SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 08 April 2026

Generated on 08 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-2026-32186	Server-side request forgery (ssrf) in Microsoft Bing allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
CVE-2026-33107	Server-side request forgery (ssrf) in Azure Databricks allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
CVE-2026-33105	Improper authorization in Microsoft Azure Kubernetes Service allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
CVE-2026-39337	ChurchCRM is an open-source church management system. Prior to 7.1.0, critical pre-authentication remote code execution vulnerability in ChurchCRM's setup wizard allows unauthenticated attackers to inject arbitrary PHP code during the initial installation process, leading to complete server compromise. The "$dbPassword" variable is not sanitized. This vulnerability exists due to an incomplete fix for CVE-2025-62521. This vulnerability is fixed in 7.1.0.	10.0	More Details
CVE-2026-32213	Improper authorization in Azure AI Foundry allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
CVE-2026-34976	Dgraph is an open source distributed GraphQL database. Prior to 25.3.1, the restoreTenant admin mutation is missing from the authorization middleware config (admin.go), making it completely unauthenticated. Unlike the similar restore mutation which requires Guardian-of-Galaxy authentication, restoreTenant executes with zero middleware. This mutation accepts attacker-controlled backup source URLs (including file:// for local filesystem access), S3/MinIO credentials, encryption key file paths, and Vault credential file paths. An unauthenticated attacker can overwrite the entire database, read server-side files, and perform SSRF. This vulnerability is fixed in 25.3.1.	10.0	More Details
CVE-2026-34208	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.36, SandboxJS blocks direct assignment to global objects (for example Math.random = ...), but this protection can be bypassed through an exposed callable constructor path: this.constructor.call(target, attackerObject). Because this.constructor resolves to the internal SandboxGlobal function and Function.prototype.call is allowed, attacker code can write arbitrary properties into host global objects and persist those mutations across sandbox instances in the same process. This vulnerability is fixed in 0.8.36.	10.0	More Details
CVE-2026-4370	A vulnerability was identified in Juju from version 3.2.0 until 3.6.19 and from version 4.0 until 4.0.4, where the internal Dqlite database cluster fails to perform proper TLS client and server authentication. Specifically, the Juju controller's database endpoint does not validate client certificates when a new node attempts to join the cluster. An unauthenticated attacker with network reachability to the Juju controller's Dqlite port can exploit this flaw to join the database cluster. Once joined, the attacker gains full read and write access to the underlying database, allowing for total data compromise.	10.0	More Details
CVE-2025-54328	An issue was discovered in SMS in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, 9110, W920, W930, W1000, Modem 5123, Modem 5300, and Modem 5400. A Stack-based Buffer Overflow occurs while parsing SMS RP-DATA messages.	10.0	More Details
CVE-2026-34938	PraisonAI is a multi-agent teams system. Prior to version 1.5.90, execute_code() in praisonai-agents runs attacker-controlled Python inside a three-layer sandbox that can be fully bypassed by passing a str subclass with an overridden startswith() method to the _safe_getattr wrapper, achieving arbitrary OS command execution on the host. This issue has been patched in version 1.5.90.	10.0	More Details
CVE-2026-34612	Kestra is an open-source, event-driven orchestration platform. Prior to version 1.3.7, Kestra (default docker-compose deployment) contains a SQL Injection vulnerability that leads to Remote Code Execution (RCE) in the following endpoint "GET /api/v1/main/flows/search". Once a user is authenticated, simply visiting a crafted link is enough to trigger the vulnerability. The injected payload is executed by PostgreSQL using COPY ... TO PROGRAM ..., which in turn runs arbitrary OS commands on the host. This issue has been patched in version 1.3.7.	9.9	More Details

CVE-2026-34569	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 when creating or editing blog categories. An attacker can inject a malicious JavaScript payload into the category title field, which is then stored server-side. This stored payload is later rendered unsafely across public-facing blog category pages, administrative interfaces, and blog post views without proper output encoding, leading to stored cross-site scripting (XSS). This issue has been patched in version 0.31.0.0.	9.9	More Details
CVE-2026-23696	Windmill CE and EE versions 1.276.0 through 1.603.2 contain an SQL injection vulnerability in the folder ownership management functionality that allows authenticated attackers to inject SQL through the owner parameter. An attacker can use the injection to read sensitive data such as the JWT signing secret and administrative user identifiers, forge an administrative token, and then execute arbitrary code via the workflow execution endpoints.	9.9	More Details
CVE-2026-34571	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, a Stored Cross-Site Scripting (Stored XSS) vulnerability exists in the backend user management functionality. The application fails to properly sanitize user-controlled input before rendering it in the administrative interface, allowing attackers to inject persistent JavaScript code. This results in automatic execution whenever backend users access the affected page, enabling session hijacking, privilege escalation, and full administrative account compromise. This issue has been patched in version 0.31.0.0.	9.9	More Details
CVE-2026-34838	Group-Office is an enterprise customer relationship management and groupware tool. Prior to versions 6.8.156, 25.0.90, and 26.0.12, a vulnerability in the AbstractSettingsCollection model leads to insecure deserialization when these settings are loaded. By injecting a serialized FileCookieJar object into a setting string, an authenticated attacker can achieve Arbitrary File Write, leading directly to Remote Code Execution (RCE) on the server. This issue has been patched in versions 6.8.156, 25.0.90, and 26.0.12.	9.9	More Details
CVE-2026-39355	Genealogy is a family tree PHP application. Prior to 5.9.1, a critical broken access control vulnerability in the genealogy application allows any authenticated user to transfer ownership of arbitrary non-personal teams to themselves. This enables complete takeover of other users' team workspaces and unrestricted access to all genealogy data associated with the compromised team. This vulnerability is fixed in 5.9.1.	9.9	More Details
CVE-2026-34717	OpenProject is an open-source, web-based project management software. Prior to version 17.2.3, the =n operator in modules/reporting/lib/report/operator.rb:177 embeds user input directly into SQL WHERE clauses without parameterization. This issue has been patched in version 17.2.3.	9.9	More Details
CVE-2026-25212	An issue was discovered in Percona PMM before 3.7. Because an internal database user retains specific superuser privileges, an attacker with pmm-admin rights can abuse the "Add data source" feature to break out of the database context and execute shell commands on the underlying operating system.	9.9	More Details
CVE-2025-71279	XenForo before 2.3.7 contains a security issue affecting Passkeys that have been added to user accounts. An attacker may be able to compromise the security of Passkey-based authentication.	9.8	More Details
CVE-2026-35171	Kedro is a toolbox for production-ready data science. Prior to 1.3.0, Kedro allows the logging configuration file path to be set via the KEDRO_LOGGING_CONFIG environment variable and loads it without validation. The logging configuration schema supports the special () key, which enables arbitrary callable instantiation. An attacker can exploit this to execute arbitrary system commands during application startup. This is a critical remote code execution (RCE) vulnerability caused by unsafe use of logging.config.dictConfig() with user-controlled input. This vulnerability is fixed in 1.3.0.	9.8	More Details
CVE-2024-14034	Hirschmann HiEOS devices versions prior to 01.1.00 contain an authentication bypass vulnerability in the HTTP(S) management module that allows unauthenticated remote attackers to gain administrative access by sending specially crafted HTTP(S) requests. Attackers can exploit improper authentication handling to obtain elevated privileges and perform unauthorized actions including configuration download or upload and firmware modification.	9.8	More Details
CVE-2017-20237	Hirschmann Industrial HiVision versions prior to 06.0.07 and 07.0.03 contains an authentication bypass vulnerability in the master service that allows unauthenticated remote attackers to execute arbitrary commands with administrative privileges. Attackers can invoke exposed interface methods over the remote service to bypass authentication and achieve remote code execution on the underlying operating system.	9.8	More Details
CVE-2026-34841	Bruno is an open source IDE for exploring and testing APIs. Prior to 3.2.1, Bruno was affected by a supply chain attack involving compromised versions of the axios npm package, which introduced a hidden dependency deploying a cross-platform Remote Access Trojan (RAT). Users of @usebruno/cli who ran npm install between 00:21 UTC and ~03:30 UTC on March 31, 2026 may have been impacted. Upgrade to 3.2.1	9.8	More Details
CVE-2026-31151	An issue in the login mechanism of Kaleris YMS v7.2.2.1 allows attackers to bypass login verification to access the application 's resources.	9.8	More Details
CVE-2018-25237	Hirschmann HiSecOS devices versions prior to 05.3.03 contain a buffer overflow vulnerability in the HTTPS login interface when RADIUS authentication is enabled that allows remote attackers to crash the device or execute arbitrary code by submitting a password longer than 128 characters. Attackers can exploit improper bounds checking in password handling to overflow a fixed-size buffer and achieve denial of service or remote code execution.	9.8	More Details
CVE-2017-20234	GarrettCom Magnum 6K and 10K managed switches contain an authentication bypass vulnerability that allows unauthenticated attackers to gain unauthorized access by exploiting a hardcoded string in the authentication mechanism. Attackers can bypass login controls to access administrative functions and sensitive switch configuration without valid credentials.	9.8	More Details
CVE-2026-31059	A remote command execution (RCE) vulnerability in the /goform/formDia component of UTT Aggressive HiPER 520W v3v1.7.7-180627 allows attackers to execute arbitrary commands via a crafted string.	9.8	More Details
CVE-2017-20236	ProSoft Technology ICX35-HWC versions 1.3 and prior cellular gateways contain an input validation vulnerability in the web user interface that allows remote attackers to inject and execute system commands by submitting malicious input through unvalidated fields. Attackers can exploit this vulnerability to gain root privileges and execute arbitrary commands on the device through the accessible web interface.	9.8	More Details
CVE-2018-25236	Hirschmann HiOS and HiSecOS products RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED, EAGLE contain an authentication bypass vulnerability in the HTTP(S) management module that allows unauthenticated remote attackers to gain administrative access by crafting specially formed HTTP requests. Attackers can exploit improper authentication handling to obtain the authentication status and privileges of a previously authenticated user without providing valid credentials.	9.8	More Details
CVE-2019-	Pegasus CMS 1.0 contains a remote code execution vulnerability in the extra_fields.php plugin that allows unauthenticated		

25687	attackers to execute arbitrary commands by exploiting unsafe eval functionality. Attackers can send POST requests to the submit.php endpoint with malicious PHP code in the action parameter to achieve code execution and obtain an interactive shell.	9.8	More Details
CVE-2026-34934	PraisonAI is a multi-agent teams system. Prior to version 4.5.90, the get_all_user_threads function constructs raw SQL queries using f-strings with unescaped thread IDs fetched from the database. An attacker stores a malicious thread ID via update_thread. When the application loads the thread list, the injected payload executes and grants full database access. This issue has been patched in version 4.5.90.	9.8	More Details
CVE-2026-34935	PraisonAI is a multi-agent teams system. From version 4.5.15 to before version 4.5.69, the --mcp CLI argument is passed directly to shlex.split() and forwarded through the call chain to anyio.open_process() with no validation, allowlist check, or sanitization at any hop, allowing arbitrary OS command execution as the process user. This issue has been patched in version 4.5.69.	9.8	More Details
CVE-2018-25254	NICO-FTP 3.0.1.19 contains a structured exception handler buffer overflow vulnerability that allows remote attackers to execute arbitrary code by sending crafted FTP commands. Attackers can connect to the FTP service and send oversized data in response handlers to overwrite SEH pointers and redirect execution to injected shellcode.	9.8	More Details
CVE-2026-34877	An issue was discovered in Mbed TLS versions from 2.19.0 up to 3.6.5, Mbed TLS 4.0.0. Insufficient protection of serialized SSL context or session structures allows an attacker who can modify the serialized structures to induce memory corruption, leading to arbitrary code execution. This is caused by Incorrect Use of Privileged APIs.	9.8	More Details
CVE-2026-33746	Convoy is a KVM server management panel for hosting businesses. From version 3.9.0-beta to before version 4.5.1, the JWTService::decode() method did not verify the cryptographic signature of JWT tokens. While the method configured a symmetric HMAC-SHA256 signer via lcobucci/jwt, it only validated time-based claims (exp, nbf, iat) using the StrictValidAt constraint. The SignedWith constraint was not included in the validation step. This means an attacker could forge or tamper with JWT token payloads — such as modifying the user_uuid claim — and the token would be accepted as valid, as long as the time-based claims were satisfied. This directly impacts the SSO authentication flow (LoginController::authorizeToken), allowing an attacker to authenticate as any user by crafting a token with an arbitrary user_uuid. This issue has been patched in version 4.5.1.	9.8	More Details
CVE-2026-35616	A improper access control vulnerability in Fortinet FortiClientEMS 7.4.5 through 7.4.6 may allow an unauthenticated attacker to execute unauthorized code or commands via crafted requests.	9.8	More Details
CVE-2026-20911	A heap-based buffer overflow vulnerability exists in the HuffTable::initval functionality of LibRaw Commit 0b56545 and Commit d20315b. A specially crafted malicious file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2026-29014	MetInfo CMS versions 7.9, 8.0, and 8.1 contain an unauthenticated PHP code injection vulnerability that allows remote attackers to execute arbitrary code by sending crafted requests with malicious PHP code. Attackers can exploit insufficient input neutralization in the execution path to achieve remote code execution and gain full control over the affected server.	9.8	More Details
CVE-2026-31027	TOTOlink A3600R v5.9c.4959 contains a buffer overflow vulnerability in the setAppEasyWizardConfig interface of /lib/cste_modules/app.so. The vulnerability occurs because the rootSsid parameter is not properly validated for length, allowing remote attackers to trigger a buffer overflow, potentially leading to arbitrary code execution or denial of service.	9.8	More Details
CVE-2024-40489	There is an injection vulnerability in jeecg boot versions 3.0.0 to 3.5.3 due to lax character filtering, which allows attackers to execute arbitrary code on components through specially crafted HTTP requests.	9.8	More Details
CVE-2024-43028	A command injection vulnerability in the component /jmreport/show of jeecg boot v3.0.0 to v3.5.3 allows attackers to execute arbitrary code via a crafted HTTP request.	9.8	More Details
CVE-2026-20093	A vulnerability in the change password functionality of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to bypass authentication and gain access to the system as Admin. This vulnerability is due to incorrect handling of password change requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to bypass authentication, alter the passwords of any user on the system, including an Admin user, and gain access to the system as that user.	9.8	More Details
CVE-2026-20160	A vulnerability in Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected SSM On-Prem host. This vulnerability is due to the unintentional exposure of an internal service. An attacker could exploit this vulnerability by sending a crafted request to the API of the exposed service. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges.	9.8	More Details
CVE-2026-30643	An issue was discovered in DedeCMS 5.7.118 allowing attackers to execute code via crafted setup tag values in a module upload.	9.8	More Details
CVE-2026-34159	llama.cpp is an inference of several LLM models in C/C++. Prior to version b8492, the RPC backend's deserialize_tensor() skips all bounds validation when a tensor's buffer field is 0. An unauthenticated attacker can read and write arbitrary process memory via crafted GRAPH_COMPUTE messages. Combined with pointer leaks from ALLOC_BUFFER/BUFFER_GET_BASE, this gives full ASLR bypass and remote code execution. No authentication required, just TCP access to the RPC server port. This issue has been patched in version b8492.	9.8	More Details
CVE-2026-34875	An issue was discovered in Mbed TLS through 3.6.5 and TF-PSA-Crypto 1.0.0. A buffer overflow can occur in public key export for FFDH keys.	9.8	More Details
CVE-2026-4631	Cockpit's remote login feature passes user-supplied hostnames and usernames from the web interface to the SSH client without validation or sanitization. An attacker with network access to the Cockpit web service can craft a single HTTP request to the login endpoint that injects malicious SSH options or shell commands, achieving code execution on the Cockpit host without valid credentials. The injection occurs during the authentication flow before any credential verification takes place, meaning no login is required to exploit the vulnerability.	9.8	More Details
CVE-2026-35490	changedetection.io is a free open source web page change detection tool. Prior to 0.54.8, the @login_optionally_required decorator is placed before (outer to) @blueprint.route() instead of after it. In Flask, @route() must be the outermost decorator because it registers the function it receives. When the order is reversed, @route() registers the original undecorated function, and the auth wrapper is never in the call chain. This silently disables authentication on these routes. This vulnerability is fixed in 0.54.8.	9.8	More Details
	A heap-based buffer overflow vulnerability exists in the lossless_jpeg_load_raw functionality of LibRaw Commit 0b56545 and		

CVE-2026-21413	Commit d20315b. A specially crafted malicious file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2026-22679	Weaver (Fanwei) E-cology 10.0 versions prior to 20260312 contain an unauthenticated remote code execution vulnerability in the /papi/esearch/data/devops/dubboApi/debug/method endpoint that allows attackers to execute arbitrary commands by invoking exposed debug functionality. Attackers can craft POST requests with attacker-controlled interfaceName and methodName parameters to reach command-execution helpers and achieve arbitrary command execution on the system. Exploitation evidence was first observed by the Shadowserver Foundation on 2026-03-31 (UTC).	9.8	More Details
CVE-2026-5731	Memory safety bugs present in Firefox ESR 115.34.0, Firefox ESR 140.9.0, Thunderbird ESR 140.9.0, Firefox 149.0.1 and Thunderbird 149.0.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 149.0.2, Firefox ESR < 115.34.1, Firefox ESR < 140.9.1, Thunderbird < 149.0.2, and Thunderbird < 140.9.1.	9.8	More Details
CVE-2026-35022	Anthropic Claude Code CLI and Claude Agent SDK contain an OS command injection vulnerability in authentication helper execution where helper configuration values are executed using shell=true without input validation. Attackers who can influence authentication settings can inject shell metacharacters through parameters like apiKeyHelper, awsAuthRefresh, awsCredentialExport, and gcpAuthRefresh to execute arbitrary commands with the privileges of the user or automation environment, enabling credential theft and environment variable exfiltration.	9.8	More Details
CVE-2026-2699	Customer Managed ShareFile Storage Zones Controller (SZC) allows an unauthenticated attacker to access restricted configuration pages. This leads to changing system configuration and potential remote code execution.	9.8	More Details
CVE-2026-35184	EcclesiaCRM is CRM Software for church management. Prior to 8.0.0, there is a SQL injection vulnerability in v2/templates/query/queryview.php via the custom and value parameters. This vulnerability is fixed in 8.0.0.	9.8	More Details
CVE-2026-0740	The Ninja Forms - File Uploads plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'NF_FU_AJAX_Controllers_Uploads::handle_upload' function in all versions up to, and including, 3.3.26. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. Note: The vulnerability was partially patched in version 3.3.25 and fully patched in version 3.3.27.	9.8	More Details
CVE-2021-4473	Tianxin Internet Behavior Management System contains a command injection vulnerability in the Reporter component endpoint that allows unauthenticated attackers to execute arbitrary commands by supplying a crafted objClass parameter containing shell metacharacters and output redirection. Attackers can exploit this vulnerability to write malicious PHP files into the web root and achieve remote code execution with the privileges of the web server process. This vulnerability has been fixed in version NACFirmware_4.0.0.7_20210716.180815_topsec_0_basic.bin. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-06-01 (UTC).	9.8	More Details
CVE-2016-20052	Snews CMS 1.7 contains an unrestricted file upload vulnerability that allows unauthenticated attackers to upload arbitrary files including PHP executables to the snews_files directory. Attackers can upload malicious PHP files through the multipart form-data upload endpoint and execute them by accessing the uploaded file path to achieve remote code execution.	9.8	More Details
CVE-2026-5734	Memory safety bugs present in Firefox ESR 140.9.0, Thunderbird ESR 140.9.0, Firefox 149.0.1 and Thunderbird 149.0.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 149.0.2, Firefox ESR < 140.9.1, Thunderbird < 149.0.2, and Thunderbird < 140.9.1.	9.8	More Details
CVE-2026-5735	Memory safety bugs present in Firefox 149.0.1 and Thunderbird 149.0.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 149.0.2 and Thunderbird < 149.0.2.	9.8	More Details
CVE-2026-20889	A heap-based buffer overflow vulnerability exists in the x3f_thumb_loader functionality of LibRaw Commit d20315b. A specially crafted malicious file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2026-26135	Server-side request forgery (ssrf) in Azure Custom Locations Resource Provider (RP) allows an authorized attacker to elevate privileges over a network.	9.6	More Details
CVE-2026-28373	The Stackfield Desktop App before 1.10.2 for macOS and Windows contains a path traversal vulnerability in certain decryption functionality when processing the filePath property. A malicious export can write arbitrary content to any path on the victim's filesystem.	9.6	More Details
CVE-2026-5288	Use after free in WebView in Google Chrome on Android prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-5290	Use after free in Compositing in Google Chrome prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-5289	Use after free in Navigation in Google Chrome prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-31818	Budibase is an open-source low-code platform. Prior to version 3.33.4, a server-side request forgery (SSRF) vulnerability exists in Budibase's REST datasource connector. The platform's SSRF protection mechanism (IP blacklist) is rendered completely ineffective because the BLACKLIST_IPS environment variable is not set by default in any of the official deployment configurations. When this variable is empty, the blacklist function unconditionally returns false, allowing all requests through without restriction. This issue has been patched in version 3.33.4.	9.6	More Details
CVE-2026-33950	Signal K Server is a server application that runs on a central hub in a boat. Prior to version 2.24.0-beta.4, there is a privilege escalation vulnerability by Admin Role Injection via /enableSecurity. An unauthenticated attacker can gain full Administrator access to the SignalK server at any time, allowing them to modify sensitive vessel routing data, alter server configurations, and access restricted endpoints. This issue has been patched in version 2.24.0-beta.4.	9.4	More Details
CVE-2026-39397	@delmaredigital/payload-puck is a PayloadCMS plugin for integrating Puck visual page builder. Prior to 0.6.23, all /api/puck/* CRUD endpoint handlers registered by createPuckPlugin() called Payload's local API with the default overrideAccess: true, bypassing all collection-level access control. The access option passed to createPuckPlugin() and any access rules defined on Puck-registered collections were silently ignored on these endpoints. This vulnerability is fixed in 0.6.23.	9.4	More Details

