CPU#1: syz.2.17/961 WARNING: net/mptcp/pm_kernel.c:1071 at mptcp_nl_remove_subflow_and_signal_addr net/mptcp/pm_kernel.c:1103 [inline], CPU#1: syz.2.17/961 WARNING: net/mptcp/pm_kernel.c:1071 at mptcp_pm_nl_del_addr_doit+0x81d/0x8f0 net/mptcp/pm_kernel.c:1210, CPU#1: syz.2.17/961 Modules linked in: CPU: 1 UID: 0 PID: 961 Comm: syz.2.17 Not tainted 6.19.0-08368-gfafda3b4b06b #22 PREEMPT(full) Hardware name: QEMU Ubuntu 25.10 PC v2 (i440FX + PIIX, + 10.1 machine, 1996), BIOS 1.17.0-debian-1.17.0-1build1 04/01/2014 RIP: 0010:__mark_subflow_endp_available net/mptcp/pm_kernel.c:1071 [inline] RIP: 0010:mptcp_nl_remove_subflow_and_signal_addr net/mptcp/pm_kernel.c:1103 [inline] RIP: 0010:mptcp_pm_nl_del_addr_doit+0x81d/0x8f0 net/mptcp/pm_kernel.c:1210 Code: 89 c5 e8 46 30 6f fe e9 21 fd ff ff 49 83 ed 80 e8 38 30 6f fe 4c 89 ef be 03 00 00 00 e8 db 49 df fe eb ac e8 24 30 6f fe 90 <0f> 0b 90 e9 1d ff ff ff e8 16 30 6f fe eb 05 e8 0f 30 6f fe e8 9a RSP: 0018:ffffc90001663880 EFLAGS: 00010293 RAX: ffffffff82de1a6c RBX: 0000000000000000 RCX: ffff88800722b500 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffff8880158b22d0 R08: 0000000000010425 R09: ffffffffffffffff R10: ffffffff82de18ba R11: 0000000000000000 R12: ffff88800641a640 R13: ffff8880158b1880 R14: ffff88801ec3c900 R15: ffff88800641a650 FS: 00005555722c3500(0000) GS:ffff8880f909d000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f66346e0f60 CR3: 000000001607c000 CR4: 0000000000350ef0 Call Trace: <TASK> genl_family_rcv_msg_doit+0x117/0x180 net/netlink/genetlink.c:1115 genl_family_rcv_msg net/netlink/genetlink.c:1195 [inline] genl_rcv_msg+0x3a8/0x3f0 net/netlink/genetlink.c:1210 netlink_rcv_skb+0x16d/0x240 net/netlink/af_netlink.c:2550 genl_rcv+0x28/0x40 net/netlink/genetlink.c:1219 netlink_unicast_kernel net/netlink/af_netlink.c:1318 [inline] netlink_unicast+0x3e9/0x4c0 net/netlink/af_netlink.c:1344 netlink_sendmsg+0x4aa/0x5b0 net/netlink/af_netlink.c:1894 sock_sendmsg_nosec net/socket.c:727 [inline] __sock_sendmsg+0xc9/0xf0 net/socket.c:742 ____sys_sendmsg+0x272/0x3b0 net/socket.c:2592 ___sys_sendmsg+0x2de/0x320 net/socket.c:2646 __sys_sendmsg net/socket.c:2678 [inline] __do_sys_sendmsg net/socket.c:2683 [inline] __se_sys_sendmsg net/socket.c:2681 [inline] __x64_sys_sendmsg+0x110/0x1a0 net/socket.c:2681 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0x143/0x440 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f66346f826d Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 e8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffc83d8bdc8 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007f6634985fa0 RCX: 00007f66346f826d RDX: 00000000040000b0 RSI: 0000200000000740 RDI: 0000000000000007 RBP: 0000000000000000 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 00007f6634985fa8 R13:	N/A	More Details

	00007f6634985fac R14: 0000000000000000 R15: 0000000000001770 </TASK> The actions that caused that seem to be: - Set the MPTCP subflows limit to 0 - Create an MPTCP endpoint with both the 'signal' and 'subflow' flags - Create a new MPTCP connection from a different address: an ADD_ADDR linked to the MPTCP endpoint will be sent ('signal' flag), but no subflows is initiated ('subflow' flag) - Remove the MPTCP endpoint ---truncated---		
CVE-2026-23322	In the Linux kernel, the following vulnerability has been resolved: ipmi: Fix use-after-free and list corruption on sender error The analysis from Breno: When the SMI sender returns an error, smi_work() delivers an error response but then jumps back to restart without cleaning up properly: 1. intf->curr_msg is not cleared, so no new message is pulled 2. newmsg still points to the message, causing sender() to be called again with the same message 3. If sender() fails again, deliver_err_response() is called with the same recv_msg that was already queued for delivery This causes list_add corruption ("list_add double add") because the recv_msg is added to the user_msgs list twice. Subsequently, the corrupted list leads to use-after-free when the memory is freed and reused, and eventually a NULL pointer dereference when accessing recv_msg->done. The buggy sequence: sender() fails -> deliver_err_response(recv_msg) // recv_msg queued for delivery -> goto restart // curr_msg not cleared! sender() fails again (same message!) -> deliver_err_response(recv_msg) // tries to queue same recv_msg -> LIST CORRUPTION Fix this by freeing the message and setting it to NULL on a send error. Also, always free the newmsg on a send error, otherwise it will leak.	N/A	More Details
CVE-2026-33977	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.24.2, a malicious RDP server can crash the FreeRDP client by sending audio data in IMA ADPCM format with an invalid initial step index value (>= 89). The unvalidated step index is read directly from the network and used to index into a 89-entry lookup table, triggering a WINPR_ASSERT() failure and process abort via SIGABRT. This affects any FreeRDP client that has audio redirection (RDPSND) enabled, which is the default configuration. This issue has been patched in version 3.24.2.	N/A	More Details
CVE-2026-33952	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.24.2, an unvalidated auth_length field read from the network triggers a WINPR_ASSERT() failure in rts_read_auth_verifier_no_checks(), causing any FreeRDP client connecting through a malicious RDP Gateway to crash with SIGABRT. This is a pre-authentication denial of service affecting all FreeRDP clients using RPC-over-HTTP gateway transport. The assertion is active in default release builds (WITH_VERBOSE_WINPR_ASSERT=ON). This issue has been patched in version 3.24.2.	N/A	More Details
CVE-2026-23323	In the Linux kernel, the following vulnerability has been resolved: hwmon: (macsmc) Fix regressions in Apple Silicon SMC hwmon driver The recently added macsmc-hwmon driver contained several critical bugs in its sensor population logic and float conversion routines. Specifically: - The voltage sensor population loop used the wrong prefix ("volt-" instead of "voltage-") and incorrectly assigned sensors to the temperature sensor array (hwmon->temp.sensors) instead of the voltage sensor array (hwmon->volt.sensors). This would lead to out-of-bounds memory access or data corruption when both temperature and voltage sensors were present. - The float conversion in macsmc_hwmon_write_f32() had flawed exponent logic for values >= 2^24 and lacked masking for the mantissa, which could lead to incorrect values being written to the SMC. Fix these issues to ensure correct sensor registration and reliable manual fan control. Confirm that the reported overflow in FIELD_PREP is fixed by declaring macsmc_hwmon_write_f32() as __always_inline for a compile test.	N/A	More Details
CVE-2026-4789	Kyverno, versions 1.16.0 and later, are vulnerable to SSRF due to unrestricted CEL HTTP functions.	N/A	More Details
CVE-2026-5115	The PaperCut NG/MF (specifically, the embedded application for Konica Minolta devices) is vulnerable to session hijacking. The PaperCut NG/MF Embedded application is a software interface that runs directly on the touch screen of a multi-function device. It was internally discovered that the communication channel between the embedded application and the server was insecure, which could leak data including sensitive information that may be used to mount an attack on the device. Such an attack could potentially be used to steal data or to perform a phishing attack on the end user.	N/A	More Details