CVE-2026-28766	A specific endpoint exposes all user account information for registered Gardyn users without requiring authentication.	9.3	More Details
CVE-2026-34953	PraisonAI is a multi-agent teams system. Prior to version 4.5.97, OAuthManager.validate_token() returns True for any token not found in its internal store, which is empty by default. Any HTTP request to the MCP server with an arbitrary Bearer token is treated as authenticated, granting full access to all registered tools and agent capabilities. This issue has been patched in version 4.5.97.	9.1	More Details
CVE-2026-34520	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, the C parser (the default for most installs) accepted null bytes and control characters in response headers. This issue has been patched in version 3.13.4.	9.1	More Details
CVE-2026-34566	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 Page Management functionality when creating or editing pages. Multiple input fields accept attacker-controlled JavaScript payloads that are stored server-side. These stored values are later rendered without proper output encoding across administrative page lists and public-facing page views, leading to stored DOM-based cross-site scripting (XSS). This issue has been patched in version 0.31.0.0.	9.1	More Details
CVE-2026-34565	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 when adding Posts to navigation menus through the Menu Management functionality. Post-related data selected via the Posts section is stored server-side and rendered without proper output encoding. These stored values are later rendered unsafely within administrative dashboards and public-facing navigation menus, 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-2026-34564	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 when adding Pages to navigation menus through the Menu Management functionality. Page-related data selected via the Pages section is stored server-side and rendered without proper output encoding. This stored payload is later rendered unsafely within administrative interfaces and public-facing navigation menus, leading to stored DOM-based cross-site scripting (XSS). This issue has been patched in version 0.31.0.0.	9.1	More Details
CVE-2026-34563	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 when handling backup uploads and processing backup metadata. An attacker can inject a malicious JavaScript payload into the backup filename via the uploaded xss.sql, which uses SQL functionality to insert the XSS payload server-side. This stored payload is later rendered unsafely in multiple backup management views without proper output encoding, leading to stored blind cross-site scripting (Blind XSS). This issue has been patched in version 0.31.0.0.	9.1	More Details
CVE-2026-34560	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 renders user-controlled input unsafely within the logs interface. If any stored XSS payload exists within logged data, it is rendered without proper output encoding. This issue becomes a Blind XSS scenario because the attacker does not see immediate execution. Instead, the payload is stored within application logs and only executes later when an administrator views the logs page. This issue has been patched in version 0.31.0.0.	9.1	More Details
CVE-2026-34559	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 when creating or editing blog tags. An attacker can inject a malicious JavaScript payload into the tag name field, which is then stored server-side. This stored payload is later rendered unsafely across public tag pages and administrative interfaces without proper output encoding, leading to stored cross-site scripting (XSS). This issue has been patched in version 0.31.0.0.	9.1	More Details
CVE-2026-34873	An issue was discovered in Mbed TLS 3.5.0 through 4.0.0. Client impersonation can occur while resuming a TLS 1.3 session.	9.1	More Details
CVE-2026-34872	An issue was discovered in Mbed TLS 3.5.x and 3.6.x through 3.6.5 and TF-PSA-Crypto 1.0. There is a lack of contributory behavior in FFDH due to improper input validation. Using finite-field Diffie-Hellman, the other party can force the shared secret into a small set of values (lack of contributory behavior). This is a problem for protocols that depend on contributory behavior (which is not the case for TLS). The attack can be carried by the peer, or depending on the protocol by an active network attacker (person in the middle).	9.1	More Details
CVE-2026-34952	PraisonAI is a multi-agent teams system. Prior to version 4.5.97, the PraisonAI Gateway server accepts WebSocket connections at /ws and serves agent topology at /info with no authentication. Any network client can connect, enumerate registered agents, and send arbitrary messages to agents and their tool sets. This issue has been patched in version 4.5.97.	9.1	More Details
CVE-2026-35580	Emissary is a P2P based data-driven workflow engine. Prior to 8.39.0, GitHub Actions workflow files contained shell injection points where user-controlled workflow_dispatch inputs were interpolated directly into shell commands via ${{ }} expression syntax. An attacker with repository write access could inject arbitrary shell commands, leading to repository poisoning and supply chain compromise affecting all downstream users. This vulnerability is fixed in 8.39.0.	9.1	More Details
CVE-2026-34456	Reviactyl is an open-source game server management panel built using Laravel, React, FilamentPHP, Vite, and Go. From version 26.2.0-beta.1 to before version 26.2.0-beta.5, a vulnerability in the OAuth authentication flow allowed automatic linking of social accounts based solely on matching email addresses. An attacker could create or control a social account (e.g., Google, GitHub, Discord) using a victim’s email address and gain full access to the victim's account without knowing their password. This results in a full account takeover with no prior authentication required. This issue has been patched in version 26.2.0-beta.5.	9.1	More Details
CVE-2026-35573	ChurchCRM is an open-source church management system. Prior to 6.5.3, a path traversal vulnerability in ChurchCRM's backup restore functionality allows authenticated administrators to upload arbitrary files and achieve remote code execution by overwriting Apache .htaccess configuration files. The vulnerability exists in src/ChurchCRM/Backup/RestoreJob.php. The $rawUploadedFile['name'] parameter is user-controlled and allows uploading files with arbitrary names to /var/www/html/tmp_attach/ChurchCRMBackups/. This vulnerability is fixed in 6.5.3.	9.1	More Details
CVE-2026-34751	Payload is a free and open source headless content management system. Prior to version 3.79.1 in @payloadcms/graphql and payload, a vulnerability in the password recovery flow could allow an unauthenticated attacker to perform actions on behalf of a user who initiates a password reset. This issue has been patched in version 3.79.1 for @payloadcms/graphql and payload.	9.1	More Details
	ChurchCRM is an open-source church management system. Prior to 7.1.0, a critical authentication bypass vulnerability in		

CVE-2026-39339	ChurchCRM's API middleware (ChurchCRM/Slim/Middleware/AuthMiddleware.php) allows unauthenticated attackers to access all protected API endpoints by including "api/public" anywhere in the request URL, leading to complete exposure of church member data and system information. This vulnerability is fixed in 7.1.0.	9.1	More Details
CVE-2026-33990	Docker Model Runner (DMR) is software used to manage, run, and deploy AI models using Docker. Prior to version 1.1.25, Docker Model Runner contains an SSRF vulnerability in its OCI registry token exchange flow. When pulling a model, Model Runner follows the realm URL from the registry's WWW-Authenticate header without validating the scheme, hostname, or IP range. A malicious OCI registry can set the realm to an internal URL (e.g., http://127.0.0.1:3000/), causing Model Runner running on the host to make arbitrary GET requests to internal services and reflect the full response body back to the caller. Additionally, the token exchange mechanism can relay data from internal services back to the attacker-controlled registry via the Authorization: Bearer header. This issue has been patched in version 1.1.25. For Docker Desktop users, enabling Enhanced Container Isolation (ECI) blocks container access to Model Runner, preventing exploitation. However, if the Docker Model Runner is exposed to localhost over TCP in specific configurations, the vulnerability is still exploitable.	9.1	More Details
CVE-2025-15484	The Order Notification for WooCommerce WordPress plugin before 3.6.3 overrides WooCommerce's permission checks to grant full access to all unauthenticated requests, enabling complete read/write access to store resources like products, coupons, and customers.	9.1	More Details
CVE-2026-34567	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 when creating or editing blog posts within the Categories section. An attacker can inject a malicious JavaScript payload into the Categories content, which is then stored server-side. This stored payload is later rendered unsafely when the Categories are viewed via blog posts, without proper output encoding, leading to stored cross-site scripting (XSS). This issue has been patched in version 0.31.0.0.	9.1	More Details
CVE-2026-34568	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 when creating or editing blog posts. An attacker can inject a malicious JavaScript payload into blog post content, which is then stored server-side. This stored payload is later rendered unsafely in multiple application views without proper output encoding, leading to stored cross-site scripting (XSS). This issue has been patched in version 0.31.0.0.	9.1	More Details
CVE-2026-35459	pyLoad is a free and open-source download manager written in Python. In 0.5.0b3.dev96 and earlier, pyLoad has a server-side request forgery (SSRF) vulnerability. The fix for CVE-2026-33992 added IP validation to BaseDownloader.download() that checks the hostname of the initial download URL. However, pycurl is configured with FOLLOWLOCATION=1 and MAXREDIRS=10, causing it to automatically follow HTTP redirects. Redirect targets are never validated against the SSRF filter. An authenticated user with ADD permission can bypass the SSRF fix by submitting a URL that redirects to an internal address.	9.1	More Details
CVE-2026-35030	LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. Prior to 1.83.0, when JWT authentication is enabled (enable_jwt_auth: true), the OIDC userinfo cache uses token[:20] as the cache key. JWT headers produced by the same signing algorithm generate identical first 20 characters. This configuration option is not enabled by default. Most instances are not affected. An unauthenticated attacker can craft a token whose first 20 characters match a legitimate user's cached token. On cache hit, the attacker inherits the legitimate user's identity and permissions. This affects deployments with JWT/OIDC authentication enabled. Fixed in v1.83.0.	9.1	More Details
CVE-2021-4477	Hirschmann HiLCOS OpenBAT and BAT450 products contain a firewall bypass vulnerability in IPv6 IPsec deployments that allows traffic from VPN connections to bypass configured firewall rules. Attackers can exploit this vulnerability by establishing IPv6 IPsec connections (IKEv1 or IKEv2) while simultaneously using an IPv6 Internet connection to circumvent firewall policy enforcement.	9.1	More Details
CVE-2026-26026	GLPI is a free asset and IT management software package. From 11.0.0 to before 11.0.6, template injection by an administrator lead to RCE. This vulnerability is fixed in 11.0.6.	9.1	More Details
CVE-2017-20235	ProSoft Technology ICX35-HWC version 1.3 and prior cellular gateways contain an authentication bypass vulnerability in the web user interface that allows unauthenticated attackers to gain access to administrative functions without valid credentials. Attackers can bypass the authentication mechanism in affected firmware versions to obtain full administrative access to device configuration and settings.	9.1	More Details
CVE-2026-25197	A specific endpoint allows authenticated users to pivot to other user profiles by modifying the id number in the API call.	9.1	More Details
CVE-2026-34950	fast-jwt provides fast JSON Web Token (JWT) implementation. In 6.1.0 and earlier, the publicKeyPemMatcher regex in fast-jwt/src/crypto.js uses a ^ anchor that is defeated by any leading whitespace in the key string, re-enabling the exact same JWT algorithm confusion attack that CVE-2023-48223 patched.	9.1	More Details
CVE-2026-33615	An unauthenticated remote attacker can exploit an unauthenticated SQL Injection vulnerability in the setinfo endpoint due to improper neutralization of special elements in a SQL UPDATE command. This can result in a total loss of integrity and availability.	9.1	More Details
CVE-2026-32211	Missing authentication for critical function in Azure MCP Server allows an unauthorized attacker to disclose information over a network.	9.1	More Details
CVE-2026-35039	fast-jwt provides fast JSON Web Token (JWT) implementation. From 0.0.1 to before 6.1.0, setting up a custom cacheKeyBuilder method which does not properly create unique keys for different tokens can lead to cache collisions. This could cause tokens to be mis-identified during the verification process leading to valid tokens returning claims from different valid tokens and users being mis-identified as other users based on the wrong token.	9.1	More Details
CVE-2026-35050	text-generation-webui is an open-source web interface for running Large Language Models. Prior to 4.1.1, users can save extention settings in "py" format and in the app root directory. This allows to overwrite python files, for instance the "download-model.py" file could be overwritten. Then, this python file can be triggered to get executed from "Model" menu when requesting to download a new model. This vulnerability is fixed in 4.1.1.	9.1	More Details
CVE-2026-34758	OneUptime is an open-source monitoring and observability platform. Prior to version 10.0.42, unauthenticated access to Notification test and Phone Number management endpoints allows SMS/Call/Email/WhatsApp abuse and phone number purchase. This issue has been patched in version 10.0.42.	9.1	More Details
CVE-2026-35174	Chyrp Lite is an ultra-lightweight blogging engine. Prior to 2026.01, a path traversal vulnerability exists in the administration console that allows an administrator or a user with Change Settings permission to change the uploads path to any folder. This vulnerability allows the user to download any file on the server, including config.json.php with database credentials and	9.1	More Details

	overwrite critical system files, leading to remote code execution. This vulnerability is fixed in 2026.01.		
CVE-2025-58349	An issue was discovered in L2 in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, 9110, W920, W930, W1000, Modem 5123, Modem 5300, and Modem 5400. Incorrect handling of LTE MAC packets containing many MAC Control Elements (CEs) leads to baseband crashes.	9.1	More Details
CVE-2026-34745	Fireshare facilitates self-hosted media and link sharing. Prior to version 1.5.3, the fix for CVE-2026-33645 was applied to the authenticated /api/uploadChunked endpoint but was not applied to the unauthenticated /api/uploadChunked/public endpoint in the same file (app/server/fireshare/api.py). An unauthenticated attacker can exploit the checkSum parameter to write arbitrary files with attacker-controlled content to any writable path on the server filesystem. This issue has been patched in version 1.5.3.	9.1	More Details
CVE-2026-2701	Authenticated user can upload a malicious file to the server and execute it, which leads to remote code execution.	9.1	More Details
CVE-2026-39847	Emmett is a full-stack Python web framework designed with simplicity. From 2.5.0 to before 2.8.1, the RSGI static handler for Emmett's internal assets (/__emmett__ paths) is vulnerable to path traversal attacks. An attacker can use ../ sequences (eg /__emmett__/../rsgi/handlers.py) to read arbitrary files outside the assets directory. This vulnerability is fixed in 2.8.1.	9.1	More Details
CVE-2026-35216	Budibase is an open-source low-code platform. Prior to version 3.33.4, an unauthenticated attacker can achieve Remote Code Execution (RCE) on the Budibase server by triggering an automation that contains a Bash step via the public webhook endpoint. No authentication is required to trigger the exploit. The process executes as root inside the container. This issue has been patched in version 3.33.4.	9.0	More Details
CVE-2026-39305	PraisonAI is a multi-agent teams system. Prior to 1.5.113, the Action Orchestrator feature contains a Path Traversal vulnerability that allows an attacker (or compromised agent) to write to arbitrary files outside of the configured workspace directory. By supplying relative path segments (../) in the target path, malicious actions can overwrite sensitive system files or drop executable payloads on the host. This vulnerability is fixed in 1.5.113.	9.0	More Details
CVE-2026-28798	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. Prior to version 1.5.3, a proxy endpoint (/v1/sys/proxy) exposed by ZimaOS's web interface can be abused (via an externally reachable domain using a Cloudflare Tunnel) to make requests to internal localhost services. This results in unauthenticated access to internal-only endpoints and sensitive local services when the product is reachable from the Internet through a Cloudflare Tunnel. This issue has been patched in version 1.5.3.	9.0	More Details
CVE-2026-39846	SiYuan is a personal knowledge management system. Prior to 3.6.4, a malicious note synced to another user can trigger remote code execution in the SiYuan Electron desktop client. The root cause is that table caption content is stored without safe escaping and later unescaped into rendered HTML, creating a stored XSS sink. Because the desktop renderer runs with nodeIntegration enabled and contextIsolation disabled, attacker-controlled JavaScript executes with access to Node.js APIs. In practice, an attacker can import a crafted note into a synced workspace, wait for the victim to sync, and achieve code execution when the victim opens the note. This vulnerability is fixed in 3.6.4.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2026-39328	ChurchCRM is an open-source church management system. Prior to 7.1.0, a stored cross-site scripting vulnerability exists in ChurchCRM's person profile editing fur malicious JavaScript into their Facebook, LinkedIn, and X profile fields. Due to a 50-character field limit, the payload is distributed across all three fields and chains administrators, views the attacker's profile, their session cookies are exfiltrated to a remote server. This vulnerability is fixed in 7.1.0.
CVE-2026-35463	pyLoad is a free and open-source download manager written in Python. In 0.5.0b3.dev96 and earlier, the ADMIN_ONLY_OPTIONS protection mechanism restricts se admin-only access. However, this protection is only applied to core config options, not to plugin config options. The AntiVirus plugin stores an executable path (avfi SETTINGS permission can change this path to achieve remote code execution.
CVE-2025-43219	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.6. Processing a maliciously crafted image may corrupt process
CVE-2026-5610	A vulnerability has been found in Belkin F9K1015 1.00.10. Affected by this issue is the function formWISP5G of the file /goform/formWISP5G. Such manipulation of t 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 an
CVE-2026-34572	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 account is deactivated. Due to a logic flaw in the backend design, account state changes are enforced only during authentication (login), not for already-establishe the lifetime of their session. There is no session expiration or account expiration mechanism in place, causing deactivated accounts to retain indefinite access until and results in persistent unauthorized access, representing a critical security flaw. This issue has been patched in version 0.31.0.0.
CVE-2025-43202	This issue was addressed with improved memory handling. This issue is fixed in iOS 18.6 and iPadOS 18.6, macOS Sequoia 15.6. Processing a file may lead to mem
CVE-2026-5709	Unsanitized input in the FileBrowser API in AWS Research and Engineering Studio (RES) version 2024.10 through 2025.12.01 might allow a remote authenticated a input when using the FileBrowser functionality. To remediate this issue, users are advised to upgrade to RES version 2026.03 or apply the corresponding mitigation
CVE-2026-5708	Unsanitized control of user-modifiable attributes in the session creation component in AWS Research and Engineering Studio (RES) prior to version 2026.03 could a host instance profile permissions, and interact with AWS resources and services via a crafted API request. To remediate this issue, users are advised to upgrade to environment.
CVE-2026-5707	Unsanitized input in an OS command in the virtual desktop session name handling in AWS Research and Engineering Studio (RES) version 2025.03 through 2025.1 on the virtual desktop host via a crafted session name. To remediate this issue, users are advised to upgrade to RES version 2026.03 or apply the corresponding m
CVE-2026-5687	A weakness has been identified in Tenda CX12L 16.03.53.12. This issue affects the function fromNatStaticSetting of the file /goform/NatStaticSetting. This manipula initiated remotely. The exploit has been made available to the public and could be used for attacks.

CVE-2026-5686	A security flaw has been discovered in Tenda CX12L 16.03.53.12. This vulnerability affects the function fromRouteStatic of the file /goform/RouteStatic. The manipu launched remotely. The exploit has been released to the public and may be used for attacks.
CVE-2026-5685	A vulnerability was identified in Tenda CX12L 16.03.53.12. This affects the function fromAddressNat of the file /goform/addressNat. The manipulation of the argum The exploit is publicly available and might be used.
CVE-2023-7342	HiSecOS web server versions 03.4.00 prior to 04.1.00 contains a privilege escalation vulnerability that allows authenticated users with operator or auditor roles to e web server. Attackers can exploit this flaw to gain full administrative access to the affected device.
CVE-2026-34570	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 account is deleted. Due to a logic flaw in the backend design, account state changes are enforced only during authentication (login), not for already-established se lifetime of their session. There is no session expiration or account expiration mechanism in place, causing deleted accounts to retain indefinite access until the use results in persistent unauthorized access. This issue has been patched in version 0.31.0.0.
CVE-2026-34430	ByteDance Deer-Flow versions prior to commit 92c7a20 contain a sandbox escape vulnerability in bash tool handling that allows attackers to execute arbitrary com such as directory changes and relative paths. Attackers can exploit the incomplete shell semantics modeling to read and modify files outside the sandbox boundar interpretation enabled.
CVE-2026-0522	A local file inclusion vulnerability in the upload/download flow of the VertiGIS FM application allows authenticated attackers to read arbitrary files from the server b downloaded, the file in the attacker controlled path is returned. Due to the application's ASP.NET architecture, this could potentially lead to remote code execution paths which may enable NTLM-relaying attacks. This issue affects VertiGIS FM: 10.5.00119 (0d29d428).
CVE-2026-5628	A security vulnerability has been detected in Belkin F9K1015 1.00.10. Impacted is the function formSetSystemSettings of the file /goform/formSetSystemSettings o stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor was contacted ear
CVE-2026-5612	A vulnerability was determined in Belkin F9K1015 1.00.10. This vulnerability affects the function formWlEncrypt of the file /goform/formWlEncrypt. Executing a mar 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 res
CVE-2026-3666	The wpForo Forum plugin for WordPress is vulnerable to arbitrary file deletion in all versions up to, and including, 2.4.16. This is due to a missing file name/path va attackers, with subscriber level access and above, to delete arbitrary files on the server by embedding a crafted path traversal string in a forum post body and the
CVE-2026-24096	Insufficient permission validation on multiple REST API Quick Setup endpoints in Checkmk 2.5.0 (beta) before version 2.5.0b2 and 2.4.0 before version 2.4.0p25 all information
CVE-2026-35395	WeGIA is a Web manager for charitable institutions. Prior to 3.6.9, WeGIA (Web gerenciador para instituições assistenciais) contains a SQL injection vulnerability in $_REQUEST without validation and directly interpolated into SQL queries, allowing any authenticated user to execute arbitrary SQL commands against the databas
CVE-2026-39317	ChurchCRM is an open-source church management system. Prior to 7.1.0, a SQL injection vulnerability exists in ChurchCRM's SettingsIndividual.php where user-co without sanitization. This allows any authenticated user to extract sensitive data from the database. This vulnerability is fixed in 7.1.0.
CVE-2026-39318	ChurchCRM is an open-source church management system. Prior to 7.1.0, the GroupPropsFormRowOps.php file contains a SQL injection vulnerability. User input in The mysqli_real_escape_string() function does not escape backtick characters, allowing attackers to break out of SQL identifier context and execute arbitrary SQL s
CVE-2026-39319	ChurchCRM is an open-source church management system. Prior to 7.1.0, a second order SQL injection vulnerability was found in the endpoint /FundRaiserEditor.p These users can inject arbitrary SQL statements through the iCurrentFundraiser PHP session parameter and thus extract and modify information from the database
CVE-2026-39323	ChurchCRM is an open-source church management system. Prior to 7.1.0, a critical SQL injection vulnerability exists in ChurchCRM's PropertyTypeEditor.php where direct concatenation into SQL queries. This allows authenticated users with "Manage Properties" permission to execute arbitrary SQL commands including data exf reflected across multiple application pages without output encoding. This vulnerability is fixed in 7.1.0.
CVE-2026-39326	ChurchCRM is an open-source church management system. Prior to 7.1.0, an SQL injection vulnerability was found in the endpoint /PropertyTypeEditor.php in Chur SQL statements through the Name and Description parameters and thus extract and modify information from the database. This vulnerability is fixed in 7.1.0.
CVE-2026-39327	ChurchCRM is an open-source church management system. Prior to 7.1.0, an SQL injection vulnerability was found in the endpoint /MemberRoleChange.php in Chu (ManageGroups) can inject arbitrary SQL statements through the NewRole parameter and thus extract and modify information from the database. This vulnerabilit
CVE-2026-34955	PraisonAI is a multi-agent teams system. Prior to version 4.5.97, SubprocessSandbox in all modes (BASIC, STRICT, NETWORK_ISOLATED) calls subprocess.run() with commands. The blocklist does not include sh or bash as standalone executables, allowing trivial sandbox escape in STRICT mode via sh -c '<command>'. This issu
CVE-2026-5613	A vulnerability was identified in Belkin F9K1015 1.00.10. This issue affects the function formReboot of the file /goform/formReboot. The manipulation of the argume 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.
CVE-2026-5614	A security flaw has been discovered in Belkin F9K1015 1.00.10. Impacted is the function formSetPassword of the file /goform/formSetPassword. The manipulation o 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 resp
CVE-2026-5544	A security flaw has been discovered in UTT HiPER 1250GW up to 3.2.7-210907-180535. The impacted element is an unknown function of the file /goform/formRemo overflow. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.
CVE-2026-35093	A flaw was found in libinput. A local attacker who can place a specially crafted Lua bytecode file in certain system or user configuration directories can bypass secu permissions as the program using libinput, such as a graphical compositor. This could lead to the attacker monitoring keyboard input and sending that information

CVE-2026-35610	PolarLearn is a free and open-source learning program. In 0-PRERELEASE-14 and earlier, setCustomPassword(userId, password) and deleteUser(userId) in the accou condition, authenticated non-admin users were allowed to execute both actions, while real admins were rejected. This is a direct privilege-escalation issue in the ap
CVE-2026-5609	A flaw has been found in Tenda i12 1.0.0.11(3862). Affected by this vulnerability is the function formwrlSSIDset of the file /goform/wifiSSIDset of the component Pa based buffer overflow. It is possible to initiate the attack remotely. The exploit has been published and may be used.
CVE-2019-25685	phpBB contains an arbitrary file upload vulnerability that allows authenticated attackers to upload malicious files by exploiting the plupload functionality and phar:/ objects that execute arbitrary code when deserialized through the imagick parameter in attachment settings.
CVE-2026-5733	Incorrect boundary conditions in the Graphics: WebGPU component. This vulnerability affects Firefox < 149.0.2 and Thunderbird < 149.0.2.
CVE-2026-5732	Incorrect boundary conditions, integer overflow in the Graphics: Text component. This vulnerability affects Firefox < 149.0.2, Firefox ESR < 140.9.1, Thunderbird <
CVE-2026-23818	A vulnerability has been identified in the graphical user interface (GUI) of HPE Aruba Networking Private 5G Core On-Prem that could allow an attacker to abuse an exploitation may redirect an authenticated user to an attacker-controlled server hosting a spoofed login page prompting the unsuspecting victim to give away thei back to the legitimate login page.
CVE-2026-35517	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, the Pi-hole FTL engine contains a F parameter (dns.upstreams). This vulnerability allows an authenticated attacker to inject arbitrary dnsmasq configuration directives through newline characters, ulti fixed in 6.6.
CVE-2026-35518	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, the Pi-hole FTL engine contains a F parameter (dns.cnameRecords). This vulnerability allows an authenticated attacker to inject arbitrary dnsmasq configuration directives through newline characters is fixed in 6.6.
CVE-2026-5604	A security flaw has been discovered in Tenda CH22 1.0.0.1. The impacted element is the function formCertLocalPrecreate of the file /goform/CertLocalPrecreate of standard results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for atta
CVE-2026-35519	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, the Pi-hole FTL engine contains a F parameter (dns.hostRecord). This vulnerability allows an authenticated attacker to inject arbitrary dnsmasq configuration directives through newline characters, ulti fixed in 6.6.
CVE-2026-35520	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, the Pi-hole FTL engine contains a F parameter (dhcp.leaseTime). This vulnerability allows an authenticated attacker to inject arbitrary dnsmasq configuration directives through newline characters, ul fixed in 6.6.
CVE-2026-35521	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, the Pi-hole FTL engine contains a F (dhcp.hosts). This vulnerability allows an authenticated attacker to inject arbitrary dnsmasq configuration directives through newline characters, ultimately achievi
CVE-2019-25673	UniSharp Laravel File Manager v2.0.0-alpha7 and v2.0 contain an arbitrary file upload vulnerability that allows authenticated attackers to upload malicious files by with the type parameter set to Files and execute arbitrary code by accessing the uploaded file through the working directory path.
CVE-2026-34197	Improper Input Validation, Improper Control of Generation of Code ('Code Injection') vulnerability in Apache ActiveMQ Broker, Apache ActiveMQ. Apache ActiveMQ (default Jolokia access policy permits exec operations on all ActiveMQ MBeans (org.apache.activemq:*), including BrokerService.addNetworkConnector(String) and E operations with a crafted discovery URI that triggers the VM transport's brokerConfig parameter to load a remote Spring XML application context using ResourceXm singleton beans before the BrokerService validates the configuration, arbitrary code execution occurs on the broker's JVM through bean factory methods such as R before 6.2.3; Apache ActiveMQ: . Users are recommended to upgrade to version 5.19.5 or 6.2.3, which fixes the issue.
CVE-2026-5465	The Booking for Appointments and Events Calendar – Amelia plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and includ changes to the `externalId` field when a Provider (Employee) user updates their own profile. The `externalId` maps directly to a WordPress user ID and is passed t makes it possible for authenticated attackers, with Provider-level (Employee) access and above, to take over any WordPress account — including Administrator — E
CVE-2026-21765	HCL BigFix Platform is affected by insecure permissions on private cryptographic keys. The private cryptographic keys located on a Windows host machine might b
CVE-2026-5605	A weakness has been identified in Tenda CH22 1.0.0.1. This affects the function formWrlExtraSet of the file /goform/WrlExtraSet. Executing a manipulation of the a remotely. The exploit has been made available to the public and could be used for attacks.
CVE-2019-25671	VA MAX 8.3.4 contains a remote code execution vulnerability that allows authenticated attackers to execute arbitrary commands by injecting shell metacharacters endpoint with malicious payload in the mtu_eth0 field to execute commands as the apache user.
CVE-2026-35567	ChurchCRM is an open-source church management system. Prior to 7.1.0, the NewRole POST parameter in src/MemberRoleChange.php is used in an SQL query wit The attack requires an authenticated session with ManageGroups role, knowledge of a valid GroupID and PersonID (obtainable from GroupView or PersonView page
CVE-2025-65115	Remote Code Execution Vulnerability in JP1/IT Desktop Management 2 - Manager on Windows, JP1/IT Desktop Management 2 - Operations Director on Windows, Job Desktop Management - Manager on Windows, Job Management Partner 1/IT Desktop Management - Manager on Windows, JP1/NETM/DM Manager on Windows, JP1/ Manager on Windows, Job Management Partner 1/Software Distribution Client on Windows.This issue affects JP1/IT Desktop Management 2 - Manager: from 13-50 b before 13-01-07, from 13-00 before 13-00-05, from 12-60 before 12-60-12, from 10-50 through 12-50-11; JP1/IT Desktop Management 2 - Operations Director: from from 13-01 before 13-01-07, from 13-00 before 13-00-05, from 12-60 before 12-60-12, from 10-50 through 12-50-11; Job Management Partner 1/IT Desktop Manag Manager: from 09-50 through 10-10-16; Job Management Partner 1/IT Desktop Management - Manager: from 09-50 through 10-10-16; JP1/NETM/DM Manager: from Management Partner 1/Software Distribution Manager: from 09-00 through 09-51-13; Job Management Partner 1/Software Distribution Client: from 09-00 through 0
CVE-2026-	In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege, if a UE has connected to a rogue needed. User interaction is needed for exploitation. Patch ID: MOLY01088681; Issue ID: MSV-4460.

20433	
CVE-2025-43264	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.6. Processing a maliciously crafted image may corrupt process m
CVE-2026-20094	A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with read-only privileges to perform command user. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted commands to the web-ba the attacker to execute arbitrary commands on the underlying operating system as the root user.
CVE-2026-22683	Windmill versions 1.56.0 through 1.614.0 contain a missing authorization vulnerability that allows users with the Operator role to perform prohibited entity creation and priced as unable to create or modify entities, the API does not enforce the Operator restriction on workspace endpoints, allowing an Operator to create and up the jobs API, this allows direct privilege escalation to remote code execution within the Windmill deployment. This vulnerability has existed since the introduction o
CVE-2026-27314	Privilege escalation in Apache Cassandra 5.0 on an mTLS environment using MutualTlsAuthenticator allows a user with only CREATE permission to associate their c authenticate as that role via ADD IDENTITY. Users are recommended to upgrade to version 5.0.7+, which fixes this issue.
CVE-2026-5567	A flaw has been found in Tenda M3 1.0.0.10. This vulnerability affects the function setAdvPolicyData of the file /goform/setAdvPolicyData of the component Destina overflow. The attack can be executed remotely. The exploit has been published and may be used.
CVE-2026-5566	A vulnerability was detected in UTT HiPER 1250GW up to 3.2.7-210907-180535. This affects the function strcpy of the file /goform/formNatStaticMap. Performing a of the attack is possible. The exploit is now public and may be used.
CVE-2026-5608	A vulnerability was detected in Belkin F9K1122 1.00.33. Affected is the function formWlanSetup of the file /goform/formWlanSetup. The manipulation of the argume remote. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-5550	A vulnerability was identified in Tenda AC10 16.03.10.10_multi_TDE01. This affects the function fromSysToolChangePwd of the file /bin/httpd. The manipulation lea endpoints might be affected.
CVE-2026-5548	A vulnerability was found in Tenda AC10 16.03.10.10_multi_TDE01. Affected by this vulnerability is the function fromSysToolChangePwd of the file /bin/httpd. Perfo overflow. The attack can be initiated remotely.
CVE-2026-5611	A vulnerability was found in Belkin F9K1015 1.00.10. This affects the function formCrossBandSwitch of the file /goform/formCrossBandSwitch. Performing a manipu 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.
CVE-2026-5629	A vulnerability was detected in Belkin F9K1015 1.00.10. The affected element is the function formSetFirewall of the file /goform/formSetFirewall. The manipulation executed 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.
CVE-2025-47392	Memory corruption when decoding corrupted satellite data files with invalid signature offsets.
CVE-2026-5281	Use after free in Dawn in Google Chrome prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to execute arbitrary code
CVE-2026-5280	Use after free in WebCodecs in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML p
CVE-2026-5279	Object corruption in V8 in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (
CVE-2026-5278	Use after free in Web MIDI in Google Chrome on Android prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Ch
CVE-2026-33175	OAuthenticator is software that allows OAuth2 identity providers to be plugged in and used with JupyterHub. Prior to version 17.4.0, an authentication bypass vulne Auth0 tenant to login to JupyterHub. When email is used as the usrname_claim, this gives users control over their username and the possibility of account takeover
CVE-2026-28797	RAGFlow is an open-source RAG (Retrieval-Augmented Generation) engine. In versions 0.24.0 and prior, a Server-Side Template Injection (SSTI) vulnerability exists components. These components use Python's jinja2.Template (unsandboxed) to render user-supplied templates, allowing any authenticated user to execute arbitra publicly available patches.
CVE-2026-5275	Heap buffer overflow in ANGLE in Google Chrome on Mac prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Cl
CVE-2026-5274	Integer overflow in Codecs in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromiu
CVE-2026-35470	OpenSTAManager is an open source management software for technical assistance and invoicing. Prior to 2.10.2, confronta_righe.php files across different module received via $_GET['righe'] is directly concatenated into an SQL query without any sanitization, parameterization or validation. An authenticated attacker can inject credentials, customer information, invoice data and any other stored data. This vulnerability is fixed in 2.10.2.
CVE-2026-5272	Heap buffer overflow in GPU in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium s

CVE-2026-35168	OpenSTAManager is an open source management software for technical assistance and invoicing. Prior to version 2.10.2, the Aggiornamenti (Updates) module in C database) that accepts a JSON array of SQL statements via POST and executes them directly against the database without any validation, allowlist, or sanitization. arbitrary SQL statements including CREATE, DROP, ALTER, INSERT, UPDATE, DELETE, SELECT INTO OUTFILE, and any other SQL command supported by the MySQL FOREIGN_KEY_CHECKS=0), further reducing database integrity protections. This issue has been patched in version 2.10.2.
CVE-2026-3692	In Progress Flowmon versions prior to 12.5.8, a vulnerability exists whereby an authenticated low-privileged user may craft a request during the report generation
CVE-2026-35164	Brave CMS is an open-source CMS. Prior to 2.0.6, an unrestricted file upload vulnerability exists in the CKEditor upload functionality. It is found in app/Http/Controlle validate uploaded file types and relies entirely on user input. This allows an authenticated user to upload executable PHP scripts and gain Remote Code Execution.
CVE-2026-33510	Homarr is an open-source dashboard. Prior to 1.57.0, a DOM-based Cross-Site Scripting (XSS) vulnerability has been discovered in Homarr's /auth/login page. The a and router.push. An attacker can craft a malicious link that, when opened by an authenticated user, performs a client-side redirect and executes arbitrary JavaScrip pivoting, and unauthorized actions performed on behalf of the victim. This vulnerability is fixed in 1.57.0.
CVE-2026-5349	A vulnerability was identified in Trendnet TEW-657BRM 1.00.1. The affected element is the function add_apcdb of the file /setup.cgi. The manipulation of the argum remotely. The exploit is publicly available and might be used. The vendor confirms, that "[t]he product in question (...) has been discontinued and end of life since product, so we are not able to confirm the vulnerabilities. We will make an announcement on our website's product support page and notify customers who registe supported by the maintainer.
CVE-2026-34791	Endian Firewall version 3.3.25 and prior allow authenticated users to execute arbitrary OS commands via the DATE parameter to /cgi-bin/logs_proxy.cgi. The DATE which allows command injection due to an incomplete regular expression validation.
CVE-2026-34792	Endian Firewall version 3.3.25 and prior allow authenticated users to execute arbitrary OS commands via the DATE parameter to /cgi-bin/logs_clamav.cgi. The DAT which allows command injection due to an incomplete regular expression validation.
CVE-2026-34793	Endian Firewall version 3.3.25 and prior allow authenticated users to execute arbitrary OS commands via the DATE parameter to /cgi-bin/logs_firewall.cgi. The DAT which allows command injection due to an incomplete regular expression validation.
CVE-2026-34794	Endian Firewall version 3.3.25 and prior allow authenticated users to execute arbitrary OS commands via the DATE parameter to /cgi-bin/logs_ids.cgi. The DATE pa allows command injection due to an incomplete regular expression validation.
CVE-2026-34795	Endian Firewall version 3.3.25 and prior allow authenticated users to execute arbitrary OS commands via the DATE parameter to /cgi-bin/logs_log.cgi. The DATE pa allows command injection due to an incomplete regular expression validation.
CVE-2026-34796	Endian Firewall version 3.3.25 and prior allow authenticated users to execute arbitrary OS commands via the DATE parameter to /cgi-bin/logs_openvpn.cgi. The DA which allows command injection due to an incomplete regular expression validation.
CVE-2026-34797	Endian Firewall version 3.3.25 and prior allow authenticated users to execute arbitrary OS commands via the DATE parameter to /cgi-bin/logs_smtp.cgi. The DATE which allows command injection due to an incomplete regular expression validation.
CVE-2026-35044	BentoML is a Python library for building online serving systems optimized for AI apps and model inference. Prior to 1.4.38, the Dockerfile generation function gener unsandboxed jinja2.Environment with the jinja2.ext.do extension to render user-provided dockerfile_template files. When a victim imports a malicious bento archiv arbitrary Python directly on the host machine, bypassing all container isolation. This vulnerability is fixed in 1.4.38.
CVE-2026-35029	LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. Prior to 1.83.0, the /config/update endpoint does not enforce admin role author endpoint to modify proxy configuration and environment variables, register custom pass-through endpoint handlers pointing to attacker-controlled Python code, ac and fetching via /get_image, and take over other privileged accounts by overwriting UI_USERNAME and UI_PASSWORD environment variables. Fixed in v1.83.0.
CVE-2025-71281	XenForo before 2.3.7 does not properly restrict methods callable from within templates. A loose prefix match was used instead of a stricter first-word match for me allowing unauthorized method invocations.
CVE-2025-71278	XenForo before 2.3.5 allows OAuth2 client applications to request unauthorized scopes. This affects any customer using OAuth2 clients on any version of XenForo 2 intended authorization level.
CVE-2026-28805	OpenSTAManager is an open source management software for technical assistance and invoicing. Prior to version 2.10.2, multiple AJAX select handlers in OpenSTA GET parameter. The user-supplied value is read from $superselect['stato'] and concatenated directly into SQL WHERE clauses as a bare expression, without any sa inject arbitrary SQL statements to extract sensitive data from the database, including usernames, password hashes, financial records, and any other information st
CVE-2026-5350	A security flaw has been discovered in Trendnet TEW-657BRM 1.00.1. The impacted element is the function update_pcdb of the file /setup.cgi. The manipulation of launched remotely. The exploit has been released to the public and may be used for attacks. The vendor confirms, that "[t]he product in question (...) has been dis longer provide support for this product, so we are not able to confirm the vulnerabilities. We will make an announcement on our website's product support page an affects products that are no longer supported by the maintainer.
CVE-2026-39329	ChurchCRM is an open-source church management system. Prior to 7.1.0, an SQL injection vulnerability was identified in /EventNames.php in ChurchCRM. Authenti parameter during event type creation. The vulnerable flow reaches an ON DUPLICATE KEY UPDATE clause where unescaped user input is interpolated directly. This
CVE-2026-35182	Brave CMS is an open-source CMS. Prior to 2.0.6, this vulnerability is a missing authorization check found in the update role endpoint at routes/web.php. The POST middleware. This allows any authenticated user to change account roles and promote themselves to Super Admin. This vulnerability is fixed in 2.0.6.
CVE-2026-34121	An authentication bypass vulnerability within the HTTP handling of the DS configuration service in TP-Link Tapo C520WS v2.6 was identified, due to inconsistent pa unauthenticated attacker can append an authentication-exempt action to a request containing privileged DS do actions, bypassing authorization checks. Successfu which may result in unauthorized modification of device state.

CVE-2026-3524	Mattermost Plugin Legal Hold versions <=1.1.4 fail to halt request processing after a failed authorization check in ServeHTTP which allows an authenticated attack the plugin's endpoints. Mattermost Advisory ID: MMSA-2026-00621
CVE-2026-5292	Out of bounds read in WebCodecs in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to perform an out of bounds memory read via a crafted HT
CVE-2026-5287	Use after free in PDF in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chrom
CVE-2026-39330	ChurchCRM is an open-source church management system. Prior to 7.1.0, an SQL injection vulnerability was found in the endpoint /PropertyAssign.php in ChurchCR Edit Records (isEditRecordsEnabled) can inject arbitrary SQL statements through the Value parameter and thus extract and modify information from the database.
CVE-2026-5286	Use after free in Dawn in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium securit
CVE-2026-5285	Use after free in WebGL in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2026-39334	ChurchCRM is an open-source church management system. Prior to 7.1.0, an SQL injection vulnerability was found in the endpoint /SettingsIndividual.php in Churc SQL statements through the type array parameter via the index and thus extract and modify information from the database. This vulnerability is fixed in 7.1.0.
CVE-2026-39332	ChurchCRM is an open-source church management system. Prior to 7.1.0, a reflected Cross-Site Scripting (XSS) vulnerability in GeoPage.php allows any authentica Because the payload fires automatically via autofocus with no user interaction required, an attacker can steal session cookies and fully take over any victim accou This vulnerability is fixed in 7.1.0.
CVE-2026-35576	ChurchCRM is an open-source church management system. Prior to 7.0.0, a stored cross-site scripting (XSS) vulnerability exists in ChurchCRM within the Person Pr 38766 and allows an authenticated user to inject arbitrary JavaScript code via dynamically assigned person properties. The malicious payload is persistently stored printable view, potentially leading to session hijacking or full account compromise. This vulnerability is fixed in 7.0.0.
CVE-2026-39333	ChurchCRM is an open-source church management system. Prior to 7.1.0, he FindFundRaiser.php endpoint reflects user-supplied input (DateStart and DateEnd) int context. An authenticated attacker can craft a malicious URL that executes arbitrary JavaScript when visited by another authenticated user. This constitutes a refle
CVE-2026-35408	Directus is a real-time API and App dashboard for managing SQL database content. Prior to 11.17.0, Directus's Single Sign-On (SSO) login pages lacked a Cross-Ori cross-origin window that opens the Directus login page retains the ability to access and manipulate the window object of that page. An attacker can exploit this to client, causing the victim to unknowingly grant access to their authentication provider account (e.g. Google, Discord). This vulnerability is fixed in 11.17.0.
CVE-2026-35554	A race condition in the Apache Kafka Java producer client's buffer pool management can cause messages to be silently delivered to incorrect topics. When a produ batch is still in flight, the batch's ByteBuffer is prematurely deallocated and returned to the buffer pool. If a subsequent producer batch—potentially destined for a the buffer contents may become corrupted. This can result in messages being delivered to unintended topics without any error being reported to the producer. Dat topic, potentially exposing sensitive data to consumers who have access to the destination topic but not the intended source topic. Data Integrity: Consumers on th deserialization failures, processing errors, and corrupted downstream data. This issue affects Apache Kafka versions ≤ 3.9.1, ≤ 4.0.1, and ≤ 4.1.1. Kafka users are
CVE-2026-35218	Budibase is an open-source low-code platform. Prior to version 3.32.5, Budibase's Builder Command Palette renders entity names (tables, views, queries, automati with Builder access can create a table, automation, view, or query whose name contains an HTML payload (e.g. <img src=x onerror=alert(document.domain)>). W (Ctrl+K), the payload executes in their browser, stealing their session cookie and enabling full account takeover. This issue has been patched in version 3.32.5.
CVE-2026-35214	Budibase is an open-source low-code platform. Prior to version 3.33.4, the plugin file upload endpoint (POST /api/plugin/upload) passes the user-supplied filename with Global Builder privileges can craft a multipart upload with a filename containing ../ to delete arbitrary directories via rmSync and write arbitrary files via tarbal patched in version 3.33.4.
CVE-2026-34748	Payload is a free and open source headless content management system. Prior to version 3.78.0 in @payloadcms/next, a stored Cross-Site Scripting (XSS) vulnerab collection could save content that, when viewed by another user, would execute in their browser. This issue has been patched in version 3.78.0.
CVE-2026-34728	phpMyFAQ is an open source FAQ web application. Prior to version 4.1.1, the MediaBrowserController::index() method handles file deletion for the media browser. concatenated with the base upload directory path without any path traversal validation. The FILTER_SANITIZE_SPECIAL_CHARS filter only encodes HTML special cha directory traversal sequences like ../. Additionally, the endpoint does not validate CSRF tokens, making it exploitable via CSRF attacks. This issue has been patched
CVE-2025-43257	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sequoia 15.6. An app may be able to break out of its sandbox.
CVE-2025-15620	HiOS Switch Platform versions 09.1.00 prior to 09.4.05 and 10.3.01 contains a denial-of-service vulnerability in the web interface that allows remote attackers to re endpoint. Attackers can trigger an uncontrolled reboot condition through crafted HTTP requests to cause service disruption and unavailability of the switch.
CVE-2025-10681	Storage credentials are hardcoded in the mobile app and device firmware. These credentials do not adequately limit end user permissions and do not expire within production storage containers.
CVE-2026-34445	Open Neural Network Exchange (ONNX) is an open standard for machine learning interoperability. Prior to version 1.21.0, the ExternalDataInfo class in ONNX was u directly from an ONNX model file. It didn't check if the "keys" in the file were valid. Due to this, an attacker could craft a malicious model that overwrites internal ob
CVE-2026-34577	Postiz is an AI social media scheduling tool. Prior to version 2.21.3, the GET /public/stream endpoint in PublicController accepts a user-supplied url query parameter url.endsWith('mp4'), which is trivially bypassable by appending .mp4 as a query parameter value or URL fragment. The endpoint requires no authentication and ha internal services, cloud metadata endpoints, and other network-internal resources. This issue has been patched in version 2.21.3.
CVE-2026-34954	PraisonAI is a multi-agent teams system. Prior to version 1.5.95, FileTools.download_file() in praisonaiagents validates the destination path but performs no validati follow_redirects=True. An attacker who controls the URL can reach any host accessible from the server including cloud metadata services and internal network ser