CVE-2026-23308	In the Linux kernel, the following vulnerability has been resolved: pinctrl: equilibrium: fix warning trace on load The callback functions 'eqbr_irq_mask()' and 'eqbr_irq_ack()' are also called in the callback function 'eqbr_irq_mask_ack()'. This is done to avoid source code duplication. The problem, is that in the function 'eqbr_irq_mask()' also calles the gpiolib function 'gpiochip_disable_irq()' This generates the following warning trace in the log for every gpio on load. [6.088111] ------------[cut here]------------ [6.092440] WARNING: CPU: 3 PID: 1 at drivers/gpio/gpiolib.c:3810 gpiochip_disable_irq+0x39/0x50 [6.097847] Modules linked in: [6.097847] CPU: 3 UID: 0 PID: 1 Comm: swapper/0 Tainted: G W 6.12.59+ #0 [6.097847] Tainted: [W]=WARN [6.097847] RIP: 0010:gpiochip_disable_irq+0x39/0x50 [6.097847] Code: 39 c6 48 19 c0 21 c6 48 c1 e6 05 48 03 b2 38 03 00 00 48 81 fe 00 f0 ff ff 77 11 48 8b 46 08 f6 c4 02 74 06 f0 80 66 09 fb c3 <0f> 0b 90 0f 1f 40 00 c3 66 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 [6.097847] RSP: 0000:ffffc9000000b830 EFLAGS: 00010046 [6.097847] RAX: 0000000000000045 RBX: ffff888001be02a0 RCX: 0000000000000008 [6.097847] RDX: ffff888001be9000 RSI: ffff888001b2dd00 RDI: ffff888001be02a0 [6.097847] RBP: ffffc9000000b860 R08: 0000000000000000 R09: 0000000000000000 [6.097847] R10: 0000000000000001 R11: ffff888001b2a154 R12: ffff888001be0514 [6.097847] R13: ffff888001be02a0 R14: 0000000000000008 R15: 0000000000000000 [6.097847] FS: 0000000000000000(0000) GS:ffff888041d80000(0000) knlGS:0000000000000000 [6.097847] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [6.097847] CR2: 0000000000000000 CR3: 0000000003030000 CR4: 00000000001026b0 [6.097847] Call Trace: [6.097847] <TASK> [6.097847] ? eqbr_irq_mask+0x63/0x70 [6.097847] ? no_action+0x10/0x10 [6.097847] eqbr_irq_mask_ack+0x11/0x60 In an other driver (drivers/pinctrl/starfive/pinctrl-starfive-jh7100.c) the interrupt is not disabled here. To fix this, do not call the 'eqbr_irq_mask()' and 'eqbr_irq_ack()' function. Implement instead this directly without disabling the interrupts.	N/A	More Details
CVE-2026-23342	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix race in cpumap on PREEMPT_RT On PREEMPT_RT kernels, the per-CPU xdp_bulk_queue (bq) can be accessed concurrently by multiple preemptible tasks on the same CPU. The original code assumes bq_enqueue() and __cpu_map_flush() run atomically with respect to each other on the same CPU, relying on local_bh_disable() to prevent preemption. However, on PREEMPT_RT, local_bh_disable() only calls migrate_disable() (when PREEMPT_RT_NEEDS_BH_LOCK is not set) and does not disable preemption, which allows CFS scheduling to preempt a task during bq_flush_to_queue(), enabling another task on the same CPU to enter bq_enqueue() and operate on the same per-CPU bq concurrently. This leads to several races: 1. Double __list_del_clearprev(): after bq->count is reset in bq_flush_to_queue(), a preempting task can call bq_enqueue() -> bq_flush_to_queue() on the same bq when bq->count reaches CPU_MAP_BULK_SIZE. Both tasks then call __list_del_clearprev() on the same bq->flush_node, the second call dereferences the prev pointer that was already set to NULL by the first. 2. bq->count and bq->q[] races: concurrent bq_enqueue() can corrupt the packet queue while bq_flush_to_queue() is processing it. The race between task A (__cpu_map_flush -> bq_flush_to_queue) and task B (bq_enqueue -> bq_flush_to_queue) on the same CPU: Task A (xdp_do_flush) Task B (cpu_map_enqueue) ---------- ---------- bq_flush_to_queue(bq) spin_lock(&q->producer_lock) /* flush bq->q[] to ptr_ring */ bq->count = 0 spin_unlock(&q->producer_lock) bq_enqueue(rcpu, xdpf) <-- CFS preempts Task A --> bq->q[bq->count++] = xdpf /* ... more enqueues until full ... */ bq_flush_to_queue(bq) spin_lock(&q->producer_lock) /* flush to ptr_ring */ spin_unlock(&q->producer_lock) __list_del_clearprev(flush_node) /* sets flush_node.prev = NULL */ <-- Task A resumes --> __list_del_clearprev(flush_node) flush_node.prev->next = ... /* prev is NULL -> kernel oops */ Fix this by adding a local_lock_t to xdp_bulk_queue and acquiring it in bq_enqueue() and __cpu_map_flush(). These paths already run under local_bh_disable(), so use local_lock_nested_bh() which on non-RT is a pure annotation with no overhead, and on PREEMPT_RT provides a per-CPU sleeping lock that serializes access to the bq. To reproduce, insert an mdelay(100) between bq->count = 0 and __list_del_clearprev() in bq_flush_to_queue(), then run reproducer provided by syzkaller.	N/A	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: can: ems_usb: ems_usb_read_bulk_callback(): check the proper length of a message When looking at the data in a USB urb, the actual_length is the size of the buffer passed to the driver, not the transfer_buffer_length which is set by the driver as the max size of the buffer. When parsing the messages in ems_usb_read_bulk_callback() properly check the size	N/A	More Details

23307	both at the beginning of parsing the message to make sure it is big enough for the expected structure, and at the end of the message to make sure we don't overflow past the end of the buffer for the next message.		
CVE-2026-4263	Vulnerability of incorrect authorization in HiJiffy Chatbot allows an attacker to download private messages from other users via the parameter 'visitor' in '/api/v1/webchat/message'.	N/A	More Details
CVE-2026-4262	Vulnerability of incorrect authorization in HiJiffy Chatbot allows an attacker to download private messages from other users via the parameter 'ID' in '/api/v1/download/<ID>/'.	N/A	More Details
CVE-2026-23290	In the Linux kernel, the following vulnerability has been resolved: net: usb: pegasus: validate USB endpoints The pegasus driver should validate that the device it is probing has the proper number and types of USB endpoints it is expecting before it binds to it. If a malicious device were to not have the same urbs the driver will crash later on when it blindly accesses these endpoints.	N/A	More Details
CVE-2026-23291	In the Linux kernel, the following vulnerability has been resolved: nfc: pn533: properly drop the usb interface reference on disconnect When the device is disconnected from the driver, there is a "dangling" reference count on the usb interface that was grabbed in the probe callback. Fix this up by properly dropping the reference after we are done with it.	N/A	More Details
CVE-2026-23292	In the Linux kernel, the following vulnerability has been resolved: scsi: target: Fix recursive locking in __configfs_open_file() In flush_write_buffer, &p->frag_sem is acquired and then the loaded store function is called, which, here, is target_core_item_dbroot_store(). This function called filp_open(), following which these functions were called (in reverse order), according to the call trace: down_read __configfs_open_file do_dentry_open vfs_open do_open path_openat do_filp_open file_open_name filp_open target_core_item_dbroot_store flush_write_buffer configfs_write_iter target_core_item_dbroot_store() tries to validate the new file path by trying to open the file path provided to it; however, in this case, the bug report shows: db_root: not a directory: /sys/kernel/config/target/dbroot indicating that the same configfs file was tried to be opened, on which it is currently working on. Thus, it is trying to acquire frag_sem semaphore of the same file of which it already holds the semaphore obtained in flush_write_buffer(), leading to acquiring the semaphore in a nested manner and a possibility of recursive locking. Fix this by modifying target_core_item_dbroot_store() to use kern_path() instead of filp_open() to avoid opening the file using filesystem-specific function __configfs_open_file(), and further modifying it to make this fix compatible.	N/A	More Details
CVE-2026-23293	In the Linux kernel, the following vulnerability has been resolved: net: vxlan: fix nd_tbl NULL dereference when IPv6 is disabled When booting with the 'ipv6.disable=1' parameter, the nd_tbl is never initialized because inet6_init() exits before ndisc_init() is called which initializes it. If an IPv6 packet is injected into the interface, route_shortcircuit() is called and a NULL pointer dereference happens on neigh_lookup(). BUG: kernel NULL pointer dereference, address: 0000000000000380 Oops: Oops: 0000 [#1] SMP NOPTI [...] RIP: 0010:neigh_lookup+0x20/0x270 [...] Call Trace: <TASK> vxlan_xmit+0x638/0x1ef0 [vxlan] dev_hard_start_xmit+0x9e/0x2e0 __dev_queue_xmit+0xbee/0x14e0 packet_sendmsg+0x116f/0x1930 __sys_sendto+0x1f5/0x200 __x64_sys_sendto+0x24/0x30 do_syscall_64+0x12f/0x1590 entry_SYSCALL_64_after_hwframe+0x76/0x7e Fix this by adding an early check on route_shortcircuit() when protocol is ETH_P_IPV6. Note that ipv6_mod_enabled() cannot be used here because VXLAN can be built-in even when IPv6 is built as a module.	N/A	More Details
CVE-2026-23294	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix race in devmap on PREEMPT_RT On PREEMPT_RT kernels, the per-CPU xdp_dev_bulk_queue (bq) can be accessed concurrently by multiple preemptible tasks on the same CPU. The original code assumes bq_enqueue() and __dev_flush() run atomically with respect to each other on the same CPU, relying on local_bh_disable() to prevent preemption. However, on PREEMPT_RT, local_bh_disable() only calls migrate_disable() (when PREEMPT_RT_NEEDS_BH_LOCK is not set) and does not disable preemption, which allows CFS scheduling to preempt a task during bq_xmit_all(), enabling another task on the same CPU to enter bq_enqueue() and operate on the same per-CPU bq concurrently. This leads to several races: 1. Double-free / use-after-free on bq->q[]: bq_xmit_all() snapshots cnt = bq->count, then iterates bq->q[0..cnt-1] to transmit frames. If preempted after the snapshot, a second task can call bq_enqueue() -> bq_xmit_all() on the same bq, transmitting (and freeing) the same frames. When the first task resumes, it operates on stale pointers in bq->q[], causing use-after-free. 2. bq->count and bq->q[] corruption: concurrent bq_enqueue() modifying bq->count and bq->q[] while bq_xmit_all() is reading them. 3. dev_rx/xdp_prog teardown race: __dev_flush() clears bq->dev_rx and bq->xdp_prog after bq_xmit_all(). If preempted between bq_xmit_all() return and bq->dev_rx = NULL, a preempting bq_enqueue() sees dev_rx still set (non-NULL), skips adding bq to the flush_list, and enqueues a frame. When __dev_flush() resumes, it clears dev_rx and removes bq from the flush_list, orphaning the newly enqueued frame. 4. __list_del_clearprev() on flush_node: similar to the cpumap race, both tasks can call __list_del_clearprev() on the same flush_node, the second dereferences the prev pointer already set to NULL. The race between task A (__dev_flush -> bq_xmit_all) and task B (bq_enqueue -> bq_xmit_all) on the same CPU: Task A (xdp_do_flush) Task B (ndo_xdp_xmit redirect) ---------- ---------- __dev_flush(flush_list) bq_xmit_all(bq) cnt = bq->count /* e.g. 16 */ /* start iterating bq->q[] */ <-- CFS preempts Task A --> bq_enqueue(dev, xdpf) bq->count == DEV_MAP_BULK_SIZE bq_xmit_all(bq, 0) cnt = bq->count /* same 16! */ ndo_xdp_xmit(bq->q[]) /* frames freed by driver */ bq->count = 0 <-- Task A resumes --> ndo_xdp_xmit(bq->q[]) /* use-after-free: frames already freed! */ Fix this by adding a local_lock_t to xdp_dev_bulk_queue and acquiring it in bq_enqueue() and __dev_flush(). These paths already run under local_bh_disable(), so use local_lock_nested_bh() which on non-RT is a pure annotation with no overhead, and on PREEMPT_RT provides a per-CPU sleeping lock that serializes access to the bq.	N/A	More Details
CVE-2026-23295	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Fix dead lock for suspend and resume When an application issues a query IOCTL while auto suspend is running, a deadlock can occur. The query path holds dev_lock and then calls pm_runtime_resume_and_get(), which waits for the ongoing suspend to complete. Meanwhile, the suspend callback attempts to acquire dev_lock and blocks, resulting in a deadlock. Fix this by releasing dev_lock before calling pm_runtime_resume_and_get() and reacquiring it after the call completes. Also acquire dev_lock in the resume callback to keep the locking consistent.	N/A	More Details
CVE-2026-23296	In the Linux kernel, the following vulnerability has been resolved: scsi: core: Fix refcount leak for tagset_refcnt This leak will cause a hang when tearing down the SCSI host. For example, iscsid hangs with the following call trace: [130120.652718] scsi_alloc_sdev: Allocation failure during SCSI scanning, some SCSI devices might not be configured PID: 2528 TASK: ffff9d0408974e00 CPU: 3 COMMAND: "iscsid" #0 [ffffb5b9c134b9e0] __schedule at ffffffff860657d4 #1 [ffffb5b9c134ba28] schedule at ffffffff86065c6f #2 [ffffb5b9c134ba40] schedule_timeout at ffffffff86069fb0 #3 [ffffb5b9c134bab0] __wait_for_common at ffffffff8606674f #4 [ffffb5b9c134bb10] scsi_remove_host at ffffffff85bfe84b #5 [ffffb5b9c134bb30] iscsi_sw_tcp_session_destroy at ffffffffc03031c4 [iscsi_tcp] #6 [ffffb5b9c134bb48] iscsi_if_recv_msg at ffffffffc0292692 [scsi_transport_iscsi] #7 [ffffb5b9c134bb98] iscsi_if_rx at ffffffffc02929c2 [scsi_transport_iscsi] #8 [ffffb5b9c134bbf0] netlink_unicast at ffffffff85e551d6 #9 [ffffb5b9c134bc38] netlink_sendmsg at ffffffff85e554ef	N/A	More Details
CVE-2026-23297	In the Linux kernel, the following vulnerability has been resolved: nfsd: Fix cred ref leak in nfsd_nl_threads_set_doit(). syzbot reported memory leak of struct cred. [0] nfsd_nl_threads_set_doit() passes get_current_cred() to nfsd_svc(), but put_cred() is not called after that. The cred is finally passed down to _svc_xprt_create(), which calls get_cred() with the cred for struct svc_xprt. The ownership of the refcount by get_current_cred() is not transferred to anywhere and is just leaked. nfsd_svc() is also called from write_threads(), but it does not bump file->f_cred there. nfsd_nl_threads_set_doit() is called from sendmsg() and current->cred does not go away. Let's use current_cred() in nfsd_nl_threads_set_doit(). [0]: BUG: memory leak unreferenced object 0xffff888108b89480 (size 184): comm "syz-executor", pid 5994, jiffies 4294943386 hex dump (first 32 bytes): 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace (crc 369454a7): kmemleak_alloc_recursive include/linux/kmemleak.h:44 [inline] slab_post_alloc_hook mm/slub.c:4958 [inline] slab_alloc_node mm/slub.c:5263 [inline] kmem_cache_alloc_noprof+0x412/0x580 mm/slub.c:5270	N/A	More Details

	prepare_creds+0x22/0x600 kernel/cred.c:185 copy_creds+0x44/0x290 kernel/cred.c:286 copy_process+0x7a7/0x2870 kernel/fork.c:2086 kernel_clone+0xac/0x6e0 kernel/fork.c:2651 __do_sys_clone+0x7f/0xb0 kernel/fork.c:2792 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xa4/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f		
CVE-2026-23298	In the Linux kernel, the following vulnerability has been resolved: can: ucan: Fix infinite loop from zero-length messages If a broken ucan device gets a message with the message length field set to 0, then the driver will loop for forever in ucan_read_bulk_callback(), hanging the system. If the length is 0, just skip the message and go on to the next one. This has been fixed in the kvaser_usb driver in the past in commit 0c73772cd2b8 ("can: kvaser_usb: leaf: Fix potential infinite loop in command parsers"), so there must be some broken devices out there like this somewhere.	N/A	More Details
CVE-2026-23299	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: purge error queues in socket destructors When TX timestamping is enabled via SO_TIMESTAMPING, SKBs may be queued into sk_error_queue and will stay there until consumed. If userspace never gets to read the timestamps, or if the controller is removed unexpectedly, these SKBs will leak. Fix by adding skb_queue_purge() calls for sk_error_queue in affected bluetooth destructors. RFCOMM does not currently use sk_error_queue.	N/A	More Details
CVE-2026-34073	cryptography is a package designed to expose cryptographic primitives and recipes to Python developers. Prior to version 46.0.6, DNS name constraints were only validated against SANs within child certificates, and not the "peer name" presented during each validation. Consequently, cryptography would allow a peer named bar.example.com to validate against a wildcard leaf certificate for *.example.com, even if the leaf's parent certificate (or upwards) contained an excluded subtree constraint for bar.example.com. This issue has been patched in version 46.0.6.	N/A	More Details