CVE-2026-32173	Improper authentication in Azure SRE Agent allows an unauthorized attacker to disclose information over a network.
CVE-2026-5463	Command injection vulnerability in console.run_module_with_output() in pymetasploit3 through version 1.0.6 allows attackers to inject newline characters into mod the Metasploit console to execute additional unintended commands, potentially leading to arbitrary command execution and manipulation of Metasploit sessions.
CVE-2026-33752	curl_cffi is the a Python binding for curl. Prior to 0.15.0, curl_cffi does not restrict requests to internal IP ranges, and follows redirects automatically via the underlyi services such as cloud metadata endpoints. In addition, curl_cffi's TLS impersonation feature can make these requests appear as legitimate browser traffic, which r
CVE-2026-34975	Plunk is an open-source email platform built on top of AWS SES. Prior to 0.8.0, a CRLF header injection vulnerability was discovered in SESService.ts, where user-su filenames were interpolated directly into raw MIME messages without sanitization. An authenticated API user could inject arbitrary email headers (e.g. Bcc, Reply-T email forwarding, reply redirection, or sender spoofing. The fix adds input validation at the schema level to reject any of these fields containing \r or \n characters, vulnerability is fixed in 0.8.0.
CVE-2026-34747	Payload is a free and open source headless content management system. Prior to version 3.79.1, certain request inputs were not properly validated. An attacker co modifying data in collections. This issue has been patched in version 3.79.1.
CVE-2026-34885	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in David Lingren Media LIbrary Assistant allows SQL Injection.T
CVE-2026-30289	An arbitrary file overwrite vulnerability in Tinybeans Private Family Album App v5.9.5-prod allows attackers to overwrite critical internal files via the file import proc
CVE-2019-25681	Xlight FTP Server 3.9.1 contains a structured exception handler (SEH) overwrite vulnerability that allows local attackers to crash the application and overwrite SEH through the program execution field in virtual server configuration to trigger a buffer overflow that corrupts the SEH chain and enables potential code execution.
CVE-2019-25656	R i386 3.5.0 contains a local buffer overflow vulnerability in the GUI Preferences dialog that allows local attackers to trigger a structured exception handler (SEH) o 'Language for menus and messages' field to overwrite SEH records and achieve code execution with calculator or arbitrary shellcode.
CVE-2026-30287	An arbitrary file overwrite vulnerability in Deep Thought Industries ACE Scanner PDF Scanner v1.4.5 allows attackers to overwrite critical internal files via the file im
CVE-2019-25670	River Past Video Cleaner 7.6.3 contains a structured exception handler buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplyi bytes of padding, a next structured exception handler override, and shellcode to trigger code execution when the application processes the input.
CVE-2026-35020	Anthropic Claude Code CLI and Claude Agent SDK contain an OS command injection vulnerability in the command lookup helper and deep-link terminal launcher th TERMINAL environment variable. Attackers can inject shell metacharacters into the TERMINAL variable which are interpreted by /bin/sh when the command lookup be triggered during normal CLI execution as well as via the deep-link handler path, resulting in arbitrary command execution with the privileges of the user running
CVE-2018-25251	Snes9K 0.0.9z contains a buffer overflow vulnerability in the Netplay Socket Port Number field that allows local attackers to trigger a structured exception handler (Port Number field via the Netplay Options menu to achieve code execution through SEH chain exploitation.
CVE-2026-30292	An arbitrary file overwrite vulnerability in Docudepot PDF Reader: PDF Viewer APP v1.0.34 allows attackers to overwrite critical internal files via the file import proc
CVE-2026-30291	An arbitrary file overwrite vulnerability in Ora Tools PDF Reader ' Reader & Editor APPv4.3.5 allows attackers to overwrite critical internal files via the file import pro
CVE-2018-25255	10-Strike LANState 8.8 contains a local buffer overflow vulnerability in structured exception handling that allows local attackers to execute arbitrary code by craftin payload in the ObjCaption parameter that overflows the buffer, overwrites the SEH chain, and executes shellcode when the file is opened in the application.
CVE-2026-34780	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. From versions 39.0.0-alpha.1 to before 39.8.0, 40.0.0-alpha VideoFrame objects (from the WebCodecs API) across the contextBridge are vulnerable to a context isolation bypass. An attacker who can execute JavaScript in the the isolated world, including any Node.js APIs exposed to the preload script. Apps are only affected if a preload script returns, resolves, or passes a VideoFrame obj VideoFrame objects are not affected. This issue has been patched in versions 39.8.0, 40.7.0, and 41.0.0-beta.8.
CVE-2026-34072	Cr*nMaster (cronmaster) is a Cronjob management UI with human readable syntax, live logging and log history for cronjobs. Prior to version 2.2.0, an authenticatio cookie to be treated as authenticated when the middleware's session-validation fetch fails. This can result in unauthorized access to protected pages and unauthor version 2.2.0.
CVE-2026-35394	Mobile Next is an MCP server for mobile development and automation. Prior to 0.0.50, the mobile_open_url tool in mobile-mcp passes user-supplied URLs directly t arbitrary Android intents, including USSD codes, phone calls, SMS messages, and content provider access. This vulnerability is fixed in 0.0.50.
CVE-2026-34524	SillyTavern is a locally installed user interface that allows users to interact with text generation large language models, image generation engines, and text-to-spee endpoints allows an authenticated attacker to read and delete arbitrary files under their user data root (for example secrets.json and settings.json) by supplying av
CVE-2025-59711	An issue was discovered in Biztalk360 before 11.5. Because of mishandling of user-provided input in an upload mechanism, an authenticated attacker is able to wr service, aka Directory Traversal.
CVE-	PilusCart 1.4.1 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'send

2019-25672	endpoint with RLIKE-based boolean SQL injection payloads to extract sensitive database information.
CVE-2019-25702	Kados R10 GreenBee contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the id_project para id_project parameter to extract sensitive database information or modify data.
CVE-2019-25678	C4G Basic Laboratory Information System 3.4 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to execute arbitrary SQL commar requests to the users_select.php endpoint with crafted SQL payloads to extract sensitive database information including patient records and system credentials.
CVE-2019-25704	Kados R10 GreenBee contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the filter_user_ma extract sensitive database information or modify data.
CVE-2019-25680	Advance Gift Shop Pro Script 2.0.3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malic the 's' parameter of search requests to extract sensitive database information including version details and other data.
CVE-2019-25696	Kados R10 GreenBee contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the language_tag parameter to extract sensitive database information or modify data.
CVE-2019-25684	OpenDocMan 1.3.4 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the SQL payloads in the 'where' parameter to extract sensitive database information.
CVE-2026-34982	Vim is an open source, command line text editor. Prior to version 9.2.0276, a modeline sandbox bypass in Vim allows arbitrary OS command execution when a use missing the `P_MLE` flag, allowing a modeline to be executed. Additionally, the `mapset()` function lacks a `check_secure()` call, allowing it to be abused from san
CVE-2026-4924	Improper authentication in the two-factor authentication (2FA) feature in Devolutions Server 2026.1.11 and earlier allows a remote attacker with valid credentials t account via reuse of a partially authenticated session token.
CVE-2026-34045	Podman Desktop is a graphical tool for developing on containers and Kubernetes. Prior to 1.26.2, an unauthenticated HTTP server exposed by Podman Desktop allo sensitive information. By abusing missing connection limits and timeouts, an attacker can exhaust file descriptors and kernel memory, leading to application crash system details (including usernames on Windows), aiding further exploitation. The issue requires no authentication or user interaction and is exploitable over the n
CVE-2024-44250	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.1. An app may be able to execute arbitrary code out of its s
CVE-2026-4740	A flaw was found in Open Cluster Management (OCM), the technology underlying Red Hat Advanced Cluster Management (ACM). Improper validation of Kubernetes certificate that can be approved by the OCM controller. This enables cross-cluster privilege escalation and may allow an attacker to gain control over other manage
CVE-2026-35091	A flaw was found in Corosync. A remote unauthenticated attacker can exploit a wrong return value vulnerability in the Corosync membership commit token sanity lead to an out-of-bounds read, causing a denial of service (DoS) and potentially disclosing limited memory contents. This vulnerability affects Corosync when runni
CVE-2019-25688	Kados R10 GreenBee contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through t payloads in the menu_lev1 parameter to extract sensitive database information or modify database contents.
CVE-2019-25690	Kados R10 GreenBee contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the mng_profile_id mng_profile_id parameter to extract sensitive database information.
CVE-2026-4828	Improper authentication in the OAuth login functionality in Devolutions Server 2026.1.11 and earlier allows a remote attacker with valid credentials to bypass multi
CVE-2026-35457	libp2p-rust is the official rust language Implementation of the libp2p networking stack. Prior to 0.17.1, the rendezvous server stores pagination cookies without bou unbounded memory growth. This vulnerability is fixed in 0.17.1.
CVE-2019-25700	Kados R10 GreenBee contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the sort_direction parameter to extract sensitive database information or modify data.
CVE-2026-34725	DbGate is cross-platform database manager. From version 7.0.0 to before version 7.1.5, a stored XSS vulnerability exists in DbGate because attacker-controlled SV script execution in another user's browser; in the Electron desktop app this can escalate to local code execution because Electron is configured with nodeIntegratio
CVE-2019-25676	Ask Expert Script 3.0.5 contains cross-site scripting and SQL injection vulnerabilities that allow unauthenticated attackers to inject malicious code by manipulating categorysearch.php or SQL code through the view parameter in list-details.php to execute arbitrary code or extract database information.
CVE-2015-10148	Hirschmann HiLCOS devices OpenBAT, WLC, BAT300, BAT54 prior to 8.80 and OpenBAT prior to 9.10 are shipped with identical default SSH and SSL keys that cann encrypted management communications. Attackers can perform man-in-the-middle attacks, impersonate devices, and expose sensitive information by leveraging
CVE-2019-25698	Kados R10 GreenBee contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the id_to_delete p id_to_delete field to extract or modify sensitive database information.
CVE-	Kados R10 GreenBee contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through t

2019-25694	payloads to extract sensitive database information or modify data.
CVE-2019-25675	eDirectory contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to bypass administrator authentication and disclose sensitive files by login endpoint with union-based SQL injection to authenticate as administrator, then leverage authenticated file disclosure vulnerabilities in language_file.php to re
CVE-2019-25662	ResourceSpace 8.6 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code throu endpoint with crafted SQL payloads to extract sensitive database information including usernames and credentials.
CVE-2019-25668	News Website Script 2.0.5 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code thro with malicious SQL statements to extract sensitive database information.
CVE-2019-25669	qdPM 9.1 contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the search_by_extrafields[] pa search_by_extrafields[] values to trigger SQL syntax errors and extract database information.
CVE-2019-25674	CMSsite 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'post' extract sensitive database information or perform time-based blind SQL injection attacks.
CVE-2026-34236	Auth0-PHP is a PHP SDK for Auth0 Authentication and Management APIs. From version 8.0.0 to before version 8.19.0, in applications built with the Auth0 PHP SDK, brute-forcing the encryption key and forging session cookies. This issue has been patched in version 8.19.0.
CVE-2019-25692	Kados R10 GreenBee contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the 'id_to_modify' id_to_modify field to extract sensitive database information or modify data.
CVE-2026-24450	An integer overflow vulnerability exists in the uncompressed_fp_dng_load_raw functionality of LibRaw Commit 8dc68e2. A specially crafted malicious file can lead t vulnerability.
CVE-2026-24660	A heap-based buffer overflow vulnerability exists in the x3f_load_huffman functionality of LibRaw Commit d20315b. A specially crafted malicious file can lead to a h vulnerability.
CVE-2026-20884	An integer overflow vulnerability exists in the deflate_dng_load_raw functionality of LibRaw Commit 8dc68e2. A specially crafted malicious file can lead to a heap b
CVE-2026-35045	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. Prior to 2.6.4, the PUT /api/recipe/batch_update/ endpoint in T that Space, including recipes marked as private by other users. This bypasses all object-level authorization checks enforced on standard single-recipe endpoints (P grant of access via the shared list, and metadata tampering. This vulnerability is fixed in 2.6.4.
CVE-2026-4272	Missing Authentication for Critical Function vulnerability in Honeywell Handheld Scanners allows Authentication Abuse.This issue affects Handheld Scanners: from C HE000085BAA, from A1/B1 Base(IMX25) before BK000763BAA_BK000765BAA_CU000101BAA. This vulnerability could allow a remote attacker within Bluetooth rang commands on the host connected to the base station without authentication. This issue has been assigned CVE-2026-4272 https://nvd.nist.gov/vuln/detail/CVE-202 upgrade to the latest version identified to resolve the vulnerability.
CVE-2026-34581	goshs is a SimpleHTTPServer written in Go. From version 1.1.0 to before version 2.0.0-beta.2, when using the Share Token it is possible to bypass the limited selec been patched in version 2.0.0-beta.2.
CVE-2026-4347	The MW WP Form plugin for WordPress is vulnerable to arbitrary file moving due to insufficient file path validation via the 'generate_user_filepath' function and the makes it possible for unauthenticated attackers to move arbitrary files on the server, which can easily lead to remote code execution when the right file is moved (added to the form and the “Saving inquiry data in database” option is enabled.
CVE-2026-35442	Directus is a real-time API and App dashboard for managing SQL database content. Prior to 11.17.0, aggregate functions (min, max) applied to fields with the conce placeholder. When combined with groupBy, any authenticated user with read access to the affected collection can extract concealed field values, including static A is fixed in 11.17.0.
CVE-2026-34522	SillyTavern is a locally installed user interface that allows users to interact with text generation large language models, image generation engines, and text-to-spee /api/chats/import allows an authenticated attacker to write attacker-controlled files outside the intended chats directory by injecting traversal sequences into chara
CVE-2026-26263	GLPI is a free asset and IT management software package. From 11.0.0 to before 11.0.6, an unauthenticated time-based blind SQL injection exists in GLPI's Search
CVE-2026-4636	A flaw was found in Keycloak. An authenticated user with the uma_protection role can bypass User-Managed Access (UMA) policy validation. This allows the attacke even if the URL path specifies an attacker-owned resource. Consequently, the attacker gains unauthorized permissions to victim-owned resources, enabling them t unauthorized actions.
CVE-2026-25726	Cloudreve is a self-hosted file management and sharing system. Prior to version 4.13.0, the application uses the weak pseudo-random number generator math/ran the secret_key, and hash_id_salt. These secrets are generated upon first startup and persisted in the database. An attacker can exploit this by obtaining the admin for the PRNG seed, and use known hashid to validate the seed. By brute-forcing the seed (demonstrated to take <3 hours on general consumer PC), an attacker ca any user, including administrators, leading to full account takeover and privilege escalation. This issue has been patched in version 4.13.0.
CVE-2026-34783	Ferret is a declarative system for working with web data. Prior to 2.0.0-alpha.4, a path traversal vulnerability in Ferret's IO::FS::WRITE standard library function allo Ferret. When an operator scrapes a website that returns filenames containing ../ sequences, and uses those filenames to construct output paths (a standard scrapi can lead to remote code execution via cron jobs, SSH authorized_keys, shell profiles, or web shells. This vulnerability is fixed in 2.0.0-alpha.4.
CVE-2026-34742	The Go MCP SDK used Go's standard encoding/json. Prior to version 1.4.0, the Model Context Protocol (MCP) Go SDK does not enable DNS rebinding protection by d without authentication with StreamableHTTPHandler or SSEHandler, a malicious website could exploit DNS rebinding to bypass same-origin policy restrictions and s access resources exposed by the MCP server on behalf of the user in those limited circumstances. This issue has been patched in version 1.4.0.

CVE-2026-34402	ChurchCRM is an open-source church management system. Prior to 7.1.0, authenticated users with Edit Records or Manage Groups permissions can exploit a time- or modify any database content, including user credentials, personal identifiable information (PII), and configuration secrets. This vulnerability is fixed in 7.1.0.
CVE-2026-4101	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 throu conditions could allow an attacker to bypass authentication mechanisms and gain unauthorized access to the application.
CVE-2026-33949	Tina is a headless content management system. Prior to version 2.2.2, a path traversal vulnerability in @tinacms/graphql allows unauthenticated users to write and relativePath parameter in GraphQL mutations. The impact includes the ability to replace critical server configuration files and potentially execute arbitrary commar
CVE-2026-22661	prompts.chat prior to commit 0f8d4c3 contains a path traversal vulnerability in skill file handling that allows attackers to write arbitrary files to the client system by sequences. Attackers can exploit missing server-side filename validation to inject path traversal sequences ../ into skill file archives, which when extracted by vulne files to achieve code execution.
CVE-2026-22665	prompts.chat prior to commit 1464475 contains an identity confusion vulnerability due to inconsistent case-sensitive and case-insensitive handling of usernames a bypass uniqueness checks. Attackers can exploit non-deterministic username resolution to impersonate victim accounts, replace profile content on canonical URLs
CVE-2026-39371	RedwoodSDK is a server-first React framework. From 1.0.0-beta.50 to 1.0.5, erver functions exported from "use server" files could be invoked via GET requests, by cross-site GET navigations to trigger state-changing functions, because browsers send SameSite=Lax cookies on top-level GET requests. This affected all server fur files. This vulnerability is fixed in 1.0.6.
CVE-2016-15058	Hirschmann HiLCOS Classic Platform switches Classic L2E, L2P, L3E, L3P versions prior to 09.0.06 and Classic L2B prior to 05.3.07 contain a credential exposure vu and transmitted in plaintext when the feature is enabled. Attackers with local network access can sniff SNMP traffic or extract configuration data to recover plainte
CVE-2026-5282	Out of bounds read in WebCodecs in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to perform an out of bounds memory read via a crafted HT
CVE-2026-34774	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to versions 39.8.1, 40.7.0, and 41.0.0, apps that use c use-after-free. If the parent offscreen WebContents is destroyed while a child window remains open, subsequent paint frames on the child dereference freed memo use offscreen rendering (webPreferences.offscreen: true) and their setWindowOpenHandler permits child windows. Apps that do not use offscreen rendering, or tha 40.7.0, and 41.0.0.
CVE-2026-39341	ChurchCRM is an open-source church management system. Prior to 7.1.0, The application is vulnerable to time-based SQL injection due to an improper input valida user input, specifically, the sanitised input is not used to create the SQL query. This vulnerability is fixed in 7.1.0.
CVE-2026-39331	ChurchCRM is an open-source church management system. Prior to 7.1.0, an authenticated API user can modify any family record's state without proper authorizat they possess the required EditRecords privilege. /family/{familyId}/verify, /family/{familyId}/verify/url, /family/{familyId}/verify/now, /family/{familyId}/activate/{s to deactivate/reactivate arbitrary families, spam verification emails, and mark families as verified and trigger geocoding. This vulnerability is fixed in 7.1.0.
CVE-2026-4896	The WCFM – Frontend Manager for WooCommerce along with Bookings Subscription Listings Compatible plugin for WordPress is vulnerable to Insecure Direct Objec including `wcfm_modify_order_status`, `delete_wcfm_article`, `delete_wcfm_product`, and the article management controller due to missing validation on user-sup access and above, to modify the status of any order, delete or modify any post/product/page, regardless of ownership.
CVE-2026-39307	PraisonAI is a multi-agent teams system. Prior to 1.5.113, The PraisonAI templates installation feature is vulnerable to a "Zip Slip" Arbitrary File Write attack. When the application uses Python's zipfile.extractall() without verifying if the files within the archive resolve outside of the intended extraction directory. This vulnerabilit
CVE-2026-25773	** UNSUPPORTED WHEN ASSIGNED ** Focalboard version 8.0 fails to sanitize category IDs before incorporating them into dynamic SQL statements when reorderin which is stored in the database and later executed unsanitized when the category reorder API processes the stored value. This Second-Order SQL Injection (Time-B password hashes of other users. NOTE: Focalboard as a standalone product is not maintained and no fix will be issued.
CVE-2026-35607	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Prior to 2.63.1, the fix in comm permission and Commands from users created via the signup handler. The same fix was not applied to the proxy auth handler. Users auto-created on first successf though the signup path was explicitly changed to prevent execution rights from being inherited by automatically provisioned accounts. This vulnerability is fixed in
CVE-2026-4350	The Perfmatters plugin for WordPress is vulnerable to arbitrary file deletion via path traversal in all versions up to, and including, 2.5.9.1. This is due to the `PMCS:: sanitization, authorization check, or nonce verification. The unsanitized filename is concatenated with the storage directory path and passed to `unlink()`. This mak delete arbitrary files on the server by using `../` path traversal sequences, including `wp-config.php` which would force WordPress into the installation wizard and a
CVE-2026-39340	ChurchCRM is an open-source church management system. Prior to 7.1.0, a SQL injection vulnerability exists in PropertyTypeEditor.php, part of the administration Family Properties). The vulnerability was introduced when legacyFilterInput() which both strips HTML and escapes SQL — was replaced with sanitizeText(), which st concatenated directly into raw INSERT and UPDATE queries with no SQL escaping. This allows any authenticated user with the MenuOptions role (a non-admin staff database, including password hashes of all users. This vulnerability is fixed in 7.1.0.
CVE-2026-35488	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. Prior to 2.6.4, RecipeBookViewSet and RecipeBookEntryViewS CustomIsShared.has_object_permission() returns True for all HTTP methods — including DELETE, PUT, and PATCH — without checking request.method in SAFE_MET even though shared access is semantically read-only. This vulnerability is fixed in 2.6.4.
CVE-2026-34840	OneUptime is an open-source monitoring and observability platform. Prior to version 10.0.42, OneUptime's SAML SSO implementation (App/FeatureSet/Identity/Util isSignatureValid() verifies the first <Signature> element in the XML DOM using xml-crypto, while getEmail() always reads from assertion[0] via xml2js. An attacker legitimately signed assertion, resulting in authentication bypass. This issue has been patched in version 10.0.42.
CVE-2026-5373	An issue that allowed all-organization administrators to promote accounts to superuser status has been resolved. This is an instance of CWE-269: Improper Privileg CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:N (8.1 High). This issue was fixed in version 4.0.260202.0 of the runZero Platform.
CVE-2026-34528	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Prior to version 2.62.2, the sign d.settings.Defaults.Apply(user), then strips only Admin. The Execute permission and Commands list from the default user template are not stripped. When an admi default user template, any unauthenticated user who self-registers inherits shell execution capabilities and can run arbitrary commands on the server. This issue h
CVE-2026-	In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege, if a UE has connected to a rogue needed. User interaction is needed for exploitation. Patch ID: MOLY01406170; Issue ID: MSV-4461.