CVE-2026-23300	In the Linux kernel, the following vulnerability has been resolved: net: ipv6: fix panic when IPv4 route references loopback IPv6 nexthop When a standalone IPv6 nexthop object is created with a loopback device (e.g., "ip -6 nexthop add id 100 dev lo"), fib6_nh_init() misclassifies it as a reject route. This is because nexthop objects have no destination prefix (fc_dst=::), causing fib6_is_reject() to match any loopback nexthop. The reject path skips fib_nh_common_init(), leaving nhc_pcpu_rth_output unallocated. If an IPv4 route later references this nexthop, __mkroute_output() dereferences NULL nhc_pcpu_rth_output and panics. Simplify the check in fib6_nh_init() to only match explicit reject routes (RTF_REJECT) instead of using fib6_is_reject(). The loopback promotion heuristic in fib6_is_reject() is handled separately by ip6_route_info_create_nh(). After this change, the three cases behave as follows: 1. Explicit reject route ("ip -6 route add unreachable 2001:db8::/64"): RTF_REJECT is set, enters reject path, skips fib_nh_common_init(). No behavior change. 2. Implicit loopback reject route ("ip -6 route add 2001:db8::/32 dev lo"): RTF_REJECT is not set, takes normal path, fib_nh_common_init() is called. ip6_route_info_create_nh() still promotes it to reject afterward. nhc_pcpu_rth_output is allocated but unused, which is harmless. 3. Standalone nexthop object ("ip -6 nexthop add id 100 dev lo"): RTF_REJECT is not set, takes normal path, fib_nh_common_init() is called. nhc_pcpu_rth_output is properly allocated, fixing the crash when IPv4 routes reference this nexthop.	N/A	More Details
CVE-2026-34060	Ruby LSP is an implementation of the language server protocol for Ruby. Prior to Shopify.ruby-lsp version 0.10.2 and ruby-lsp version 0.26.9, the rubyLsp.branch VS Code workspace setting was interpolated without sanitization into a generated Gemfile, allowing arbitrary Ruby code execution when a user opens a project containing a malicious .vscode/settings.json. This issue has been patched in Shopify.ruby-lsp version 0.10.2 and ruby-lsp version 0.26.9.	N/A	More Details
CVE-2026-23301	In the Linux kernel, the following vulnerability has been resolved: ASoC: SDCA: Add allocation failure check for Entity name Currently find_sdca_entity_iot() can allocate a string for the Entity name but it doesn't check if that allocation succeeded. Add the missing NULL check after the allocation.	N/A	More Details
CVE-2026-3457	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Thales Sentinel LDK Runtime on Windows allows Stored XSS.This issue affects Sentinel LDK Runtime: before 10.22.	N/A	More Details
CVE-2026-23302	In the Linux kernel, the following vulnerability has been resolved: net: annotate data-races around sk->sk_{data_ready,write_space} skmsg (and probably other layers) are changing these pointers while other cpus might read them concurrently. Add corresponding READ_ONCE()/WRITE_ONCE() annotations for UDP, TCP and AF_UNIX.	N/A	More Details
CVE-2026-34041	act is a project which allows for local running of github actions. Prior to version 0.2.86, act unconditionally processes the deprecated ::set-env:: and ::add-path:: workflow commands, which was disabled due to environment injection risks. When a workflow step echoes untrusted data to stdout, an attacker can inject these commands to set arbitrary environment variables or modify the PATH for all subsequent steps in the job. This issue has been patched in version 0.2.86.	N/A	More Details
CVE-2026-23303	In the Linux kernel, the following vulnerability has been resolved: smb: client: Don't log plaintext credentials in cifs_set_cifscreds When debug logging is enabled, cifs_set_cifscreds() logs the key payload and exposes the plaintext username and password. Remove the debug log to avoid exposing credentials.	N/A	More Details
CVE-2026-23304	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix NULL pointer deref in ip6_rt_get_dev_rcu() l3mdev_master_dev_rcu() can return NULL when the slave device is being un-slaved from a VRF. All other callers deal with this, but we lost the fallback to loopback in ip6_rt_pcpu_alloc() -> ip6_rt_get_dev_rcu() with commit 4832c30d5458 ("net: ipv6: put host and anycast routes on device with address"). KASAN: null-ptr-deref in range [0x0000000000000108-0x000000000000010f] RIP: 0010:ip6_rt_pcpu_alloc (net/ipv6/route.c:1418) Call Trace: ip6_pol_route (net/ipv6/route.c:2318) fib6_rule_lookup (net/ipv6/fib6_rules.c:115) ip6_route_output_flags (net/ipv6/route.c:2607) vrf_process_v6_outbound (drivers/net/vrf.c:437) I was tempted to rework the un-slaving code to clear the flag first and insert synchronize_rcu() before we remove the upper. But looks like the explicit fallback to loopback_dev is an established pattern. And I guess avoiding the synchronize_rcu() is nice, too.	N/A	More Details
CVE-2026-23305	In the Linux kernel, the following vulnerability has been resolved: accel/rocket: fix unwinding in error path in rocket_probe When rocket_core_init() fails (as could be the case with EPROBE_DEFER), we need to properly unwind by decrementing the counter we just incremented and if this is the first core we failed to probe, remove the rocket DRM device with rocket_device_fini() as well. This matches the logic in rocket_remove(). Failing to properly unwind results in out-of-bounds accesses.	N/A	More Details
CVE-2026-23306	In the Linux kernel, the following vulnerability has been resolved: scsi: pm8001: Fix use-after-free in pm8001_queue_command() Commit e29c47fe8946 ("scsi: pm8001: Simplify pm8001_task_exec()") refactors pm8001_queue_command(), however it introduces a potential cause of a double free scenario when it changes the function to return -ENODEV in case of phy down/device gone state. In this path, pm8001_queue_command() updates task status and calls task_done to indicate to upper layer that the task has been handled. However, this also frees the underlying SAS task. A -ENODEV is then returned to the caller. When libsas sas_ata_qc_issue() receives this error value, it assumes the task wasn't handled/queued by LLDD and proceeds to clean up and free the task again, resulting in a double free. Since pm8001_queue_command() handles the SAS task in this case, it should return 0 to the caller indicating that the task has been handled.	N/A	More Details
CVE-2026-25101	Bludit allows user's session identifier to be set before authentication. The value of this session ID stays the same after authentication. This behavior enables an attacker to fix a session ID for a victim and later hijack the authenticated session. This issue was fixed in version 3.17.2.	N/A	More Details
CVE-2026-	Missing Authorization vulnerability in NEC Platforms, Ltd. Aterm Series allows a attacker to get a specific device information and change the	N/A	More

4309	settings via network.		Details
CVE-2026-23324	In the Linux kernel, the following vulnerability has been resolved: can: usb: etas_es58x: correctly anchor the urb in the read bulk callback When submitting an urb, that is using the anchor pattern, it needs to be anchored before submitting it otherwise it could be leaked if usb_kill_anchored_urbs() is called. This logic is correctly done elsewhere in the driver, except in the read bulk callback so do that here also.	N/A	More Details
CVE-2026-30313	DSAI-Cline's command auto-approval module contains a critical OS command injection vulnerability that renders its whitelist security mechanism completely ineffective. The system relies on string-based parsing to validate commands; while it intercepts dangerous operators such as ;, &&, ||, |, and command substitution patterns, it fails to account for raw newline characters embedded within the input. An attacker can construct a payload by embedding a literal newline between a whitelisted command and malicious code (e.g., git log malicious_command), forcing DSAI-Cline to misidentify it as a safe operation and automatically approve it. The underlying PowerShell interpreter treats the newline as a command separator, executing both commands sequentially, resulting in Remote Code Execution without any user interaction.	N/A	More Details
CVE-2026-23334	In the Linux kernel, the following vulnerability has been resolved: can: usb: f81604: handle short interrupt urb messages properly If an interrupt urb is received that is not the correct length, properly detect it and don't attempt to treat the data as valid.	N/A	More Details
CVE-2026-23335	In the Linux kernel, the following vulnerability has been resolved: RDMA/irdma: Fix kernel stack leak in irdma_create_user_ah() struct irdma_create_ah_resp { // 8 bytes, no padding __u32 ah_id; // offset 0 - SET (uresp.ah_id = ah->sc_ah.ah_info.ah_idx) __u8 rsvd[4]; // offset 4 - NEVER SET <- LEAK }; rsvd[4]: 4 bytes of stack memory leaked unconditionally. Only ah_id is assigned before ib_respond_udata(). The reserved members of the structure were not zeroed.	N/A	More Details
CVE-2026-33029	Nginx UI is a web user interface for the Nginx web server. Prior to version 2.3.4, an input validation vulnerability in the logrotate configuration allows an authenticated user to cause a complete Denial of Service (DoS). By submitting a negative integer for the rotation interval, the backend enters an infinite loop or an invalid state, rendering the web interface unresponsive. This issue has been patched in version 2.3.4.	N/A	More Details
CVE-2026-33028	Nginx UI is a web user interface for the Nginx web server. Prior to version 2.3.4, the nginx-ui application is vulnerable to a Race Condition. Due to the complete absence of synchronization mechanisms (Mutex) and non-atomic file writes, concurrent requests lead to the severe corruption of the primary configuration file (app.ini). This vulnerability results in a persistent Denial of Service (DoS) and introduces a non-deterministic path for Remote Code Execution (RCE) through configuration cross-contamination. This issue has been patched in version 2.3.4.	N/A	More Details
CVE-2026-33027	Nginx UI is a web user interface for the Nginx web server. Prior to version 2.3.4, the nginx-ui configuration improperly handles URL-encoded traversal sequences. When specially crafted paths are supplied, the backend resolves them to the base Nginx configuration directory and executes the operation on the base directory (/etc/nginx). In particular, this allows an authenticated user to remove the entire /etc/nginx directory, resulting in a partial Denial of Service. This issue has been patched in version 2.3.4.	N/A	More Details
CVE-2026-23336	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: cancel rfkill_block work in wiphy_unregister() There is a use-after-free error in cfg80211_shutdown_all_interfaces found by syzkaller: BUG: KASAN: use-after-free in cfg80211_shutdown_all_interfaces+0x213/0x220 Read of size 8 at addr ffff888112a78d98 by task kworker/0:5/5326 CPU: 0 UID: 0 PID: 5326 Comm: kworker/0:5 Not tainted 6.19.0-rc2 #2 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Workqueue: events cfg80211_rfkill_block_work Call Trace: <TASK> dump_stack_lvl+0x116/0x1f0 print_report+0xcd/0x630 kasan_report+0xe0/0x110 cfg80211_shutdown_all_interfaces+0x213/0x220 cfg80211_rfkill_block_work+0x1e/0x30 process_one_work+0x9cf/0x1b70 worker_thread+0x6c8/0xf10 kthread+0x3c5/0x780 ret_from_fork+0x56d/0x700 ret_from_fork_asm+0x1a/0x30 </TASK> The problem arises due to the rfkill_block work is not cancelled when wiphy is being unregistered. In order to fix the issue cancel the corresponding work in wiphy_unregister(). Found by Linux Verification Center (linuxtesting.org) with Syzkaller.	N/A	More Details
CVE-2026-23337	In the Linux kernel, the following vulnerability has been resolved: pinctrl: pinconf-generic: Fix memory leak in pinconf_generic_parse_dt_config() In pinconf_generic_parse_dt_config(), if parse_dt_cfg() fails, it returns directly. This bypasses the cleanup logic and results in a memory leak of the cfg buffer. Fix this by jumping to the out label on failure, ensuring kfree(cfg) is called before returning.	N/A	More Details
CVE-2026-23338	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/userq: Do not allow userspace to trivially triger kernel warnings Userspace can either deliberately pass in the too small num_fences, or the required number can legitimately grow between the two calls to the userq wait ioctl. In both cases we do not want the emit the kernel warning backtrace since nothing is wrong with the kernel and userspace will simply get an errno reported back. So lets simply drop the WARN_ONs. (cherry picked from commit 2c333ea579de6cc20ea7bc50e9595ef72863e65c)	N/A	More Details
CVE-2026-4620	OS Command Injection vulnerability in NEC Platforms, Ltd. Aterm Series allows a attacker to execute arbitrary OS commands via network.	N/A	More Details
CVE-2026-4621	Hidden Functionality vulnerability in NEC Platforms, Ltd. Aterm Series allows a attacker to enable telnet via network.	N/A	More Details
CVE-2026-4622	OS Command Injection vulnerability in NEC Platforms, Ltd. Aterm Series allows a attacker to execute arbitrary OS commands via network.	N/A	More Details
CVE-2026-4340	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-2026-23339	In the Linux kernel, the following vulnerability has been resolved: nfc: nci: free skb on nci_transceive early error paths nci_transceive() takes ownership of the skb passed by the caller, but the -EPROTO, -EINVAL, and -EBUSY error paths return without freeing it. Due to issues clearing NCI_DATA_EXCHANGE fixed by subsequent changes the nci/nci_dev selftest hits the error path occasionally in NIPA, and kmemleak detects leaks: unreferenced object 0xff11000015ce6a40 (size 640): comm "nci_dev", pid 3954, jiffies 4295441246 hex dump (first 32 bytes): 6b 6b 6b 6b 00 a4 00 0c 02 e1 03 6b 6b 6b 6b 6b kkkk.....kkkkk 6b 6b 6b 6b 6b 6b 6b 6b 6b 6b 6b 6b 6b 6b 6b 6b kkkkkkkkkkkkkkkk backtrace (crc 7c40cc2a): kmem_cache_alloc_node_noprof+0x492/0x630 __alloc_skb+0x11e/0x5f0 alloc_skb_with_frags+0xc6/0x8f0 sock_alloc_send_pskb+0x326/0x3f0 nfc_alloc_send_skb+0x94/0x1d0 rawsock_sendmsg+0x162/0x4c0 do_syscall_64+0x117/0xfc0	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net: sched: avoid qdisc_reset_all_tx_gt() vs dequeue race for lockless qdiscs When shrinking the number of real tx queues, netif_set_real_num_tx_queues() calls qdisc_reset_all_tx_gt() to flush qdiscs for queues which will no longer be used. qdisc_reset_all_tx_gt() currently serializes qdisc_reset() with qdisc_lock(). However, for lockless qdiscs, the dequeue path is serialized by qdisc_run_begin/end() using qdisc->seqlock instead, so qdisc_reset() can run concurrently with __qdisc_run() and free skbs while they are still being dequeued, leading to UAF. This can easily be reproduced on e.g. virtio-net by imposing heavy traffic while frequently changing the number of queue pairs: iperf3 -ub0 -c $peer -t 0 & while :; do ethtool -L eth0 combined 1 ethtool -L eth0 combined 2 done With		

CVE-2026-23340	KASAN enabled, this leads to reports like: BUG: KASAN: slab-use-after-free in __qdisc_run+0x133f/0x1760 ... Call Trace: <TASK> ... __qdisc_run+0x133f/0x1760 __dev_queue_xmit+0x248f/0x3550 ip_finish_output2+0xa42/0x2110 ip_output+0x1a7/0x410 ip_send_skb+0x2e6/0x480 udp_send_skb+0xb0a/0x1590 udp_sendmsg+0x13c9/0x1fc0 ... </TASK> Allocated by task 1270 on cpu 5 at 44.558414s: ... alloc_skb_with_frags+0x84/0x7c0 sock_alloc_send_pskb+0x69a/0x830 __ip_append_data+0x1b86/0x48c0 ip_make_skb+0x1e8/0x2b0 udp_sendmsg+0x13a6/0x1fc0 ... Freed by task 1306 on cpu 3 at 44.558445s: ... kmem_cache_free+0x117/0x5e0 pfifo_fast_reset+0x14d/0x580 qdisc_reset+0x9e/0x5f0 netif_set_real_num_tx_queues+0x303/0x840 virtnet_set_channels+0x1bf/0x260 [virtio_net] ethnl_set_channels+0x684/0xae0 ethnl_default_set_doit+0x31a/0x890 ... Serialize qdisc_reset_all_tx_gt() against the lockless dequeue path by taking qdisc->seqlock for TCQ_F_NOLOCK qdiscs, matching the serialization model already used by dev_reset_queue(). Additionally clear QDISC_STATE_NON_EMPTY after reset so the qdisc state reflects an empty queue, avoiding needless re-scheduling.	N/A	More Details
CVE-2026-4982	A user with permission "update world" in any Venueless world is able to exfiltrate chat messages from direct messages or channels in other worlds on the same server due to a bug in the reporting feature. The exploitability is limited by the fact that the attacker needs to know the internal channel UUID of the chat channel, which is unlikely to be obtained by an outside attacker, especially for direct messages.	N/A	More Details