20432	
CVE-2025-24818	Nokia MantaRay NM is vulnerable to an OS command injection vulnerability due to improper neutralization of special elements used in an OS command in Log Sear
CVE-2026-35575	ChurchCRM is an open-source church management system. Prior to 6.5.3, a Stored Cross-Site Scripting (Stored XSS) vulnerability in the admin panel's group-creati that executes automatically when an administrator views the page. This enables attackers to steal the administrator's session cookies, potentially leading to full ac
CVE-2026-20155	A vulnerability in the web-based management interface of Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker w access. This vulnerability is due to improper authorization checks on a REST API endpoint of an affected device. An attacker could exploit this vulnerability by session information of active Cisco EPNM users, including users with administrative privileges, which could result in the affected device being compromised.
CVE-2026-5684	A vulnerability was determined in Tenda CX12L 16.03.53.12. Affected by this issue is the function fromwebExcptypemanFilter of the file /goform/webExcptypemanI overflow. The attack requires access to the local network. The exploit has been publicly disclosed and may be utilized.
CVE-2024-14032	Twitch Studio version 0.114.8 and prior contain a privilege escalation vulnerability in its privileged helper tool that allows local attackers to execute arbitrary code installFromPath:toPath:withReply: method to overwrite system files and privileged binaries, achieving full system compromise. Twitch Studio was discontinued in M
CVE-2026-32861	There is a memory corruption vulnerability due to an out-of-bounds write when loading a corrupted LVCLASS file in NI LabVIEW. This vulnerability may result in info attacker to get a user to open a specially crafted .lvclass file. This vulnerability affects NI LabVIEW 2026 Q1 (26.1.0) and prior versions.
CVE-2026-32860	There is a memory corruption vulnerability due to an out-of-bounds write when loading a corrupted LVLIB file in NI LabVIEW. This vulnerability may result in inform attacker to get a user to open a specially crafted .lvlib file. This vulnerability affects NI LabVIEW 2026 Q1 (26.1.0) and prior versions.
CVE-2025-47391	Memory corruption while processing a frame request from user.
CVE-2025-47390	Memory corruption while preprocessing IOCTL request in JPEG driver.
CVE-2025-47389	Memory corruption when buffer copy operation fails due to integer overflow during attestation report generation.
CVE-2026-32926	V-SFT versions 6.2.10.0 and prior contain an out-of-bounds read vulnerability in VS6ComFile!load_link_inf. Opening a crafted V7 file may lead to information disclos
CVE-2026-34990	OpenPrinting CUPS is an open source printing system for Linux and other Unix-like operating systems. In versions 2.4.16 and prior, a local unprivileged user can co reusable Authorization: Local ... token. That token is enough to drive /admin/ requests on localhost, and the attacker can combine CUPS-Create-Local-Printer with p policy rejects such URIs. Printing to that queue gives an arbitrary root file overwrite; the PoC below uses that primitive to drop a sudoers fragment and demonstrat patches.
CVE-2026-21371	Memory Corruption when retrieving output buffer with insufficient size validation.
CVE-2026-32927	V-SFT versions 6.2.10.0 and prior contain an out-of-bounds read vulnerability in VS6MemInIF!set_temp_type_default. Opening a crafted V7 file may lead to informat
CVE-2026-34937	PraisonAI is a multi-agent teams system. Prior to version 1.5.90, run_python() in praisonai constructs a shell command string by interpolating user-controlled code escaping logic only handles \ and ", leaving $() and backtick substitutions unescaped, allowing arbitrary OS command execution before Python is invoked. This issu
CVE-2026-35021	Anthropic Claude Code CLI and Claude Agent SDK contain an OS command injection vulnerability in the prompt editor invocation utility that allows attackers to exe metacharacters such as $() or backtick expressions into file paths that are interpolated into shell commands executed via execSync. Although the file path is wrapp substitution within double quotes, allowing injected expressions to be evaluated and resulting in arbitrary command execution with the privileges of the user runni
CVE-2026-23406	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix side-effect bug in match_char() macro usage The match_char() macro evaluates its When invoked with *str++, the string pointer advances on each iteration of the inner do-while loop, causing the DFA to check different characters at each iteration pointer advances past the input buffer boundary. [94.984676] == aa_dfa_match+0x5ae/0x760 [94.985655] Read of size 1 at addr ffff888100342000 by task file/976 [94.986319] CPU: 7 UID: 1000 PID: 976 Comm: file Not tainted Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [94.986329] Call Trace: [94.986341] <TASK> [94.986347] dump_stack_lvl+0x5e/0x80 94.986388] kasan_report+0x118/0x150 [94.986401] ? aa_dfa_match+0x5ae/0x760 [94.986405] aa_dfa_match+0x5ae/0x760 [94.986408] __aa_path_perm+0x1 apparmor_file_open+0x345/0x570 [94.986431] security_file_open+0x5c/0x140 [94.986442] do_dentry_open+0x2f6/0x1120 [94.986450] vfs_open+0x38/0x2b0 94.986469] ? __x64_sys_openat+0xf8/0x130 [94.986477] do_file_open+0x19d/0x360 [94.986487] do_sys_openat2+0x98/0x100 [94.986491] __x64_sys_openat+ count_memcg_events+0x15f/0x3c0 [94.986526] ? srso_alias_return_thunk+0x5/0xfbef5 [94.986540] ? handle_mm_fault+0x1639/0x1ef0 [94.986551] ? vma_sta ? srso_alias_return_thunk+0x5/0xfbef5 [94.986563] ? fpregs_assert_state_consistent+0x50/0xe0 [94.986572] ? srso_alias_return_thunk+0x5/0xfbef5 [94.986574 srso_alias_return_thunk+0x5/0xfbef5 [94.986588] ? irqentry_exit+0x3c/0x590 [94.986595] entry_SYSCALL_64_after_hwframe+0x76/0x7e [94.986597] RIP: 0033 ensuring single evaluation per outer loop.
CVE-2026-32862	There is a memory corruption vulnerability due to an out-of-bounds write in ResFileFactory::InitResourceMgr() in NI LabVIEW. This vulnerability may result in inform attacker to get a user to open a specially crafted VI file. This vulnerability affects NI LabVIEW 2026 Q1 (26.1.0) and prior versions.
CVE-2026-21373	Memory Corruption when accessing an output buffer without validating its size during IOCTL processing.

CVE-2026-21372	Memory Corruption when sending IOCTL requests with invalid buffer sizes during memcpy operations.
CVE-2026-23408	In the Linux kernel, the following vulnerability has been resolved: apparmor: Fix double free of ns_name in aa_replace_profiles() if ns_name is NULL after 1071 erro 1089 } else if (ent->ns_name) { then ns_name is assigned the ent->ns_name 1095 ns_name = ent->ns_name; however ent->ns_name is freed at 1262 aa_load_er NULLing out ent->ns_name after it is transferred to ns_name ")
CVE-2026-34588	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. From 3.1.0 to be pointer with signed 32-bit arithmetic. Because nx, ny, and wcount are int, a crafted EXR file can make this product overflow and wrap. The next channel then decoc yields both out-of-bounds reads and out-of-bounds writes. This vulnerability is fixed in 3.2.7, 3.3.9, and 3.4.9.
CVE-2026-21382	Memory Corruption when handling power management requests with improperly sized input/output buffers.
CVE-2026-5429	Unsanitized input during web page generation in the Kiro Agent webview in Kiro IDE before version 0.8.140 allows a remote unauthenticated threat actor to execut user opens the workspace. This issue requires the user to trust the workspace when prompted. To remediate this issue, users should upgrade to version 0.8.140.
CVE-2026-21380	Memory Corruption when using deprecated DMABUF IOCTL calls to manage video memory.
CVE-2026-21378	Memory Corruption when accessing an output buffer without validating its size during IOCTL processing in a camera sensor driver.
CVE-2026-21376	Memory Corruption when accessing an output buffer without validating its size during IOCTL processing in a camera sensor driver.
CVE-2026-21375	Memory Corruption when accessing an output buffer without validating its size during IOCTL processing.
CVE-2026-21374	Memory Corruption when processing auxiliary sensor input/output control commands with insufficient buffer size validation.
CVE-2026-35043	BentoML is a Python library for building online serving systems optimized for AI apps and model inference. Prior to 1.4.38, the cloud deployment path in src/bentom 1648 interpolates system_packages directly into a shell command using an f-string without any quoting. The generated script is uploaded to BentoCloud as setup.s remote code execution on the CI/CD tier. This vulnerability is fixed in 1.4.38.
CVE-2023-7343	HiSecOS web server versions 05.0.00 to 08.3.01 prior to 08.3.02 contains a privilege escalation vulnerability that allows authenticated users with operator or audito packets to the web server. Attackers can exploit this flaw to gain full administrative access to the affected device.
CVE-2026-3775	The application's update service, when checking for updates, loads certain system libraries from a search path that includes directories writable by low-privileged u may be resolved and loaded from user-writable locations, a local attacker can place a malicious library there and have it loaded with SYSTEM privileges, resulting in
CVE-2026-35558	Improper neutralization of special elements in the authentication components in Amazon Athena ODBC driver before 2.1.0.0 might allow a threat actor to execute a parameters that are processed by the driver during user-initiated authentication. To remediate this issue, users should upgrade to version 2.1.0.0.
CVE-2026-3779	The application's list box calculate array logic keeps stale references to page or form objects after they are deleted or re-created, which allows crafted documents t arbitrary code execution.
CVE-2026-5485	OS command injection in the browser-based authentication component in Amazon Athena ODBC driver before 2.0.5.1 on Linux might allow a threat actor to execut the driver during a local user-initiated connection. To remediate this issue, users should upgrade to version 2.0.5.1 or later.
CVE-2026-33641	Glances is an open-source system cross-platform monitoring tool. Prior to version 4.5.3, Glances supports dynamic configuration values in which substrings enclose behavior occurs in Config.get_value() and is implemented without validation or restriction of the executed commands. If an attacker can modify or influence config Glances process during startup or configuration reload. In deployments where Glances runs with elevated privileges (e.g., as a system service), this may lead to pr
CVE-2026-32864	There is a memory corruption vulnerability due to an out-of-bounds read in mgcore_SH_25_3!aligned_free() in NI LabVIEW. This vulnerability may result in informat to get a user to open a specially crafted VI file. This vulnerability affects NI LabVIEW 2026 Q1 (26.1.0) and prior versions.
CVE-2026-32863	There is a memory corruption vulnerability due to an out-of-bounds read in sentry_transaction_context_set_operation() in NI LabVIEW. This vulnerability may result an attacker to get a user to open a specially crafted VI file. This vulnerability affects NI LabVIEW 2026 Q1 (26.1.0) and prior versions.
CVE-2026-23407	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix missing bounds check on DEFAULT table in verify_dfa() The verify_dfa() function on the verification loop traverses the differential encoding chain, it reads k = DEFAULT_TABLE[j] and uses k as an array index without validation. A malformed DFA wit writes. [57.179855] == [57.180549] BUG: KASAN: slab- ffff888100eadec4 by task su/993 [57.181554] CPU: 1 UID: 0 PID: 993 Comm: su Not tainted 6.19.0-rc7-next-20260127 #1 PREEMPT(lazy) [57.181558] Hardware n [57.181563] Call Trace: [57.181572] <TASK> [57.181577] dump_stack_lvl+0x5e/0x80 [57.181596] print_report+0xc8/0x270 [57.181605] ? verify_dfa+0x59a/0 verify_dfa+0x59a/0x660 [57.181623] verify_dfa+0x59a/0x660 [57.181627] aa_dfa_unpack+0x1610/0x1740 [57.181629] ? __kmalloc_cache_noprof+0x1d0/0x47 srso_alias_return_thunk+0x5/0xfbef5 [57.181653] ? srso_alias_return_thunk+0x5/0xfbef5 [57.181656] ? aa_unpack_nameX+0x1a8/0x300 [57.181659] aa_unpac stack_depot_save_flags+0x33/0x700 [57.181681] ? kasan_save_track+0x4f/0x80 [57.181683] ? kasan_save_track+0x3e/0x80 [57.181686] ? __kasan_kmalloc+0 aa_simple_write_to_buffer+0x54/0x130 [57.181697] ? policy_update+0x154/0x330 [57.181704] aa_replace_profiles+0x15a/0x1dd0 [57.181707] ? srso_alias_retu 57.181712] ? aa_loaddata_alloc+0x77/0x140 [57.181715] ? srso_alias_return_thunk+0x5/0xfbef5 [57.181717] ? _copy_from_user+0x2a/0x70 [57.181730] policy rw_verify_area+0x93/0x2d0 [57.181740] vfs_write+0x235/0xab0 [57.181745] ksys_write+0xb0/0x170 [57.181748] do_syscall_64+0x8e/0x660 [57.181762] enti Remove the MATCH_FLAG_DIFF_ENCODE condition to validate all DEFAULT_TABLE entries unconditionally.

CVE-2019-25679	RealTerm Serial Terminal 2.0.0.70 contains a structured exception handling (SEH) buffer overflow vulnerability in the Echo Port tab that allows local attackers to ex overflow payload with a POP POP RET gadget chain and shellcode that triggers code execution when pasted into the Port field and the Change button is clicked.
CVE-2016-20060	Hotspot Shield 6.0.3 contains an unquoted service path vulnerability in the hshld service binary that allows local attackers to escalate privileges by injecting malici service restart or system reboot, the malicious code executes with LocalSystem privileges.
CVE-2016-20056	Spy Emergency build 23.0.205 contains an unquoted service path vulnerability in the SpyEmrgHealth and SpyEmrgSrv services that allows local attackers to escala in the unquoted service path and trigger service restart or system reboot to execute code with LocalSystem privileges.
CVE-2025-14821	A flaw was found in libssh. This vulnerability allows local man-in-the-middle attacks, security downgrades of SSH (Secure Shell) connections, and manipulation of tr availability of SSH communications via an insecure default configuration on Windows systems where the library automatically loads configuration files from the C:\
CVE-2026-0634	Code execution in AssistFeedbackService of TECNO Pova7 Pro 5G on Android allows local apps to execute arbitrary code as system via command injection.
CVE-2026-32925	V-SFT versions 6.2.10.0 and prior contain a stack-based buffer overflow in VS6ComFile!CV7BaseMap::WriteV7DataToRom. Opening a crafted V7 file may lead to arb
CVE-2016-20061	sheed AntiVirus 2.3 contains an unquoted service path vulnerability in the ShavProt service that allows local attackers to escalate privileges by exploiting the servi trigger service restart or system reboot to execute code with LocalSystem privileges.
CVE-2026-5271	pymanager included the current working directory in sys.path meaning modules could be shadowed by modules in the current working directory. As a result, if a us controlled directory, a malicious module in that directory can be imported and executed instead of the intended package.
CVE-2016-20059	IObit Malware Fighter 4.3.1 contains an unquoted service path vulnerability in the IMFservice and LiveUpdateSvc services that allows local attackers to escalate pri and trigger privilege escalation when the service restarts or the system reboots, executing code with LocalSystem privileges.
CVE-2016-20058	Netgate AMITI Antivirus build 23.0.305 contains an unquoted service path vulnerability in the AmitiAvSrv and AmitiAntivirusHealth services that allows local attacke service path and trigger service restart or system reboot to execute code with LocalSystem privileges.
CVE-2026-32929	V-SFT versions 6.2.10.0 and prior contain an out-of-bounds read in VS6ComFile!get_macro_mem_COM. Opening a crafted V7 file may lead to information disclosure
CVE-2016-20057	NETGATE Registry Cleaner build 16.0.205 contains an unquoted service path vulnerability in the NGRegClnSrv service that allows local attackers to escalate privile in the unquoted path and trigger service restart or system reboot to execute code with LocalSystem privileges.
CVE-2026-23410	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix race on rawdata dereference There is a race condition that leads to a use-after-free open()ing one of the rawdata files, and at the same time remove the last reference to this rawdata (by removing the corresponding profile, for example), which fre a dangling pointer and freed memory is accessed. The rawdata inodes weren't refcounted to avoid a circular refcount and were supposed to be held by the profile and profile destruction race, resulting in the use after free. Fix this by moving to a double refcount scheme. Where the profile refcount on rawdata is used to break to the rawdata are put.
CVE-2026-32928	V-SFT versions 6.2.10.0 and prior contain a stack-based buffer overflow in VS6ComFile!CSaveData::_conv_AnimationItem. Opening a crafted V7 file may lead to arb
CVE-2016-20055	IObit Advanced SystemCare 10.0.2 contains an unquoted service path vulnerability in the AdvancedSystemCareService10 service that allows local attackers to esc trigger privilege escalation when the service restarts or the system reboots, executing code with LocalSystem privileges.
CVE-2026-23411	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix race between freeing data and fs accessing it AppArmor was putting the reference However the inode can aand does live beyond that point and it is possible that some of the fs call back functions will be invoked after the reference has been put, the rawdata/loaddata is the most likely candidate to fail the race, as it has the fewest references. If properly crafted it might be possible to trigger a race for the ot the correct place which is during inode eviction.
CVE-2026-22664	prompts.chat prior to commit 30a8f04 contains a server-side request forgery vulnerability in Fal.ai media status polling that allows authenticated users to perform parameter. Attackers can exploit the lack of URL validation to disclose the FAL_API_KEY in the Authorization header, enabling credential theft, internal network prob
CVE-2026-39361	OpenObserve is a cloud-native observability platform. In 0.70.3 and earlier, the validate_enrichment_url function in src/handler/http/request/enrichment_table/mod brackets (e.g. "[::1]" not "::1"). An authenticated attacker can reach internal services blocked from external access. On cloud deployments this enables retrieval of self-hosted deployments it allows probing internal network services.
CVE-2026-34576	Postiz is an AI social media scheduling tool. Prior to version 2.21.3, the POST /public/v1/upload-from-url endpoint accepts a user-supplied URL and fetches it server- check (.png, .jpg, etc.) which is trivially bypassed by appending an image extension to any URL path. An authenticated API user can fetch internal network resource uploaded to storage and returned to the attacker. This issue has been patched in version 2.21.3.
CVE-2026-33544	Tinyauth is an authentication and authorization server. Prior to version 5.0.5, all three OAuth service implementations (GenericOAuthService, GithubOAuthService, on singleton instances shared across all concurrent requests. When two users initiate OAuth login for the same provider concurrently, a race condition between Ve identity. This issue has been patched in version 5.0.5.
CVE-2026-25835	Mbed TLS before 3.6.6 and TF-PSA-Crypto before 1.1.0 misuse seeds in a Pseudo-Random Number Generator (PRNG).

CVE-2026-34746	Payload is a free and open source headless content management system. Prior to version 3.79.1, an authenticated Server-Side Request Forgery (SSRF) vulnerabilit to an upload-enabled collection could cause the server to make outbound HTTP requests to arbitrary URLs. This issue has been patched in version 3.79.1.
CVE-2026-34769	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to versions 38.8.6, 39.8.0, 40.7.0, and 41.0.0-beta.8, be appended to the renderer process command line. Apps that construct webPreferences by spreading untrusted configuration objects may inadvertently allow an Apps are only affected if they construct webPreferences from external or untrusted input without an allowlist. Apps that use a fixed, hardcoded webPreferences obj and 41.0.0-beta.8.
CVE-2026-35409	Directus is a real-time API and App dashboard for managing SQL database content. Prior to 11.16.0, a Server-Side Request Forgery (SSRF) protection bypass has be requests to local and private networks could be circumvented using IPv4-Mapped IPv6 address notation. This vulnerability is fixed in 11.16.0.
CVE-2026-35187	pyLoad is a free and open-source download manager written in Python. In 0.5.0b3.dev96 and earlier, the parse_urls API function in src/pyload/core/api/__init__.py fe protocol restriction, or IP blacklist. An authenticated user with ADD permission can make HTTP/HTTPS requests to internal network resources and cloud metadata e with internal services via gopher:// and dict:// protocols, and enumerate file existence via error-based oracle (error 37 vs empty response).
CVE-2026-34222	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to version 0.8.11, there is a broken access control vulnerability
CVE-2026-34936	PraisonAI is a multi-agent teams system. Prior to version 4.5.90, passthrough() and apassthrough() in praisonai accept a caller-controlled api_base parameter that litellm primary path raises AttributeError. No URL scheme validation, private IP filtering, or domain allowlist is applied, allowing requests to any host reachable from
CVE-2026-35533	mise manages dev tools like node, python, cmake, and terraform. From 2026.2.18 through 2026.4.5, mise loads trust-control settings from a local project .mise.tor repository can make that same file appear trusted and then reach dangerous directives such as [env] _.source, templates, hooks, or tasks.
CVE-2026-21367	Transient DOS when processing nonstandard FILS Discovery Frames with out-of-range action sizes during initial scans.
CVE-2026-39384	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Prior to 1.8.212, FreeScout does not take the limit_user_customer_visibility para
CVE-2026-34426	OpenClaw versions prior to commit b57b680 contain an approval bypass vulnerability due to inconsistent environment variable normalization between approval an variables into execution without approval system validation. Attackers can exploit differing normalization logic to discard non-portable keys during approval proces potentially influencing runtime behavior including execution of attacker-controlled binaries.
CVE-2026-35534	ChurchCRM is an open-source church management system. Prior to 7.1.0, a stored cross-site scripting vulnerability exists in PersonView.php due to incorrect use o strips HTML tags, it does not escape quote characters allowing an attacker to break out of the href attribute and inject arbitrary JavaScript event handlers. Any auth field. The XSS fires against any user who views that person's profile page, including administrators, enabling session hijacking and full account takeover. This vulne
CVE-2025-13855	IBM Storage Protect Server 8.2.0 IBM Storage Protect Plus Server is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, wh database.
CVE-2026-39369	WWBN AVideo is an open source video platform. In versions 26.0 and prior, objects/aVideoEncoderReceiveImage.json.php allowed an authenticated uploader to fet expose server-local files through the GIF poster storage path. The vulnerable GIF branch could be abused to read local files such as /etc/passwd or application sour
CVE-2026-34529	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Prior to version 2.62.2, the EPU JavaScript embedded in a crafted EPUB file executes in the victim's browser when they preview the file. This issue has been patched in version 2.62.2.
CVE-2026-21381	Transient DOS when receiving a service data frame with excessive length during device matching over a neighborhood awareness network protocol connection.
CVE-2026-32646	A specific administrative endpoint is accessible without proper authentication, exposing device management functions.
CVE-2024-14033	Hirschmann Industrial IT products (BAT-R, BAT-F, BAT450-F, BAT867-R, BAT867-F, WLC, BAT Controller Virtual) contain a heap overflow vulnerability in the HiLCOS service condition by sending specially crafted requests to the web interface. Attackers can exploit this heap overflow to crash the affected device and cause servic enabled.
CVE-2026-34827	Rack is a modular Ruby web server interface. From versions 3.0.0.beta1 to before 3.1.21, and 3.2.0 to before 3.2.6, Rack::Multipart::Parser#handle_mime_head pa using repeated String#index searches combined with String#slice! prefix deletion. For escape-heavy quoted values, this causes super-linear processing. An unauth parts with long backslash-escaped parameter values to trigger excessive CPU usage during multipart parsing. This results in a denial of service condition in Rack a 3.1.21 and 3.2.6.
CVE-2026-28815	A remote attacker can supply a short X-Wing HPKE encapsulated key and trigger an out-of-bounds read in the C decapsulation path, potentially causing a crash or version 4.3.1.
CVE-2026-34876	An issue was discovered in Mbed TLS 3.x before 3.6.6. An out-of-bounds read vulnerability in mbedtls_ccm_finish() in library/ccm.c allows attackers to obtain adjace parameter. This is caused by missing validation of the tag_len parameter against the size of the internal 16-byte authentication buffer. The issue affects the public directly by applications. In Mbed TLS 4.x versions prior to the fix, the same missing validation exists in the internal implementation; however, the function is not ex multipart CCM API.
CVE-2026-30332	A Time-of-Check to Time-of-Use (TOCTOU) race condition vulnerability in Balena Etcher for Windows prior to v2.1.4 allows attackers to escalate privileges and exec flashing process.
CVE-2022-	Hirschmann EagleSDV version 05.4.01 prior to 05.4.02 contains a denial-of-service vulnerability that causes the device to crash during session establishment when

4986	with these protocol versions to disrupt service availability.
CVE-2026-35467	The stored API keys in temporary browser client is not marked as protected allowing for JavScript console or other errors to allow for extraction of the encryption cr
CVE-2026-22663	prompts.chat prior to commit 7b81836 contains multiple authorization bypass vulnerabilities due to missing isPrivate checks across API endpoints and page metad private prompts. Attackers can exploit these missing authorization checks to retrieve private prompt version history, change requests, examples, current content,
CVE-2026-34148	Fedify is a TypeScript library for building federated server apps powered by ActivityPub. Prior to 1.9.6, 1.10.5, 2.0.8, and 2.1.1, @fedify/fedify follows HTTP redirects without enforcing a maximum redirect count or visited-URL loop detection. An attacker who controls a remote ActivityPub key or actor URL can force a server using resource consumption and denial of service. This vulnerability is fixed in 1.9.6, 1.10.5, 2.0.8, and 2.1.1.
CVE-2026-35562	Allocation of resources without limits in the parsing components in Amazon Athena ODBC driver before 2.1.0.0 might allow a threat actor to cause a denial of servi driver's parsing operations. To remediate this issue, users should upgrade to version 2.1.0.0.
CVE-2025-65114	Apache Traffic Server allows request smuggling if chunked messages are malformed. This issue affects Apache Traffic Server: from 9.0.0 through 9.2.12, from 10.(which fix the issue.
CVE-2018-25246	Wikipedia 12.0 contains a denial of service vulnerability that allows unauthenticated attackers to crash the application by submitting oversized input through the s search bar to trigger an application crash.
CVE-2026-34829	Rack is a modular Ruby web server interface. Prior to versions 2.2.23, 3.1.21, and 3.2.6, Rack::Multipart::Parser only wraps the request body in a BoundedIO when Content-Length header, such as with HTTP chunked transfer encoding, multipart parsing continues until end-of-stream with no total size limit. For file parts, the upl by the buffered in-memory upload limit. An unauthenticated attacker can therefore stream an arbitrarily large multipart file upload and consume unbounded disk s multipart form data. This issue has been patched in versions 2.2.23, 3.1.21, and 3.2.6.
CVE-2026-34601	xmldom is a pure JavaScript W3C standard-based (XML DOM Level 2 Core) `DOMParser` and `XMLSerializer` module. In xmldom versions 0.6.0 and prior and @xml controlled strings containing the CDATA terminator]]> to be inserted into a CDATASection node. During serialization, XMLSerializer emitted the CDATA content ver remain text-only became active XML markup in the serialized output, enabling XML structure injection and downstream business-logic manipulation. This issue has 0.9.9.
CVE-2026-34752	Haraka is a Node.js mail server. Prior to version 3.1.4, sending an email with __proto__: as a header name crashes the Haraka worker process. This issue has been
CVE-2026-1233	The Text to Speech for WP (AI Voices by Mementor) plugin for WordPress is vulnerable to sensitive information exposure in all versions up to, and including, 1.9.8. vendor's external telemetry server in the `Mementor_TTS_Remote_Telemetry` class. This makes it possible for unauthenticated attackers to extract and decode th
CVE-2026-34771	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to versions 38.8.6, 39.8.0, 40.7.0, and 41.0.0-beta.8, vulnerable to a use-after-free when handling fullscreen, pointer-lock, or keyboard-lock permission requests. If the requesting frame navigates or the window closes freed memory, which may lead to a crash or memory corruption. Apps that do not set a permission request handler, or whose handler responds synchronously, are 41.0.0-beta.8.
CVE-2026-26027	GLPI is a free asset and IT management software package. From 11.0.0 to before 11.0.6, an unauthenticated user can store an XSS payload through the inventory
CVE-2026-34824	Mesop is a Python-based UI framework that allows users to build web applications. From version 1.2.3 to before version 1.2.5, an uncontrolled resource consumptio unauthenticated attacker can send a rapid succession of WebSocket messages, forcing the server to spawn an unbounded number of operating system threads. Th Denial of Service (DoS) for any application built on the framework. This issue has been patched in version 1.2.5.
CVE-2026-33184	nimiq/core-rs-albatross is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. Prior to version 1.3.0, the discov The immediate HandshakeAck path then honors limit = 0 and returns zero contacts, which makes the session look benign. Later, after the same session reaches Es With limit = 0, that wraps to usize::MAX and then in rand 0.9.2, choose_multiple() immediately attempts Vec::with_capacity(amount), which deterministically panic
CVE-2026-33540	Distribution is a toolkit to pack, ship, store, and deliver container content. Prior to 3.1.0, in pull-through cache mode, distribution discovers token auth endpoints by The realm URL from a bearer challenge is used without validating that it matches the upstream registry host. As a result, an attacker-controlled upstream (or an at configured upstream credentials via basic auth to an attacker-controlled realm URL. This vulnerability is fixed in 3.1.0.
CVE-2026-35385	In OpenSSH before 10.3, a file downloaded by scp may be installed setuid or setgid, an outcome contrary to some users' expectations, if the download is performe
CVE-2019-25686	Core FTP 2.0 build 653 contains a denial of service vulnerability in the PBSZ command that allows unauthenticated attackers to crash the service by sending a malf a payload exceeding 211 bytes to trigger an access violation and crash the FTP server process.
CVE-2026-27833	Piwigo is an open source photo gallery application for the web. Prior to version 16.3.0, the pwg.history.search API method in Piwigo is registered without the admin gallery visitors. This issue has been patched in version 16.3.0.
CVE-2026-34211	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.36, the @nyariv/sandboxjs parser contains unbounded recursion in the restOfExp function and the lispify/l input by supplying deeply nested expressions (e.g., ~2000 nested parentheses), causing a RangeError: Maximum call stack size exceeded that terminates the proc
CVE-2026-34785	Rack is a modular Ruby web server interface. Prior to versions 2.2.23, 3.1.21, and 3.2.6, Rack::Static determines whether a request should be served as a static file it matches any request path that begins with that string, including unrelated paths such as "/css-config.env" or "/css-backup.sql". As a result, files under the static leading to information disclosure. This issue has been patched in versions 2.2.23, 3.1.21, and 3.2.6.
CVE-2018-25241	VPN Browser+ 1.1.0.0 contains a denial of service vulnerability that allows unauthenticated attackers to crash the application by submitting oversized input throug search bar to trigger an unhandled exception that terminates the application.

CVE-2024-40849	A race condition was addressed with additional validation. This issue is fixed in macOS Sequoia 15.1. An app may be able to break out of its sandbox.
CVE-2026-33951	Signal K Server is a server application that runs on a central hub in a boat. Prior to version 2.24.0-beta.1, the SignalK Server exposes an unauthenticated HTTP end endpoint, accessible via PUT /signalk/v1/api/sourcePriorities, does not enforce authentication or authorization checks and directly assigns user-controlled input to tl sensor data sources are trusted by the system. The changes are immediately applied and persisted to disk, allowing the manipulation to survive server restarts. Th
CVE-2024-44219	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.1. A malicious application with root privileges may be able t
CVE-2018-25245	7 Tik 1.0.1.0 contains a denial of service vulnerability that allows attackers to crash the application by submitting excessively long input strings to the search funct an application crash.
CVE-2025-58136	A bug in POST request handling causes a crash under a certain condition. This issue affects Apache Traffic Server: from 10.0.0 through 10.1.1, from 9.0.0 through 9 issue. A workaround for older versions is to set proxy.config.http.request_buffer_enabled to 0 (the default value is 0).
CVE-2024-44286	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.1. An attacker with physical access can input keyboard ev
CVE-2024-44303	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.1. A malicious application may be able to modify protected parts of the file
CVE-2026-26477	An issue in Dokuwiki v.2025-05-14b 'Librarian' allows a remote attacker to cause a denial of service via the media_upload_xhr() function in the media.php file
CVE-2026-30078	OpenAirInterface V2.2.0 AMF crashes when it receives an NGAP message with invalid procedure code or invalid PDU-type. For example when the message specifica
CVE-2020-37216	Hirschmann HiOS devices versions prior to 08.1.00 and 07.1.01 contain a denial of service vulnerability in the EtherNet/IP stack where improper handling of packet specially crafted UDP EtherNet/IP packets with a length value larger than the actual packet size to render the device inoperable.
CVE-2026-27489	Open Neural Network Exchange (ONNX) is an open standard for machine learning interoperability. Prior to version 1.21.0, a path traversal vulnerability via symlink been patched in version 1.21.0.
CVE-2026-31933	Suricata is a network IDS, IPS and NSM engine. Prior to versions 7.0.15 and 8.0.4, specially crafted traffic can cause Suricata to slow down, affecting performance in
CVE-2026-31931	Suricata is a network IDS, IPS and NSM engine. From version 8.0.0 to before version 8.0.4, use of the "tls.alpn" rule keyword can cause Suricata to crash with a NUL
CVE-2026-35464	pyLoad is a free and open-source download manager written in Python. The fix for CVE-2026-33509 added an ADMIN_ONLY_OPTIONS set to block non-admin users set and passes the existing path restriction because the Flask session directory is outside both PKGDIR and userdir. A user with SETTINGS and ADD permissions can payload as a predictable session file, and trigger arbitrary code execution when any HTTP request arrives with the corresponding session cookie. This vulnerability
CVE-2026-34516	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, a response with an excessive number of multipart heade vulnerability. This issue has been patched in version 3.13.4.
CVE-2026-35485	text-generation-webui is an open-source web interface for running Large Language Models. Prior to 4.3, an unauthenticated path traversal vulnerability in load_gra Gradio does not server-side validate dropdown values, so an attacker can POST directory traversal payloads (e.g., ../../../etc/passwd) via the API and receive the ful
CVE-2025-54324	An issue was discovered in NAS in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, Modem 5400. Incorrect Handling of a DL NAS Transport packet leads to a Denial of Service.
CVE-2026-3902	An issue was discovered in 6.0 before 6.0.4, 5.2 before 5.2.13, and 4.2 before 4.2.30. `ASGIRequest` allows a remote attacker to spoof headers by exploiting an an single version with underscores. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would lik
CVE-2026-35611	Addressable is an alternative implementation to the URI implementation that is part of Ruby's standard library. From 2.3.0 to before 2.9.0, within the URI template expressions vulnerable to catastrophic backtracking. Templates using the * (explode) modifier with any expansion operator (e.g., {foo*}, {+var*}, {#var*}, {/var* quantifiers that are O(2^n) when matched against a maliciously crafted URI. Templates using multiple variables with the + or # operators (e.g., {+v1,v2,v3}) gen matched character class, causing ambiguous backtracking across k variables. When matched against a maliciously crafted URI, this can result in catastrophic back vulnerability is fixed in 2.9.0.
CVE-2026-4748	A regression in the way hashes were calculated caused rules containing the address range syntax (x.x.x.x - y.y.y.y) that only differ in the address range(s) involved pf. Ranges expressed using the address[/mask-bits] syntax were not affected. Some keywords representing actions taken on a packet-matching rule, such as 'log', such configurations, as these rules would always be redundant. Affected rules are silently ignored, which can lead to unexpected behaviour including over- and und
CVE-2026-22815	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, insufficient restrictions in header/trailer handling could c
CVE-2026-	text-generation-webui is an open-source web interface for running Large Language Models. Prior to 4.3, he superbooga and superboogav2 RAG extensions fetch us filtering, no hostname allowlist. An attacker can access cloud metadata endpoints, steal IAM credentials, and probe internal services. The fetched content is exfiltra

35486	
CVE-2026-5032	The W3 Total Cache plugin for WordPress is vulnerable to information exposure in all versions up to, and including, 2.9.3. This is due to the plugin bypassing its ent contains "W3 Total Cache", which causes raw mfunc/mclude dynamic fragment HTML comments — including the W3TC_DYNAMIC_SECURITY security token — to be discover the value of the W3TC_DYNAMIC_SECURITY constant by sending a crafted User-Agent header to any page that contains developer-placed dynamic fragme
CVE-2026-4634	A flaw was found in Keycloak. An unauthenticated attacker can exploit this vulnerability by sending a specially crafted POST request with an excessively long scope consumption and prolonged processing times, ultimately resulting in a Denial of Service (DoS) for the Keycloak server.
CVE-2026-5284	Use after free in Dawn in Google Chrome prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to execute arbitrary code
CVE-2026-34874	An issue was discovered in Mbed TLS through 3.6.5 and 4.x through 4.0.0. There is a NULL pointer dereference in distinguished name parsing that allows an attack
CVE-2026-25833	Mbed TLS 3.5.0 to 3.6.5 fixed in 3.6.6 and 4.1.0 has a buffer overflow in the x509_inet_pton_ipv6() function
CVE-2026-39356	Drizzle is a modern TypeScript ORM. Prior to 0.45.2 and 1.0.0-beta.20, Drizzle ORM improperly escaped quoted SQL identifiers in its dialect-specific escapeName() escaped before the identifier was wrapped in quotes or backticks. As a result, applications that pass attacker-controlled input to APIs that construct SQL identifiers identifier and inject SQL. This vulnerability is fixed in 0.45.2 and 1.0.0-beta.20.
CVE-2026-33034	An issue was discovered in 6.0 before 6.0.4, 5.2 before 5.2.13, and 4.2 before 4.2.30. ASGI requests with a missing or understated `Content-Length` header could `HttpRequest.body`, allowing remote attackers to load an unbounded request body into memory. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2. for reporting this issue.
CVE-2026-35526	Strawberry GraphQL is a library for creating GraphQL APIs. Prior to 0.312.3, Strawberry GraphQL's WebSocket subscription handlers for both the graphql-transport- object for every incoming subscribe message without enforcing any limit on the number of active subscriptions per connection. An unauthenticated attacker can op messages with unique IDs. Each message unconditionally spawns a new asyncio.Task and async generator, causing linear memory growth and event loop saturatio 0.312.3.
CVE-2026-34376	PdfDing is a selfhosted PDF manager, viewer and editor offering a seamless user experience on multiple devices. Prior to version 1.7.0, an access-control vulnerabi directly calling the file-serving endpoint without completing the password verification flow. This results in unauthorized access to confidential documents that users version 1.7.0.
CVE-2025-57834	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem (Exynos 980, 850, 990, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 5400, and Modem 5410). The absence of proper input validation leads to a Denial of Service.
CVE-2026-33614	An unauthenticated remote attacker can exploit an unauthenticated SQL Injection vulnerability in the getinfo endpoint due to improper neutralization of special ele
CVE-2026-35172	Distribution is a toolkit to pack, ship, store, and deliver container content. Prior to 3.1.0, distribution can restore read access in repo a after an explicit delete when enabled. The delete path clears the shared digest descriptor but leaves stale repo-scoped membership behind, so a later Stat or Get from repo b repopulates the s vulnerability is fixed in 3.1.0.
CVE-2026-33616	An unauthenticated remote attacker can exploit an unauthenticated blind SQL Injection vulnerability in the mb24api endpoint due to improper neutralization of spe confidentiality.
CVE-2026-35523	Strawberry GraphQL is a library for creating GraphQL APIs. Strawberry up until version 0.312.3 is vulnerable to an authentication bypass on WebSocket subscriptio connection_init handshake has been completed before processing start (subscription) messages. This allows a remote attacker to skip the on_ws_connect authenti message directly, without ever sending connection_init. This vulnerability is fixed in 0.312.3.
CVE-2026-35203	ZLMediaKit is a streaming media service framework. the VP9 RTP payload parser in ext-codec/VP9Rtp.cpp reads multiple fields from the RTP payload based on flag crafted VP9 RTP packet with a 1-byte payload (0xFF, all flags set) causes the parser to read past the end of the allocated buffer, resulting in a heap-buffer-overflow 435dcbcbbf700fd63b2ca9eac6cef3b5ea75169d.
CVE-2026-31932	Suricata is a network IDS, IPS and NSM engine. Prior to versions 7.0.15 and 8.0.4, inefficiency in KRB5 buffering can lead to performance degradation. This issue ha
CVE-2026-39376	FastFeedParser is a high performance RSS, Atom and RDF parser. Prior to 0.5.10, when parse() fetches a URL that returns an HTML page containing a <meta http-e limit, no visited-URL deduplication, and no redirect count cap. An attacker-controlled server that returns an infinite chain of HTML meta-refresh responses causes u vulnerability can also be chained with the companion SSRF issue to reach internal network targets after bypassing the initial URL check. This vulnerability is fixed i
CVE-2026-35209	defu is software that allows uers to assign default properties recursively. Prior to version 6.1.5, applications that pass unsanitized user input (e.g. parsed JSON requ argument to `defu()` are vulnerable to prototype pollution. A crafted payload containing a `__proto__` key can override intended default values in the merged resu object. `Object.assign` invokes the `__proto__` setter, which replaces the resulting object's `[[Prototype]]` with attacker-controlled values. Properties inherited fro `for...in` loop and land in the final result. Version 6.1.5 replaces `Object.assign({}, defaults)` with object spread (`{ ...defaults }`), which uses `[[DefineOwnProper
CVE-2025-59440	An issue was discovered in USIM in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, Modem 5400. Improper handling of SIM card proactive commands leads to a Denial of Service.
CVE-2026-31842	Tinyproxy through 1.11.3 is vulnerable to HTTP request parsing desynchronization due to a case-sensitive comparison of the Transfer-Encoding header in src/reqs.c against "chunked", even though RFC 7230 specifies that transfer-coding names are case-insensitive. By sending a request with Transfer-Encoding: Chunked, an un having no body. In this state, Tinyproxy sets content_length.client to -1, skips pull_client_data_chunked(), forwards request headers upstream, and transitions into leads to inconsistent request state between Tinyproxy and backend servers. RFC-compliant backends (e.g., Node.js, Nginx) will continue waiting for chunked body denial of service through backend worker exhaustion. Additionally, in deployments where Tinyproxy is used for request-body inspection, filtering, or security enforc potential security control bypass.
CVE-	OpenTelemetry-Go is the Go implementation of OpenTelemetry. From 1.36.0 to 1.40.0, multi-value baggage: header extraction parses each header field-value inde

2026-29181	cpu and allocations by sending many baggage: header lines, even when each individual value is within the 8192-byte per-value parse limit. This vulnerability is fixe
CVE-2025-71282	XenForo before 2.3.7 discloses filesystem paths through exception messages triggered by open_basedir restrictions. This allows an attacker to obtain information a
CVE-2026-34904	Cross-Site Request Forgery (CSRF) vulnerability in Analytify Simple Social Media Share Buttons allows Cross Site Request Forgery.This issue affects Simple Social M
CVE-2026-34986	Go JOSE provides an implementation of the Javascript Object Signing and Encryption set of standards in Go, including support for JSON Web Encryption (JWE), JSON decrypting a JSON Web Encryption (JWE) object will panic if the alg field indicates a key wrapping algorithm (one ending in KW, with the exception of A128GCMKW, happens when cipher.KeyUnwrap() in key_wrap.go attempts to allocate a slice with a zero or negative length based on the length of the encrypted_key. This code p ParseEncryptedCompact() followed by Decrypt() on the resulting object. Note that the parse functions take a list of accepted key algorithms. If the accepted key al application will be unaffected. This panic is also reachable by calling cipher.KeyUnwrap() directly with any ciphertext parameter less than 16 bytes long, but calling vulnerability is fixed in 4.1.4 and 3.0.5.
CVE-2026-34896	Cross-Site Request Forgery (CSRF) vulnerability in Analytify Under Construction, Coming Soon & Maintenance Mode allows Cross Site Request Forgery.This issue af
CVE-2026-35036	Ech0 is an open-source, self-hosted publishing platform for personal idea sharing. Prior to 4.2.8, Ech0 implements link preview (editor fetches a page title) through unsafe: the route is unauthenticated, accepts a fully attacker-controlled URL, performs a server-side GET, reads the entire response body into memory (io.ReadAll) client. Anyone who can reach the instance can force the Ech0 server to open HTTP/HTTPS URLs of their choice as seen from the server’s network position (Docker b
CVE-2026-34543	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. From version 3.4 through the decoded pixel data (information disclosure). This occurs under default settings; simply reading a malicious EXR file is sufficient to trigger the issue, wit
CVE-2026-35042	fast-jwt provides fast JSON Web Token (JWT) implementation. In 6.1.0 and earlier, fast-jwt does not validate the crit (Critical) Header Parameter defined in RFC 7515 not understand, the library accepts the token instead of rejecting it. This violates the MUST requirement in the RFC.
CVE-2026-24175	NVIDIA Triton Inference Server contains a vulnerability where an attacker could cause a server crash by sending a malformed request header to the server. A succe
CVE-2026-35405	libp2p-rust is the official rust language Implementation of the libp2p networking stack. Prior to 0.17.1, libp2p-rendezvous server has no limit on how many namespa namespaces in a loop and the server happily accepts every single one allocating memory for each registration with no pushback. Keep doing this long enough (or v fixed in 0.17.1.
CVE-2025-57835	An issue was discovered in RRC in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, Modem 5400. Improper memory initialization results in an illegal memory access, causing a system crash via a malformed RRCReconfiguration message.
CVE-2026-24174	NVIDIA Triton Inference Server contains a vulnerability where an attacker could cause a server crash by sending a malformed request to the server. A successful ex
CVE-2026-35092	A flaw was found in Corosync. An integer overflow vulnerability in Corosync's join message sanity validation allows a remote, unauthenticated attacker to send craf leading to a denial of service. This vulnerability specifically affects Corosync deployments configured to use totemudp/totemudpu mode.
CVE-2026-24173	NVIDIA Triton Inference Server contains a vulnerability where an attacker could cause a server crash by sending a malformed request to the server. A successful ex
CVE-2026-31934	Suricata is a network IDS, IPS and NSM engine. From version 8.0.0 to before version 8.0.4, there is a quadratic complexity issue when searching for URLs in mime e patched in version 8.0.4.
CVE-2026-5277	Integer overflow in ANGLE in Google Chrome on Windows prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to perfor severity: High)
CVE-2026-24146	NVIDIA Triton Inference Server contains a vulnerability where insufficient input validation and a large number of outputs could cause a server crash. A successful ex
CVE-2026-39312	SoftEtherVPN is a an open-source cross-platform multi-protocol VPN Program. In 5.2.5188 and earlier, a pre-authentication denial-of-service vulnerability exists in S Edition). An unauthenticated remote attacker can crash the vpnserver process by sending a single malformed EAP-TLS packet over raw L2TP (UDP/1701), terminati
CVE-2026-30573	A Business Logic vulnerability exists in SourceCodester Pharmacy Product Management System 1.0. The vulnerability is located in the add-sales.php file. The applic to submit negative values for sales transactions. This leads to incorrect financial calculations, corruption of sales reports, and potential financial loss.
CVE-2026-31937	Suricata is a network IDS, IPS and NSM engine. Prior to version 7.0.15, inefficiency in DCERPC buffering can lead to a performance degradation. This issue has beer
CVE-2026-31935	Suricata is a network IDS, IPS and NSM engine. Prior to versions 7.0.15 and 8.0.4, flooding of craft HTTP2 continuation frames can lead to memory exhaustion, usua issue has been patched in versions 7.0.15 and 8.0.4.
CVE-2026-35099	Lakeside SysTrack Agent 11 before 11.5.0.15 has a race condition with resultant local privilege escalation to SYSTEM. The fixed versions are 11.2.1.28, 11.3.0.38, 1