CVE-2025-13478	Cache misconfiguration vulnerability in OpenText Identity Manager on Windows, Linux allows remote authenticated users to obtain another user's session data via insecure application cache handling. This issue affects Identity Manager: 25.2(v4.10.1).	N/A	More Details
CVE-2026-32695	Traefik is an HTTP reverse proxy and load balancer. Prior to versions 3.6.11 and 3.7.0-ea.2, Traefik's Knative provider builds router rules by interpolating user-controlled values into backtick-delimited rule expressions without escaping. In live cluster validation, Knative `rules[].hosts[]` was exploitable for host restriction bypass (for example `tenant.example.com`) || Host(`attacker.com`), producing a router that serves attacker-controlled hosts. Knative `headers[].exact` also allows rule-syntax injection and proves unsafe rule construction. In multi-tenant clusters, this can route unauthorized traffic to victim services and lead to cross-tenant traffic exposure. Versions 3.6.11 and 3.7.0-ea.2 patch the issue.	N/A	More Details
CVE-2024-11604	Insertion of Sensitive Information into Log File vulnerability in the SCIM Driver module in OpenText IDM Driver and Extensions on Windows, Linux, 64 bit allows authenticated local users to obtain sensitive information via access to log files. This issue affects IDM SCIM Driver: 1.0.0.0000 through 1.0.1.0300 and 1.1.0.0000.	N/A	More Details
CVE-2026-32680	The installer of RATOC RAID Monitoring Manager for Windows allows to customize the installation folder. If the installation folder is customized to some non-default one, the folder may be left with un-secure ACLs and non-administrative users can alter contents of that folder. It may allow a non-administrative user to execute an arbitrary code with SYSTEM privilege.	N/A	More Details
CVE-2026-2287	CrewAI does not properly check that Docker is still running during runtime, and will fall back to a sandbox setting that allows for RCE exploitation.	N/A	More Details
CVE-2026-2286	CrewAI contains a server-side request forgery vulnerability that enables content acquisition from internal and cloud services, facilitated by the RAG search tools not properly validating URLs provided at runtime.	N/A	More Details
CVE-2026-2285	CrewAI contains a arbitrary local file read vulnerability in the JSON loader tool that reads files without path validation, enabling access to files on the server.	N/A	More Details
CVE-2026-23341	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Fix crash when destroying a suspended hardware context If userspace issues an ioctl to destroy a hardware context that has already been automatically suspended, the driver may crash because the mailbox channel pointer is NULL for the suspended context. Fix this by checking the mailbox channel pointer in aie2_destroy_context() before accessing it.	N/A	More Details
CVE-2026-4619	Path Traversal vulnerability in NEC Platforms, Ltd. Aterm Series allows a attacker to wtite over any file via network.	N/A	More Details
CVE-2026-23333	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_set_rbtree: validate open interval overlap [Upstream commit 648946966a08e4cb1a71619e3d1b12bd7642de7b] Open intervals do not have an end element, in particular an open interval at the end of the set is hard to validate because of it is lacking the end element, and interval validation relies on such end element to perform the checks. This patch adds a new flag field to struct nft_set_elem, this is not an issue because this is a temporary object that is allocated in the stack from the insert/deactivate path. This flag field is used to specify that this is the last element in this add/delete command. The last flag is used, in combination with the start element cookie, to check if there is a partial overlap, eg. Already exists: 255.255.255.0-255.255.255.254 Add interval: 255.255.255.0-255.255.255.255 ~~~~~~~~~~~~~~ start element overlap Basically, the idea is to check for an existing end element in the set if there is an overlap with an existing start element. However, the last open interval can come in any position in the add command, the corner case can get a bit more complicated: Already exists: 255.255.255.0-255.255.255.254 Add intervals: 255.255.255.0-255.255.255.255,255.255.255.0-255.255.255.254 ~~~~~~~~~~~~~~ start element overlap To catch this overlap, annotate that the new start element is a possible overlap, then report the overlap if the next element is another start element that confirms that previous element in an open interval at the end of the set. For deletions, do not update the start cookie when deleting an open interval, otherwise this can trigger spurious EEXIST when adding new elements. Unfortunately, there is no NFT_SET_ELEM_INTERVAL_OPEN flag which would make easier to detect open interval overlaps.	N/A	More Details
CVE-2026-23332	In the Linux kernel, the following vulnerability has been resolved: cpufreq: intel_pstate: Fix crash during turbo disable When the system is booted with kernel command line argument "nosmt" or "maxcpus" to limit the number of CPUs, disabling turbo via: echo 1 > /sys/devices/system/cpu/intel_pstate/no_turbo results in a crash: PF: supervisor read access in kernel mode PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] SMP PTI ... RIP: 0010:store_no_turbo+0x100/0x1f0 ... This occurs because for_each_possible_cpu() returns CPUs even if they are not online. For those CPUs, all_cpu_data[] will be NULL. Since commit 973207ae3d7c ("cpufreq: intel_pstate: Rearrange max frequency updates handling code"), all_cpu_data[] is dereferenced even for CPUs which are not online, causing the NULL pointer dereference. To fix that, pass CPU number to intel_pstate_update_max_freq() and use all_cpu_data[] for those CPUs for which there is a valid cpufreq policy.	N/A	More Details
CVE-2026-30305	Syntx's command auto-approval module contains a critical OS command injection vulnerability that renders its whitelist security mechanism completely ineffective. The system relies on fragile regular expressions to parse command structures; while it attempts to intercept dangerous operations, it fails to account for standard Shell command substitution syntax (specifically $(...)and backticks ...). An attacker can construct a command such as git log --grep="$(malicious_command)", forcing Syntx to misidentify it as a safe git operation and automatically approve it. The underlying Shell prioritizes the execution of the malicious code injected within the arguments, resulting in Remote Code Execution without any user interaction.	N/A	More Details
CVE-	In its design for automatic terminal command execution, HAI Build Code Generator offers two options: Execute safe commands and Execute all commands. The description for the former states that commands determined by the model to be safe will be automatically executed, whereas		

2026-30308	if the model judges a command to be potentially destructive, it still requires user approval. However, this design is highly susceptible to prompt injection attacks. An attacker can employ a generic template to wrap any malicious command and mislead the model into misclassifying it as a 'safe' command, thereby bypassing the user approval requirement and resulting in arbitrary command execution.	N/A	More Details
CVE-2026-30306	In its design for automatic terminal command execution, SakaDev offers two options: Execute safe commands and execute all commands. The description for the former states that commands determined by the model to be safe will be automatically executed, whereas if the model judges a command to be potentially destructive, it still requires user approval. However, this design is highly susceptible to prompt injection attacks. An attacker can employ a generic template to wrap any malicious command and mislead the model into misclassifying it as a 'safe' command, thereby bypassing the user approval requirement and resulting in arbitrary command execution.	N/A	More Details