CVE-2026-35535	In Sudo through 1.9.17p2 before 3e474c2, a failure of a setuid, setgid, or setgroups call, during a privilege drop before running the mailer, is not a fatal error and c
CVE-2026-34076	Clerk JavaScript is the official JavaScript repository for Clerk authentication. In @clerk/hono from versions 0.1.0 to before 0.1.5, @clerk/express from versions 2.0.0 from versions 3.1.0 to before 3.1.5, the clerkFrontendApiProxy function in @clerk/backend is vulnerable to Server-Side Request Forgery (SSRF). An unauthenticated Clerk-Secret-Key to an attacker-controlled server. This issue has been patched in @clerk/hono version 0.1.5, @clerk/express version 2.0.7, @clerk/backend version
CVE-2026-35561	Insufficient authentication security controls in the browser-based authentication components in Amazon Athena ODBC driver before 2.1.0.0 might allow a threat ac browser-based authentication flows. To remediate this issue, users should upgrade to version 2.1.0.0.
CVE-2026-35560	Improper certificate validation in the identity provider connection components in Amazon Athena ODBC driver before 2.1.0.0 might allow a man-in-the-middle threa security when connecting to identity providers. This only applies to connections with external identity providers and does not apply to connections with Athena. To
CVE-2026-4282	A flaw was found in Keycloak. The SingleUseObjectProvider, a global key-value store, lacks proper type and namespace isolation. This vulnerability allows an unaut the creation of admin-capable access tokens, resulting in privilege escalation.
CVE-2026-35489	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. Prior to 2.6.4, the POST /api/food/{id}/shopping/ endpoint reac ShoppingListEntry.objects.create(). Invalid amount values (non-numeric strings) cause an unhandled exception and HTTP 500. A unit ID from a different Space can All other endpoints creating ShoppingListEntry use ShoppingListEntrySerializer, which validates and sanitizes these fields. This vulnerability is fixed in 2.6.4.
CVE-2026-30273	pandas-ai v3.0.0 was discovered to contain a SQL injection vulnerability via the pandasai.agent.base._execute_sql_query component.
CVE-2026-1345	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 throug unauthenticated user to execute arbitrary commands as lower user privileges on the system due to improper validation of user supplied input.
CVE-2026-5575	A vulnerability was detected in SourceCodester/jkev Record Management System 1.0. Affected by this vulnerability is an unknown functionality of the file index.php injection. The attack may be launched remotely. The exploit is now public and may be used.
CVE-2026-20151	A vulnerability in the web interface of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an authenticated, remote attacker to elevate privileges o sensitive user information. An attacker could exploit this vulnerability by sending a crafted message to an affected Cisco SSM On-Prem host and retrieving session attacker to elevate privileges on the affected system from low to administrative. To exploit this vulnerability, the attacker must have valid credentials for a user ac information only about users who logged in to the Cisco SSM On-Prem host using the web interface and who are currently logged in. SSH sessions are not affected.
CVE-2026-5418	A vulnerability was identified in appsmithorg appsmith up to 1.97. Impacted is the function computeDisallowedHosts of the file app/server/appsmith-interfaces/src/ manipulation leads to server-side request forgery. The attack may be launched remotely. The exploit is publicly available and might be used. Upgrading to version upgraded. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.
CVE-2026-5584	A vulnerability has been found in Fosowl agenticSeek 0.1.0. Impacted is the function PyInterpreter.execute of the file sources/tools/PyInterpreter.py of the compone launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any
CVE-2026-5577	A vulnerability has been found in Song-Li cross_browser up to ca690f0fe6954fd9bcda36d071b68ed8682a786a. This affects an unknown part of the file flask/unique argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. This product implements a updated releases is unavailable. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-3879	Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Equipment Mailbox Details report.
CVE-2026-5256	A flaw has been found in code-projects Simple Laundry System 1.0. This vulnerability affects unknown code of the file /modify.php of the component Parameter Ha exploitation of the attack is possible. The exploit has been published and may be used.
CVE-2026-5257	A vulnerability has been found in code-projects Simple Laundry System 1.0. This issue affects some unknown processing of the file /delstaffinfo.php of the compone injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.
CVE-2026-0932	Blind server-side request forgery (SSRF) vulnerability in legacy connection methods of document co-authoring features in M-Files Server before 26.3 allow an unaut
CVE-2026-5261	A vulnerability was identified in Shandong Hoteam InforCenter PLM up to 8.3.8. The impacted element is the function uploadFileToIIS of the file /Base/BaseHandler. to initiate the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any
CVE-2026-22767	Dell AppSync, version(s) 4.6.0, contain(s) an UNIX Symbolic Link (Symlink) Following vulnerability. A low privileged attacker with local access could potentially expl
CVE-2026-22768	Dell AppSync, version(s) 4.6.0, contain(s) an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could p
CVE-2026-24156	NVIDIA DALI contains a vulnerability where an attacker could cause a deserialization of untrusted data. A successful exploit of this vulnerability might lead to arbitr
CVE-2026-5526	A security flaw has been discovered in Tenda 4G03 Pro up to 1.0/1.1/04.03.01.53/192.168.0.1. Affected by this vulnerability is an unknown functionality of the file / performed from remote. The exploit has been released to the public and may be used for attacks.

CVE-2026-5534	A vulnerability was identified in itsourcecode Online Enrollment System 1.0. This affects an unknown function of the file /sms/user/index.php?view=edit&id=10 of t sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.
CVE-2026-5536	A weakness has been identified in FedML-AI FedML up to 0.8.9. Affected is the function sendMessage of the file grpc_server.py of the component gRPC server. Exec remote. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-39306	PraisonAI is a multi-agent teams system. Prior to 1.5.113, PraisonAI's recipe registry pull flow extracts attacker-controlled .praison tar archives with tar.extractall() can upload a recipe bundle that contains ../ traversal entries and any user who later pulls that recipe will write files outside the output directory they selected. This registry workflow. It affects both the local registry pull path and the HTTP registry pull path. The checksum verification does not prevent exploitation because the m in 1.5.113.
CVE-2026-5258	A vulnerability was found in Sanster IOPaint 1.5.3. Impacted is the function _get_file of the file iopaint/file_manager/file_manager.py of the component File Manager attack is possible to be carried out remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did no
CVE-2026-5540	A vulnerability has been found in code-projects Simple Laundry System 1.0. This vulnerability affects unknown code of the file /modifymember.php of the compone injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2026-5551	A security flaw has been discovered in itsourcecode Free Hotel Reservation System 1.0. This vulnerability affects unknown code of the file /hotel/admin/login.php o in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.
CVE-2026-5554	A security flaw has been discovered in code-projects Concert Ticket Reservation System 1.0. Affected by this issue is some unknown functionality of the file /Conce Handler. Performing a manipulation of the argument searching results in sql injection. The attack may be initiated remotely. The exploit has been released to the p
CVE-2026-5555	A weakness has been identified in code-projects Concert Ticket Reservation System 1.0. This affects an unknown part of the file /ConcertTicketReservationSystem- the argument Email can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attack
CVE-2026-5562	A vulnerability was identified in provectus kafka-ui up to 0.7.2. This impacts the function validateAccess of the file /api/smartfilters/testexecutions of the componen 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.
CVE-2026-27655	Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Permissions Based on Mailboxes report.
CVE-2026-5564	A weakness has been identified in code-projects Simple Laundry System 1.0. Affected by this vulnerability is an unknown functionality of the file /searchguest.php searchServiceId causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.
CVE-2026-4108	Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Non-Owner Mailbox Permission report.
CVE-2026-4107	Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Folder Message Count and Size report.
CVE-2026-3880	Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Public Folder Client Permissions report.
CVE-2026-28703	Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Mails Exchanged Between Users report.
CVE-2026-28756	Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Permissions based on Distribution Groups report.
CVE-2026-28754	Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Distribution Lists report.
CVE-2026-5565	A security vulnerability has been detected in code-projects Simple Laundry System 1.0. Affected by this issue is some unknown functionality of the file /delmember userid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.
CVE-2025-7024	Incorrect Default Permissions vulnerability in AIRBUS PSS TETRA Connectivity Server on Windows Server OS allows Privilege Abuse. An attacker may execute arbitr into the vulnerable directory. This issue affects TETRA connectivity Server: 7.0. Vulnerability fix is available and delivered to impacted customers.
CVE-2026-35574	ChurchCRM is an open-source church management system. Prior to 6.5.3, a stored Cross-Site Scripting (XSS) vulnerability in ChurchCRM's Note Editor allows authe context of other users' browsers, including administrators. This can lead to session hijacking, privilege escalation, and unauthorized access to sensitive church mer
CVE-2026-5569	A vulnerability was found in Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30. Impacted is an unknown function of the file /Technostrobe/ of the component Endpoi from remote. The exploit has been made public and could be used. Multiple endpoints are affected. The vendor was contacted early about this disclosure but did n
CVE-2026-5570	A vulnerability was determined in Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30. The affected element is the function index_config of the file /LoginCB. This mar 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.

CVE-2026-5573	A weakness has been identified in Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30. This impacts an unknown function of the file /fs. Executing a manipulation of th 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 respor
CVE-2026-34544	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. From version 3.4 write in any application that decodes it via exr_decoding_run(). Consequences range from immediate crash (most likely) to corruption of adjacent heap allocations
CVE-2026-34545	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. From version 3.4 compression and a channel width of 32768 can write controlled data beyond the output heap buffer in any application that decodes EXR images. The write primitiv additional pixel past the overflow point. In this context, a heap write overflow can lead to remote code execution on systems. This issue has been patched in versio
CVE-2026-5238	A weakness has been identified in itsourcecode Payroll Management System 1.0. Affected by this issue is some unknown functionality of the file /view_employee.ph can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.
CVE-2026-5665	A security vulnerability has been detected in code-projects Online FIR System 1.0. Affected by this vulnerability is an unknown functionality of the file /Login/checkl leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.
CVE-2026-5244	A vulnerability has been found in Cesanta Mongoose up to 7.20. This affects the function mg_tls_recv_cert of the file mongoose.c of the component TLS 1.3 Handle attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 7.21 mitigates this issue. The name of the p affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.
CVE-2026-5669	A vulnerability has been found in Cyber-III Student-Management-System up to 1a938fa61e9f735078e9b291d2e6215b4942af3f. This vulnerability affects unknown the argument Password leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This produ version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded y
CVE-2026-5346	A vulnerability was determined in huimeicloud hm_editor up to 2.2.3. Impacted is the function client.get of the file src/mcp-server.js of the component image-to-ba request forgery. 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
CVE-2026-5642	A vulnerability was determined in Cyber-III Student-Management-System up to 1a938fa61e9f735078e9b291d2e6215b4942af3f. This affects an unknown function c manipulation of the argument Name causes improper authorization. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may b Therefore, no version details for affected nor updated releases are available. The project was informed of the problem early through an issue report but has not res
CVE-2026-5637	A security vulnerability has been detected in projectworlds Car Rental System 1.0. This vulnerability affects unknown code of the file /message_admin.php of the co sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.
CVE-2026-5368	A vulnerability was determined in projectworlds Car Rental Project 1.0. The affected element is an unknown function of the file /login.php of the component Parame exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.
CVE-2026-5741	A weakness has been identified in suvarchal docker-mcp-server up to 0.1.0. The impacted element is the function stop_container/remove_container/pull_image of t 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. The project
CVE-2026-5634	A vulnerability was identified in projectworlds Car Rental Project 1.0. Affected by this vulnerability is an unknown functionality of the file /book_car.php of the comp injection. The attack can be initiated remotely. The exploit is publicly available and might be used.
CVE-2026-5633	A vulnerability was determined in assafelovic gpt-researcher up to 3.4.3. Affected is an unknown function of the component ws Endpoint. Executing a manipulation launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but
CVE-2026-5616	A security vulnerability has been detected in JeecgBoot 3.9.0/3.9.1. The impacted element is an unknown function of the file jeecg-boot/jeecg-module-system/jeecg component AI Chat Module. Such manipulation leads to missing authentication. The attack can be executed remotely. The name of the patch is b7c9aeba7aefda9e practice to apply a patch to resolve this issue. The project fixed the issue with a commit which shall be part of the next official release.
CVE-2026-5632	A vulnerability was found in assafelovic gpt-researcher up to 3.4.3. This impacts an unknown function of the component HTTP REST API Endpoint. Performing a mar 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.
CVE-2026-5631	A vulnerability has been found in assafelovic gpt-researcher up to 3.4.3. This affects the function extract_command_data of the file backend/server/server_utils.py injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The project was informed of the problem early
CVE-2026-5739	A security flaw has been discovered in PowerJob 5.1.0/5.1.1/5.1.2. The affected element is the function GroovyEvaluator.evaluate of the file /openApi/addWorkflowN nodeParams results in code injection. The attack can be executed remotely. The project was informed of the problem early through an issue report but has not resp
CVE-2026-5334	A weakness has been identified in itsourcecode Online Enrollment System 1.0. Impacted is an unknown function of the file /enrollment/index.php?view=edit&id=3 causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.
CVE-2026-5333	A security flaw has been discovered in DefaultFuction Content-Management-System 1.0. This issue affects some unknown processing of the file /admin/tools.php. T executed remotely. The exploit has been released to the public and may be used for attacks.
CVE-2026-5645	A weakness has been identified in projectworlds Car Rental System 1.0. Affected by this vulnerability is an unknown functionality of the file /pay.php of the compor sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.
CVE-2026-5672	A vulnerability has been found in code-projects Simple IT Discussion Forum 1.0. Affected by this issue is some unknown functionality of the file /edit-category.php c sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.

CVE-2026-5646	A security vulnerability has been detected in code-projects Easy Blog Site 1.0. Affected by this issue is some unknown functionality of the file login.php. The manip initiated remotely. The exploit has been disclosed publicly and may be used.
CVE-2026-5320	A vulnerability was detected in vanna-ai vanna up to 2.0.2. Affected by this vulnerability is an unknown functionality of the file /api/vanna/v2/ of the component Ch 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.
CVE-2026-3872	A flaw was found in Keycloak. This issue allows an attacker, who controls another path on the same web server, to bypass the allowed path in redirect Uniform Res an access token, resulting in information disclosure.
CVE-2026-5678	A weakness has been identified in Totolink A7100RU 7.4cu.2313_b20191024. The affected element is the function setScheduleCfg of the file /cgi-bin/cstecgi.cgi. Ex attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.
CVE-2026-5677	A security flaw has been discovered in Totolink A7100RU 7.4cu.2313_b20191024. Impacted is the function CsteSystem of the file /cgi-bin/cstecgi.cgi. Performing a may be initiated remotely. The exploit has been released to the public and may be used for attacks.
CVE-2026-5736	A vulnerability was identified in PowerJob 5.1.0/5.1.1/5.1.2. Impacted is an unknown function of the file powerjob-server/powerjob-server-starter/src/main/java/tech Endpoint. The manipulation of the argument customQuery leads to sql injection. Remote exploitation of the attack is possible. The project was informed of the prob
CVE-2026-3780	The application's installer runs with elevated privileges but resolves system executables and DLLs using untrusted search paths that can include user-writable dire have them loaded or executed instead of the legitimate system files, resulting in local privilege escalation.
CVE-2026-5648	A flaw has been found in code-projects Simple Laundry System 1.0. This vulnerability affects unknown code of the file /userfinishregister.php of the component Par Remote exploitation of the attack is possible. The exploit has been published and may be used.
CVE-2026-5692	A vulnerability was found in Totolink A7100RU 7.4cu.2313_b20191024. This impacts the function setGameSpeedCfg of the file /cgi-bin/cstecgi.cgi. The manipulatio performed from remote. The exploit has been made public and could be used.
CVE-2026-5691	A vulnerability has been found in Totolink A7100RU 7.4cu.2313_b20191024. This affects the function setFirewallType of the file /cgi-bin/cstecgi.cgi. The manipulati to be carried out remotely. The exploit has been disclosed to the public and may be used.
CVE-2026-5690	A flaw has been found in Totolink A7100RU 7.4cu.2313_b20191024. The impacted element is the function setRemoteCfg of the file /cgi-bin/cstecgi.cgi. Executing a can be executed remotely. The exploit has been published and may be used.
CVE-2022-4987	Hirschmann Industrial HiVision version 08.1.03 prior to 08.1.04 and 08.2.00 contains a vulnerability in the execution of user-configured external applications that a sanitization, an attacker can place a malicious binary in the execution path of a configured external application, causing it to be executed instead of the intended a context of the external application.
CVE-2026-5663	A security flaw has been discovered in OFFIS DCMTK up to 3.7.0. This impacts the function executeOnReception/executeOnEndOfStudy of the file dcmnet/apps/stor injection. Remote exploitation of the attack is possible. The patch is named edbb085e45788dccaf0e64d71534cfca925784b8. Applying a patch is the recommende
CVE-2026-5676	A vulnerability was identified in Totolink A8000R 5.9c.681_B20180413. This issue affects the function setLanguageCfg of the file /cgi-bin/cstecgi.cgi. Such manipula launched remotely. The exploit is publicly available and might be used.
CVE-2026-5322	A vulnerability has been found in AlejandroArciniegas mcp-data-vis bc597e391f184d2187062fd567599a3cb72adf51/de5a51525a69822290eaee569a1ab447b4907 component MCP Handler. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be us result, specific version information for affected or updated releases is not available. The vendor was contacted early about this disclosure but did not respond in an
CVE-2026-5689	A vulnerability was detected in Totolink A7100RU 7.4cu.2313_b20191024. The affected element is the function setNtpCfg of the file /cgi-bin/cstecgi.cgi. Performing exploitation of the attack is possible. The exploit is now public and may be used.
CVE-2026-5688	A security vulnerability has been detected in Totolink A7100RU 7.4cu.2313_b20191024. Impacted is the function setDdnsCfg of the file /cgi-bin/cstecgi.cgi. Such m be launched remotely. The exploit has been disclosed publicly and may be used.
CVE-2026-39343	ChurchCRM is an open-source church management system. Prior to 7.1.0, a SQL injection vulnerability exists in the EditEventTypes.php file, which is only accessibl a SQL query, allowing an administrator to execute arbitrary SQL commands directly against the database. This vulnerability is fixed in 7.1.0.
CVE-2026-35056	XenForo before 2.3.9 and before 2.2.18 allows remote code execution (RCE) by authenticated, but malicious, admin users. An attacker with admin panel access ca
CVE-2026-29782	OpenSTAManager is an open source management software for technical assistance and invoicing. Prior to version 2.10.2, the oauth2.php file in OpenSTAManager i zz_oauth2 table using the attacker-controlled GET parameter state, and during the OAuth2 configuration flow calls unserialize() on the access_token field without a
CVE-2026-27885	Piwigo is an open source photo gallery application for the web. Prior to version 16.3.0, a SQL Injection vulnerability was discovered in Piwigo affecting the Activity L sensitive data from the database, including user credentials, email addresses, and all stored content. This issue has been patched in version 16.3.0.
CVE-2026-35581	Emissary is a P2P based data-driven workflow engine. Prior to 8.39.0, the Executrix utility class constructed shell commands by concatenating configuration-derive spaces were replaced with underscores, allowing shell metacharacters (;, |, $, `, (,), etc.) to pass through into /bin/sh -c command execution. This vulnerability is fi
CVE-	