CVE-2026-23325	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7996: Fix possible oob access in mt7996_mac_write_txwi_80211() Check frame length before accessing the mgmt fields in mt7996_mac_write_txwi_80211 in order to avoid a possible oob access.	N/A	More Details
CVE-2026-27018	Gotenberg is an API for converting document formats. Prior to version 8.29.0, the fix introduced for CVE-2024-21527 can be bypassed using mixed-case or uppercase URL schemes. This issue has been patched in version 8.29.0.	N/A	More Details
CVE-2026-23326	In the Linux kernel, the following vulnerability has been resolved: xsk: Fix fragment node deletion to prevent buffer leak After commit b692bf9a7543 ("xsk: Get rid of xdp_buff_xsk::xskb_list_node"), the list_node field is reused for both the xskb pool list and the buffer free list, this causes a buffer leak as described below. xp_free() checks if a buffer is already on the free list using list_empty(&xskb->list_node). When list_del() is used to remove a node from the xskb pool list, it doesn't reinitialize the node pointers. This means list_empty() will return false even after the node has been removed, causing xp_free() to incorrectly skip adding the buffer to the free list. Fix this by using list_del_init() instead of list_del() in all fragment handling paths, this ensures the list node is reinitialized after removal, allowing the list_empty() to work correctly.	N/A	More Details
CVE-2026-23327	In the Linux kernel, the following vulnerability has been resolved: cxl/mbox: validate payload size before accessing contents in cxl_payload_from_user_allowed() cxl_payload_from_user_allowed() casts and dereferences the input payload without first verifying its size. When a raw mailbox command is sent with an undersized payload (ie: 1 byte for CXL_MBOX_OP_CLEAR_LOG, which expects a 16-byte UUID), uuid_equal() reads past the allocated buffer, triggering a KASAN splat: BUG: KASAN: slab-out-of-bounds in memcmp+0x176/0x1d0 lib/string.c:683 Read of size 8 at addr ffff88810130f5c0 by task syz.1.62/2258 CPU: 2 UID: 0 PID: 2258 Comm: syz.1.62 Not tainted 6.19.0-dirty #3 PREEMPT(voluntary) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.17.0-0-gb52ca86e094d-prebuilt.qemu.org 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0xab/0xe0 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xce/0x650 mm/kasan/report.c:482 kasan_report+0xce/0x100 mm/kasan/report.c:595 memcmp+0x176/0x1d0 lib/string.c:683 uuid_equal include/linux/uuid.h:73 [inline] cxl_payload_from_user_allowed drivers/cxl/core/mbox.c:345 [inline] cxl_mbox_cmd_ctor drivers/cxl/core/mbox.c:368 [inline] cxl_validate_cmd_from_user drivers/cxl/core/mbox.c:522 [inline] cxl_send_cmd+0x9c0/0xb50 drivers/cxl/core/mbox.c:643 __cxl_memdev_ioctl drivers/cxl/core/memdev.c:698 [inline] cxl_memdev_ioctl+0x14f/0x190 drivers/cxl/core/memdev.c:713 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:597 [inline] __se_sys_ioctl fs/ioctl.c:583 [inline] __x64_sys_ioctl+0x18e/0x210 fs/ioctl.c:583 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xa8/0x330 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7fdaf331ba79 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007fdaf1d77038 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 00007fdaf3585fa0 RCX: 00007fdaf331ba79 RDX: 00002000000001c0 RSI: 00000000c030ce02 RDI: 0000000000000003 RBP: 00007fdaf33749df R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007fdaf3586038 R14: 00007fdaf3585fa0 R15: 00007ffced2af768 </TASK> Add 'in_size' parameter to cxl_payload_from_user_allowed() and validate the payload is large enough.	N/A	More Details
CVE-2026-33026	Nginx UI is a web user interface for the Nginx web server. Prior to version 2.3.4, the nginx-ui backup restore mechanism allows attackers to tamper with encrypted backup archives and inject malicious configuration during restoration. This issue has been patched in version 2.3.4.	N/A	More Details
CVE-2026-32275	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. From version 1.3.10 to before version 2.17.0, an unsanitized JSONP callback parameter allows cross-origin script injection and API key theft. This issue has been patched in version 2.17.0.	N/A	More Details
CVE-2026-31831	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. Prior to version 2.17.0, the /newsletter/image/images API endpoint is vulnerable to path traversal, allowing unauthenticated attackers to read arbitrary files from the application server's filesystem. This issue has been patched in version 2.17.0.	N/A	More Details
CVE-2026-30307	Roo Code's command auto-approval module contains a critical OS command injection vulnerability that renders its whitelist security mechanism completely ineffective. The system relies on fragile regular expressions to parse command structures; while it attempts to intercept dangerous operations, it fails to account for standard Shell command substitution Roo Code (specifically$(...)and backticks ...). An attacker can construct a command such as git log --grep="$(malicious_command)", forcing Syntx to misidentify it as a safe git operation and automatically approve it. The underlying Shell prioritizes the execution of the malicious code injected within the arguments, resulting in Remote Code Execution without any user interaction.	N/A	More Details
CVE-2026-28505	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. Prior to version 2.17.0, the str_eval() function in notification_handler.py implements a sandboxed eval() for notification text templates. The sandbox attempts to restrict callable names by inspecting code.co_names of the compiled code object. However, co_names only contains names from the outer code object. When a lambda expression is used, it creates a nested code object whose attribute accesses are stored in code.co_consts, NOT in code.co_names. The sandbox never inspects nested code objects. This issue has been patched in version 2.17.0.	N/A	More Details
CVE-2026-23331	In the Linux kernel, the following vulnerability has been resolved: udp: Unhash auto-bound connected sk from 4-tuple hash table when disconnected. Let's say we bind() an UDP socket to the wildcard address with a non-zero port, connect() it to an address, and disconnect it from the address. bind() sets SOCK_BINDPORT_LOCK on sk->sk_userlocks (but not SOCK_BINDADDR_LOCK), and connect() calls udp_lib_hash4() to put the socket into the 4-tuple hash table. Then, __udp_disconnect() calls sk->sk_prot->rehash(sk). It computes a new hash based on the wildcard address and moves the socket to a new slot in the 4-tuple hash table, leaving a garbage in the chain that no packet hits. Let's remove such a socket from 4-tuple hash table when disconnected. Note that udp_sk(sk)->udp_portaddr_hash needs to be udpated after udp_hash4_dec(hslot2) in udp_unhash4().	N/A	More Details
CVE-2026-21717	A flaw in V8's string hashing mechanism causes integer-like strings to be hashed to their numeric value, making hash collisions trivially predictable. By crafting a request that causes many such collisions in V8's internal string table, an attacker can significantly degrade performance of the Node.js process. The most common trigger is any endpoint that calls `JSON.parse()` on attacker-controlled input, as JSON parsing automatically internalizes short strings into the affected hash table. This vulnerability affects **20.x, 22.x, 24.x, and 25.x**.	N/A	More Details
CVE-	An incomplete fix for CVE-2024-36137 leaves `FileHandle.chmod()` and `FileHandle.chown()` in the promises API without the required permission checks, while their callback-based equivalents (`fs.fchmod()`, `fs.fchown()`) were correctly patched. As a result, code running under		

2026-21716	`--permission` with restricted `--allow-fs-write` can still use promise-based `FileHandle` methods to modify file permissions and ownership on already-open file descriptors, bypassing the intended write restrictions. This vulnerability affects **20.x, 22.x, 24.x, and 25.x** processes using the Permission Model where `--allow-fs-write` is intentionally restricted.	N/A	More Details
CVE-2026-21715	A flaw in Node.js Permission Model filesystem enforcement leaves `fs.realpathSync.native()` without the required read permission checks, while all comparable filesystem functions correctly enforce them. As a result, code running under `--permission` with restricted `--allow-fs-read` can still use `fs.realpathSync.native()` to check file existence, resolve symlink targets, and enumerate filesystem paths outside of permitted directories. This vulnerability affects **20.x, 22.x, 24.x, and 25.x** processes using the Permission Model where `--allow-fs-read` is intentionally restricted.	N/A	More Details
CVE-2026-21714	A memory leak occurs in Node.js HTTP/2 servers when a client sends WINDOW_UPDATE frames on stream 0 (connection-level) that cause the flow control window to exceed the maximum value of 2^{31}-1. The server correctly sends a GOAWAY frame, but the Http2Session object is never cleaned up. This vulnerability affects HTTP2 users on Node.js 20, 22, 24 and 25.	N/A	More Details
CVE-2026-21713	A flaw in Node.js HMAC verification uses a non-constant-time comparison when validating user-provided signatures, potentially leaking timing information proportional to the number of matching bytes. Under certain threat models where high-resolution timing measurements are possible, this behavior could be exploited as a timing oracle to infer HMAC values. Node.js already provides timing-safe comparison primitives used elsewhere in the codebase, indicating this is an oversight rather than an intentional design decision. This vulnerability affects **20.x, 22.x, 24.x, and 25.x**.	N/A	More Details
CVE-2026-21711	A flaw in Node.js Permission Model network enforcement leaves Unix Domain Socket (UDS) server operations without the required permission checks, while all comparable network paths correctly enforce them. As a result, code running under `--permission` without `--allow-net` can create and expose local IPC endpoints, allowing communication with other processes on the same host outside of the intended network restriction boundary. This vulnerability affects Node.js **25.x** processes using the Permission Model where `--allow-net` is intentionally omitted to restrict network access. Note that `--allow-net` is currently an experimental feature.	N/A	More Details
CVE-2026-21710	A flaw in Node.js HTTP request handling causes an uncaught `TypeError` when a request is received with a header named `__proto__` and the application accesses `req.headersDistinct`. When this occurs, `dest["__proto__"]` resolves to `Object.prototype` rather than `undefined`, causing `.push()` to be called on a non-array. This exception is thrown synchronously inside a property getter and cannot be intercepted by `error` event listeners, meaning it cannot be handled without wrapping every `req.headersDistinct` access in a `try/catch`. * This vulnerability affects all Node.js HTTP servers on **20.x, 22.x, 24.x, and v25.x**	N/A	More Details
CVE-2026-23328	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Fix NULL pointer dereference of mgmt_chann mgmt_chann may be set to NULL if the firmware returns an unexpected error in aie2_send_mgmt_msg_wait(). This can later lead to a NULL pointer dereference in aie2_hw_stop(). Fix this by introducing a dedicated helper to destroy mgmt_chann and by adding proper NULL checks before accessing it.	N/A	More Details
CVE-2026-23329	In the Linux kernel, the following vulnerability has been resolved: libie: don't unroll if fwlog isn't supported The libie_fwlog_deinit() function can be called during driver unload even when firmware logging was never properly initialized. This led to call trace: [148.576156] Oops: Oops: 0000 [#1] SMP NOPTI [148.576167] CPU: 80 UID: 0 PID: 12843 Comm: rmmod Kdump: loaded Not tainted 6.17.0-rc7next-queue-3oct-01915-g06d79d51cf51 #1 PREEMPT(full) [148.576177] Hardware name: HPE ProLiant DL385 Gen10 Plus/ProLiant DL385 Gen10 Plus, BIOS A42 07/18/2020 [148.576182] RIP: 0010:__dev_printk+0x16/0x70 [148.576196] Code: 1f 44 00 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 0f 1f 44 00 00 41 55 41 54 49 89 d4 55 48 89 fd 53 48 85 f6 74 3c <4c> 8b 6e 50 48 89 f3 4d 85 ed 75 03 4c 8b 2e 48 89 df e8 f3 27 98 [148.576204] RSP: 0018:ffffd2fd7ea17a48 EFLAGS: 00010202 [148.576211] RAX: ffffd2fd7ea17aa0 RBX: ffff8eb288ae2000 RCX: 0000000000000000 [148.576217] RDX: ffffd2fd7ea17a70 RSI: 00000000000000c8 RDI: ffffffffb68d3d88 [148.576222] RBP: ffffffffb68d3d88 R08: 0000000000000000 R09: 0000000000000000 [148.576227] R10: 00000000000000c8 R11: ffff8eb2b1a49400 R12: ffffd2fd7ea17a70 [148.576231] R13: ffff8eb3141fb000 R14: ffffffffc1215b48 R15: ffffffffc1215bd8 [148.576236] FS: 00007f5666ba6740(0000) GS:ffff8eb2472b9000(0000) knlGS:0000000000000000 [148.576242] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [148.576247] CR2: 0000000000000118 CR3: 000000011ad17000 CR4: 0000000000350ef0 [148.576252] Call Trace: [148.576258] <TASK> [148.576269] _dev_warn+0x7c/0x96 [148.576290] libie_fwlog_deinit+0x112/0x117 [libie_fwlog] [148.576303] ixgbe_remove+0x63/0x290 [ixgbe] [148.576342] pci_device_remove+0x42/0xb0 [148.576354] device_release_driver_internal+0x19c/0x200 [148.576365] driver_detach+0x48/0x90 [148.576372] bus_remove_driver+0x6d/0xf0 [148.576383] pci_unregister_driver+0x2e/0xb0 [148.576393] ixgbe_exit_module+0x1c/0xd50 [ixgbe] [148.576430] __do_sys_delete_module.isra.0+0x1bc/0x2e0 [148.576446] do_syscall_64+0x7f/0x980 It can be reproduced by trying to unload ixgbe driver in recovery mode. Fix that by checking if fwlog is supported before doing unroll.	N/A	More Details
CVE-2026-23330	In the Linux kernel, the following vulnerability has been resolved: nfc: nci: complete pending data exchange on device close In nci_close_device(), complete any pending data exchange before closing. The data exchange callback (e.g. rawsock_data_exchange_complete) holds a socket reference. NIPA occasionally hits this leak: unreferenced object 0xff1100000f435000 (size 2048): comm "nci_dev", pid 3954, jiffies 4295441245 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 27 00 01 40 00 00 00 00 00 00 00 00 00 00 00 00 '..@..... backtrace (crc ec2b3c5): __kmalloc_noprof+0x4db/0x730 sk_prot_alloc.isra.0+0xe4/0x1d0 sk_alloc+0x36/0x760 rawsock_create+0xd1/0x540 nfc_sock_create+0x11f/0x280 __sock_create+0x22d/0x630 __sys_socket+0x115/0x1d0 __x64_sys_socket+0x72/0xd0 do_syscall_64+0x117/0xfc0 entry_SYSCALL_64_after_hwframe+0x4b/0x53	N/A	More Details
CVE-2026-23361	In the Linux kernel, the following vulnerability has been resolved: PCI: dwc: ep: Flush MSI-X write before unmapping its ATU entry Endpoint drivers use dw_pcie_ep_raise_msix_irq() to raise an MSI-X interrupt to the host using a writel(), which generates a PCI posted write transaction. There's no completion for posted writes, so the writel() may return before the PCI write completes. dw_pcie_ep_raise_msix_irq() also unmaps the outbound ATU entry used for the PCI write, so the write races with the unmap. If the PCI write loses the race with the ATU unmap, the write may corrupt host memory or cause IOMMU errors, e.g., these when running fio with a larger queue depth against nvmet-pci-epf: arm-smmu-v3 fc900000.iommu: 0x0000010000000010 arm-smmu-v3 fc900000.iommu: 0x0000020000000000 arm-smmu-v3 fc900000.iommu: 0x000000090000f040 arm-smmu-v3 fc900000.iommu: 0x0000000000000000 arm-smmu-v3 fc900000.iommu: event: F_TRANSLATION client: 0000:01:00.0 sid: 0x100 ssid: 0x0 iova: 0x90000f040 ipa: 0x0 arm-smmu-v3 fc900000.iommu: unpriv data write s1 "Input address caused fault" stag: 0x0 Flush the write by performing a readl() of the same address to ensure that the write has reached the destination before the ATU entry is unmapped. The same problem was solved for dw_pcie_ep_raise_msi_irq() in commit 8719c64e76bf ("PCI: dwc: ep: Cache MSI outbound iATU mapping"), but there it was solved by dedicating an outbound iATU only for MSI. We can't do the same for MSI-X because each vector can have a different msg_addr and the msg_addr may be changed while the vector is masked. [bhelgaas: commit log]	N/A	More Details