2018-25250	MyBB Last User's Threads in Profile Plugin 1.2 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts by crafting thre subject field that execute when users visit the attacker's profile page.
CVE-2026-35035	CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to 0.31.2.0 , Company Information. Several administrative configuration fields accept attacker-controlled input that is stored server-side and later rendered without proper outp public-facing pages only, such as the main landing page. There is no execution in the administrative dashboard—the vulnerability only impacts the public frontend.
CVE-2026-34607	Emlog is an open source website building system. In versions 2.6.2 and prior, a path traversal vulnerability exists in the emUnZip() function (include/lib/common.ph function calls $zip->extractTo($path) without sanitizing ZIP entry names. An authenticated admin can upload a crafted ZIP containing entries with ../ sequences to Remote Code Execution (RCE). At time of publication, there are no publicly available patches.
CVE-2026-39325	ChurchCRM is an open-source church management system. Prior to 7.1.0, an SQL injection vulnerability was found in the endpoint /SettingsUser.php in ChurchCRM the type array parameter via the index and thus extract and modify information from the database. This vulnerability is fixed in 7.1.0.
CVE-2026-22666	Dolibarr ERP/CRM versions prior to 23.0.2 contain an authenticated remote code execution vulnerability in the dol_eval_standard() function that fails to apply forbic Attackers with administrator privileges can inject malicious payloads through computed extrafields or other evaluation paths using PHP dynamic callable syntax to
CVE-2026-27834	Piwigo is an open source photo gallery application for the web. Prior to version 16.3.0, a SQL Injection vulnerability exists in the pwg.users.getList Web Service API sanitization, allowing authenticated administrators to execute arbitrary SQL commands. This issue has been patched in version 16.3.0.
CVE-2026-5425	The Widgets for Social Photo Feed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'feed_data' parameter keys in all versions up to, and inc possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2026-1540	The Spam Protect for Contact Form 7 WordPress plugin before 1.2.10 allows logging to a PHP file, which could allow an attacker with editor access to achieve Remc
CVE-2026-2936	The Visitor Traffic Real Time Statistics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'page_title' parameter in all versions up to, and inclu possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an admin user accesses the Traffic by Title section.
CVE-2026-0686	The Webmention plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.6.2 in the 'MF2::parse_authorpage' functi 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
CVE-2026-25932	GLPI is a Free Asset and IT Management Software package. From 0.60 to before 10.0.24, an authenticated technician user can store an XSS payload in a supplier fi
CVE-2026-35037	Ech0 is an open-source, self-hosted publishing platform for personal idea sharing. Prior to 4.2.8, the GET /api/website/title endpoint accepts an arbitrary URL via the validation of the target host or IP address. The endpoint requires no authentication. An attacker can use this to reach internal network services, cloud metadata en exfiltrated via the HTML <title> tag extraction This vulnerability is fixed in 4.2.8.
CVE-2026-33613	Due to the improper neutralisation of special elements used in an OS command, a remote attacker can exploit an RCE vulnerability in the generateSrpArray functic attacker has some other way to write arbitrary data to the user table.
CVE-2018-25248	MyBB Downloads Plugin 2.0.3 contains a persistent cross-site scripting vulnerability that allows regular members to inject malicious scripts through the download t parameter, which executes when administrators validate the download in downloads.php.
CVE-2026-29047	GLPI is a free asset and IT management software package. From 10.0.0 to before 10.0.24 and 11.0.6, an authenticated user can perform a SQL injection via the log
CVE-2026-35536	In Tornado before 6.5.5, cookie attribute injection could occur because the domain, path, and samesite arguments to .RequestHandler.set_cookie were not checke
CVE-2026-39308	PraisonAI is a multi-agent teams system. Prior to 1.5.113, PraisonAI's recipe registry publish endpoint writes uploaded recipe bundles to a filesystem path derived f version match the HTTP route. A malicious publisher can place ../ traversal sequences in the bundle manifest and cause the registry server to create files outside th 400. This is an arbitrary file write / path traversal issue on the registry host. It affects deployments that expose the recipe registry publish flow. If the registry is inte trigger it. If a token is configured, any user with publish access can still exploit it. This vulnerability is fixed in 1.5.113.
CVE-2026-34790	Endian Firewall version 3.3.25 and prior allow authenticated users to delete arbitrary files via directory traversal in the remove ARCHIVE parameter to /cgi-bin/back sanitization of directory traversal sequences, which is then passed to an unlink() call.
CVE-2026-35167	Kedro is a toolbox for production-ready data science. Prior to 1.3.0, the _get_versioned_path() method in kedro/io/core.py constructs filesystem paths by directly in are used as path components, traversal sequences such as ../ are preserved and can escape the intended versioned dataset directory. This is reachable through m load_versions=...), and the CLI via kedro run --load-versions=dataset:../../../secrets. An attacker who can influence the version string can force Kedro to load files fr poisoning, or cross-tenant data access in shared environments. This vulnerability is fixed in 1.3.0.
CVE-2026-3445	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress plugin for WordPress is vulnerable to u This is due to a missing ownership verification on the `change_plan_sub_id` parameter in the `process_checkout()` function. This makes it possible for authenticate subscription during checkout to manipulate proration calculations, allowing them to obtain paid lifetime membership plans without payment via the `ppress_proces
CVE-2026-39370	WWBN AVideo is an open source video platform. In versions 26.0 and prior, objects/aVideoEncoder.json.php still allows attacker-controlled downloadURL values wit .webm to bypass SSRF validation. The server then fetches the response and stores it as media content. This allows an authenticated uploader to turn the upload-by caused by an incomplete fix for CVE-2026-27732.
CVE-2026-	OpenHarness prior to commit 166fcfe contains an improper access control vulnerability in built-in file tools due to inconsistent parameter handling in permission er local files outside the intended repository scope. Attackers can exploit the path parameter not being passed to the PermissionChecker in read_file, write_file, edit_f

22682	configuration files, credentials, and SSH material, or create and overwrite files in restricted host paths in full_auto mode.
CVE-2025-47400	Cryptographic issue while copying data to a destination buffer without validating its size.
CVE-2026-35176	openFPGALoader is a utility for programming FPGAs. In 1.1.1 and earlier, a heap-buffer-overflow read vulnerability exists in POFParser::parseSection() that allows o is required to trigger this vulnerability.
CVE-2026-34603	Tina is a headless content management system. Prior to version 2.2.2, @tinacms/cli recently added lexical path-traversal checks to the dev media routes, but the i junction targets. If a link already exists under the media root, Tina accepts a path like pivot/written-from-media.txt as "inside" the media directory and then perforr listing and write access, and the same root cause also affects delete. This issue has been patched in version 2.2.2.
CVE-2026-4947	Addressed a potential insecure direct object reference (IDOR) vulnerability in the signing invitation acceptance process. Under certain conditions, this issue could h user-supplied object identifiers, potentially leading to forged signatures and compromising the integrity and authenticity of documents undergoing the signing proc resources during request processing.
CVE-2017-20238	Hirschmann Industrial HiVision versions 06.0.00 and 07.0.00 prior to 06.0.06 and 07.0.01 contains an improper authorization vulnerability that allows read-only use Attackers can exploit alternative interfaces such as the web interface or SNMP browser to modify device configurations despite having restricted permissions.
CVE-2024-40858	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.1. An app may be able to access Contacts without user cons
CVE-2026-35444	SDL_image is a library to load images of various formats as SDL surfaces. In do_layer_surface() in src/IMG_xcf.c, pixel index values from decoded XCF tile data are (cm_num). A crafted .xcf file with a small colormap and out-of-range pixel indices causes heap out-of-bounds reads of up to 762 bytes past the colormap allocation bytes are written into the output surface pixel data, making them potentially observable in the rendered image. This vulnerability is fixed with commit 996bf12888
CVE-2026-35412	Directus is a real-time API and App dashboard for managing SQL database content. Prior to 11.16.1, Directus' TUS resumable upload endpoint (/files/tus) allows any files by UUID. The TUS controller performs only collection-level authorization checks, verifying the user has some permission on directus_files, but never validates i rules (e.g., "users can only update their own files") are completely bypassed via the TUS path while being correctly enforced on the standard REST upload path. Th
CVE-2026-35170	openFPGALoader is a utility for programming FPGAs. In 1.1.1 and earlier, a heap-buffer-overflow read vulnerability exists in BitParser::parseHeader() that allows ou required to trigger this vulnerability.
CVE-2026-34379	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. From 3.2.0 to be LossyDctDecoder_execute() in src/lib/OpenEXRCore/internal_dwa_decoder.h:749. When decoding a DWA or DWAB-compressed EXR file containing a FLOAT-type ch unaligned uint8_t * row pointer to float * and writing through it. Because the row buffer may not be 4-byte aligned, this constitutes undefined behavior under the C RISC-V, etc.). On x86 it is silently tolerated at runtime but remains exploitable via compiler optimizations that assume aligned access. This vulnerability is fixed in 3
CVE-2026-35183	Brave CMS is an open-source CMS. Prior to 2.0.6, an Insecure Direct Object Reference (IDOR) vulnerability exists in the article image deletion feature. It is located i method. The endpoint accepts a filename from the URL but does not verify ownership. This allows an authenticated user with edit permissions to delete images att
CVE-2026-34604	Tina is a headless content management system. Prior to version 2.2.2, @tinacms/graphql uses string-based path containment checks in FilesystemBridge. That blo symlink/junction already exists under the allowed content root, a path like content/posts/pivot/owned.md is still considered "inside" the base even though the real and glob() can operate on files outside the intended root. This issue has been patched in version 2.2.2.
CVE-2026-34828	listmonk is a standalone, self-hosted, newsletter and mailing list manager. From version 4.1.0 to before version 6.1.0, a session management vulnerability allows p security changes, specifically password reset and password change. As a result, an attacker who has already obtained a valid session cookie can retain access to t account recovery and session security guarantees. This issue has been patched in version 6.1.0.
CVE-2019-25663	SuiteCRM 7.10.7 contains a SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the parer parentTab values using boolean-based SQL injection techniques to extract sensitive database information.
CVE-2019-25664	SuiteCRM 7.10.7 contains a time-based SQL injection vulnerability in the record parameter of the Users module DetailView action that allows authenticated attacke parameter in GET requests to the index.php endpoint to extract sensitive database information through time-based blind SQL injection techniques.
CVE-2025-54601	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor amd Wearable Processor Exynos 980, 850, 1080, 1280, 1330, 1380, 1480, 1580, W920, W An attacker can trigger a race condition by invoking an ioctl function concurrently from multiple threads.
CVE-2025-54602	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 1330, 1380, 1480, 1580, W920, W free. An attacker can trigger a race condition by invoking an ioctl function concurrently from multiple threads.
CVE-2026-34770	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to versions 38.8.6, 39.8.1, 40.8.0, and 41.0.0-beta.8, the native PowerMonitor object is garbage-collected, the associated OS-level resources (a message window on Windows, a shutdown handler on macOS) retain dar (macOS) dereferences freed memory, which may lead to a crash or memory corruption. All apps that access powerMonitor events (suspend, resume, lock-screen, e has been patched in versions 38.8.6, 39.8.1, 40.8.0, and 41.0.0-beta.8.
CVE-2026-34530	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Prior to version 2.62.2, the SPA admin-controlled branding fields. An admin who sets branding.name to a malicious payload injects persistent JavaScript that executes for ALL visitors, including un
CVE-2026-33691	The OWASP core rule set (CRS) is a set of generic attack detection rules for use with compatible web application firewalls. Prior to versions 3.3.9 and 4.25.0, a bypa (.php, .phar, .jsp, .jspx) by inserting whitespace padding in the filename (e.g. photo. php or shell.jsp). The affected rules do not normalize whitespace before evalu been patched in versions 3.3.9 and 4.25.0.
CVE-2026-31067	A remote command execution (RCE) vulnerability in the /goform/formReleaseConnect component of UTT Aggressive 520W v3v1.7.7-180627 allows attackers to exe

CVE-2026-34775	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to versions 38.8.6, 39.8.4, 40.8.4, and 41.0.0, the noc certain process-sharing scenarios, workers spawned in frames configured with nodeIntegrationInWorker: false could still receive Node.js integration. Apps are only nodeIntegrationInWorker are not affected. This issue has been patched in versions 38.8.6, 39.8.4, 40.8.4, and 41.0.0.
CVE-2026-30603	An issue in the firmware update mechanism of Qianniao QN-L23PA0904 v20250721.1640 allows attackers to gain root access, install backdoors, and exfiltrate data
CVE-2026-35586	pyLoad is a free and open-source download manager written in Python. Prior to 0.5.0b3.dev97, the ADMIN_ONLY_CORE_OPTIONS authorization set in set_config_va option names are ssl_certfile and ssl_keyfile. This name mismatch causes the admin-only check to always evaluate to False, allowing any user with SETTINGS perm option was never added to the admin-only set at all. This vulnerability is fixed in 0.5.0b3.dev97.
CVE-2025-64340	FastMCP is the standard framework for building MCP applications. Prior to version 3.2.0, server names containing shell metacharacters (e.g., &) can cause comman gemini-cli. These install paths use subprocess.run() with a list argument, but on Windows the target CLIs often resolve to .cmd wrappers that are executed through has been patched in version 3.2.0.
CVE-2026-34871	An issue was discovered in Mbed TLS before 3.6.6 and 4.x before 4.1.0 and TF-PSA-Crypto before 1.1.0. There is a Predictable Seed in a Pseudo-Random Number G
CVE-2026-35197	dye is a portable and respectful color library for shell scripts. Prior to 1.1.1, certain dye template expressions would result in execution of arbitrary code. This issue vulnerability is fixed in 1.1.1.
CVE-2026-39366	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the PayPal IPN v1 handler at plugin/PayPalYPT/ipn.php lacks transaction deduplication, their wallet balance and renew subscriptions. The newer ipnV2.php and webhook.php handlers correctly deduplicate via PayPalYPT_log entries, but the v1 handler
CVE-2026-39368	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the Live restream log callback flow accepted an attacker-controlled restreamerURL and streamers. The vulnerable flow allowed a low-privilege user with streaming permission to store an arbitrary callback URL and trigger server-side requests to loopba
CVE-2026-3571	The Pie Register – User Registration, Profiles & Content Restriction plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capabil makes it possible for unauthenticated attackers to change registration form status.
CVE-2026-34978	OpenPrinting CUPS is an open source printing system for Linux and other Unix-like operating systems. In versions 2.4.16 and prior, the RSS notifier allows .. path tr RSS XML bytes outside CacheDir/rss (anywhere that is lp-writable). In particular, because CacheDir is group-writable by default (typically root:lp and mode 0770), t rename(). This PoC clobbers CacheDir/job.cache with RSS XML, and after restarting cupsd the scheduler fails to parse the job cache and previously queued jobs dis
CVE-2026-5283	Inappropriate implementation in ANGLE in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Ch
CVE-2026-35559	Out-of-bounds write in the query processing components in Amazon Athena ODBC driver before 2.1.0.0 might allow a threat actor to crash the driver by using spec remediate this issue, users should upgrade to version 2.1.0.0.
CVE-2026-39354	Scoold is a Q&A and a knowledge sharing platform for teams. Prior to 1.66.2, an authenticated authorization flaw in Scoold allows any logged-in, low-privilege user the postId parameter to POST /questions/ask. Because question IDs are exposed in normal question URLs, a low-privilege attacker can take a victim question ID fro question object. This causes direct integrity loss of user-generated content and corrupts the integrity of the existing discussion thread. This vulnerability is fixed in
CVE-2026-34787	Emlog is an open source website building system. In versions 2.6.2 and prior, a Local File Inclusion (LFI) vulnerability exists in admin/plugin.php at line 80. The $plu proper sanitization. If the CSRF token check can be bypassed (see potential bypass conditions), an attacker can include arbitrary PHP files from the server filesyste patches.
CVE-2026-34889	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force Ultimate Addons for WPBakery Page Builder a from n/a before 3.21.4.
CVE-2026-39374	Plane is an an open-source project management tool. Prior to 1.3.0, the IssueBulkUpdateDateEndpoint allows a project member (ADMIN or MEMBER) to modify the workspace or project membership. The endpoint fetches issues by ID without filtering by workspace or project, enabling cross-boundary data modification. This vul
CVE-2026-34788	Emlog is an open source website building system. In versions 2.6.2 and prior, a SQL injection vulnerability exists in include/model/tag_model.php at line 168. The u without using parameterized queries or proper escaping ($this->db->escape_string()), making it vulnerable to SQL injection attacks. At time of publication, there a
CVE-2026-34779	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to versions 38.8.6, 39.8.1, 40.8.0, and 41.0.0-beta.8, not properly handle certain characters in the application bundle path. Under specific conditions, a crafted launch path could lead to arbitrary AppleScript execution they call app.moveToApplicationsFolder(). Apps that do not use this API are not affected. This issue has been patched in versions 38.8.6, 39.8.1, 40.8.0, and 41.0.0
CVE-2026-34939	PraisonAI is a multi-agent teams system. Prior to version 4.5.90, MCPToolIndex.search_tools() compiles a caller-supplied string directly as a Python regular expressi backtracking in the re engine, blocking the Python thread for hundreds of seconds and causing a complete service outage. This issue has been patched in version 4
CVE-2026-5291	Inappropriate implementation in WebGL in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to obtain potentially sensitive information from proce
CVE-2026-5276	Insufficient policy enforcement in WebUSB in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to obtain potentially sensitive information from pro
CVE-2026-34378	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. From 3.4.0 to be allows an attacker to trigger a signed integer overflow in generic_unpack(). By setting dataWindow.min.x to a large negative value, OpenEXRCore computes an enc overflows, causing the process to terminate with SIGILL via UBSan. This vulnerability is fixed in 3.4.9.
CVE-	Kedro-Datasets is a Kendo plugin providing data connectors. Prior to 9.3.0, PartitionedDataset in kedro-datasets was vulnerable to path traversal. Partition IDs were

2026-35492	malicious input containing .. components in a partition ID could cause files to be written outside the configured dataset directory, potentially overwriting arbitrary f filesystem, S3, GCS, etc.) are affected. This vulnerability is fixed in 9.3.0.
CVE-2026-34890	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mark O'Donnell MSTW League Manager allows DOM-Based XSS
CVE-2026-34832	Scoold is a Q&A and a knowledge sharing platform for teams. Prior to version 1.66.1, Scoold contains an authenticated authorization flaw in feedback deletion that submitting its ID to POST /feedback/{id}/delete. The handler enforces authentication but does not enforce object ownership (or moderator/admin authorization) be victim account's feedback item, and the item immediately disappeared from the feedback listing/detail views. This issue has been patched in version 1.66.1.
CVE-2026-34531	Flask-HTTPAuth provides Basic, Digest and Token HTTP authentication for Flask routes. Prior to version 4.8.1, in a situation where the client makes a request to a t HTTPAuth would invoke the application's token verification callback function with the token argument set to an empty string. If the application had any users in its the client request against any of those users. This issue has been patched in version 4.8.1.
CVE-2026-33033	An issue was discovered in 6.0 before 6.0.4, 5.2 before 5.2.13, and 4.2 before 4.2.30. `MultiPartParser` allows remote attackers to degrade performance by submit whitespace. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Seokchan
CVE-2025-36375	IBM DataPower Gateway 10.6CD 10.6.1.0 through 10.6.5.0 and IBM DataPower Gateway 10.5.0 10.5.0.0 through 10.5.0.20 and IBM DataPower Gateway 10.6.0 10. forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.
CVE-2026-4079	The SQL Chart Builder WordPress plugin before 2.3.8 does not properly escape user input as it is concatened to SQL queries, making it possible for attackers to cor
CVE-2026-1900	The Link Whisper Free WordPress plugin before 0.9.1 has a publicly accessible REST endpoint that allows unauthenticated settings updates.
CVE-2026-20431	In Modem, there is a possible system crash due to a logic error. This could lead to remote denial of service, if a UE has connected to a rogue base station controlle not needed for exploitation. Patch ID: MOLY01106496; Issue ID: MSV-4467.
CVE-2026-35441	Directus is a real-time API and App dashboard for managing SQL database content. Prior to 11.17.0, Directus' GraphQL endpoints (/graphql and /graphql/system) di could exploit GraphQL aliasing to repeat an expensive relational query many times in a single request, forcing the server to execute a large number of independen number of aliases. The existing token limit on GraphQL queries still permitted enough aliases for significant resource exhaustion, while the relational depth limit ap default, meaning no built-in throttle prevented this from causing CPU, memory, and I/O exhaustion that could degrade or crash the service. Any authenticated user vulnerability is fixed in 11.17.0.
CVE-2026-34124	A denial-of-service vulnerability was identified in TP-Link Tapo C520WS v2.6 within the HTTP request path parsing logic. The implementation enforces length restric during normalization. An attacker on the adjacent network may send a crafted HTTP request to cause buffer overflow and memory corruption, leading to system in
CVE-2026-34122	A stack-based buffer overflow vulnerability was identified in TP-Link Tapo C520WS v2.6 within a configuration handling component due to insufficient input validati a vulnerable configuration parameter, resulting in a stack overflow. Successful exploitation results in Denial-of-Service (DoS) condition, leading to a service crash o
CVE-2026-34120	A heap-based buffer overflow vulnerability was identified in TP-Link Tapo C520WS v2.6 within the asynchronous parsing of local video stream content due to insuffi inputs.An attacker on the same network segment could trigger heap memory corruption conditions by sending crafted payloads that cause write operations beyon condition, causing the device's process to crash or become unresponsive.
CVE-2026-35383	Bentley Systems iTwin Platform exposed a Cesium ion access token in the source of some web pages. An unauthenticated attacker could use this token to enumer web pages and cannot be used to enumerate or delete assets.
CVE-2026-34119	A heap-based buffer overflow vulnerability was identified in TP-Link Tapo C520WS v2.6 within the HTTP parsing loop when appending segmented request bodies wi when handling externally supplied HTTP input. An attacker on the same network segment could trigger heap memory corruption conditions by sending crafted pay exploitation causes a Denial-of-Service (DoS) condition, causing the device's process to crash or become unresponsive.
CVE-2026-34118	A heap-based buffer overflow vulnerability was identified in TP-Link Tapo C520WS v2.6 in the HTTP POST body parsing logic due to missing validation of remaining handling externally supplied HTTP input. An attacker on the same network segment could trigger heap memory corruption conditions by sending crafted payloads exploitation causes a Denial-of-Service (DoS) condition, causing the device's process to crash or become unresponsive.
CVE-2026-5330	A vulnerability was found in SourceCodester/mayuri_k Best Courier Management System 1.0. Affected by this issue is some unknown functionality of the file /ajax.p manipulation of the argument ID results in improper access controls. The attack may be initiated remotely. The exploit has been made public and could be used.
CVE-2026-34897	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Lingren Media LIbrary Assistant allows Stored XSS.This is
CVE-2026-35038	Signal K Server is a server application that runs on a central hub in a boat. Prior to version 2.24.0, there is an arbitrary prototype read vulnerability via `from` field prototype boundary filtering to extract internal functions and properties from the global prototype object this violates data isolation and lets a user read more than
CVE-2025-47374	Memory Corruption when accessing freed memory due to concurrent fence deregistration and signal handling.
CVE-2026-35173	Chyrp Lite is an ultra-lightweight blogging engine. Prior to 2026.01, an IDOR / Mass Assignment issue exists in the Post model that allows authenticated users with posts they do not own and do not have permission to edit. By passing internal class properties such as id into the post_attributes payload, an attacker can alter the post rather than the attacker's own post, effectively enabling post takeover. This vulnerability is fixed in 2026.01.
CVE-2026-	Glances is an open-source system cross-platform monitoring tool. Prior to version 4.5.3, the Glances XML-RPC server (activated with glances -s or glances --server) handler does not validate the Content-Type header, an attacker-controlled webpage can issue a CORS "simple request" (POST with Content-Type: text/plain) contai

33533	check, the server processes the XML body and returns the full system monitoring dataset, and the wildcard CORS header lets the attacker's JavaScript read the res CPU/memory/disk/network stats, and the full process list including command lines (which often contain tokens, passwords, or internal paths). This issue has been p
CVE-2026-34756	vLLM is an inference and serving engine for large language models (LLMs). From 0.1.0 to before 0.19.0, a Denial of Service vulnerability exists in the vLLM OpenAI- parameter in the ChatCompletionRequest and CompletionRequest Pydantic models, an unauthenticated attacker can send a single HTTP request with an astronom immediate Out-Of-Memory crashes by allocating millions of request object copies in the heap before the request even reaches the scheduling queue. This vulnerab
CVE-2026-34755	vLLM is an inference and serving engine for large language models (LLMs). From 0.7.0 to before 0.19.0, the VideoMediaIO.load_base64() method at vllm/multimoda frames, but does not enforce a frame count limit. The num_frames parameter (default: 32), which is enforced by the load_bytes() code path, is completely bypasse thousands of comma-separated base64-encoded JPEG frames, causing the server to decode all frames into memory and crash with OOM. This vulnerability is fixed
CVE-2026-34750	Payload is a free and open source headless content management system. Prior to version 3.78.0 in @payloadcms/storage-azure, @payloadcms/storage-gcs, @payl endpoints for S3, GCS, Azure, and R2 did not properly sanitize filenames. An attacker could craft filenames to escape the intended storage location. This issue has @payloadcms/storage-gcs, @payloadcms/storage-r2, and @payloadcms/storage-s3.
CVE-2026-4668	The Booking for Appointments and Events Calendar - Amelia plugin for WordPress is vulnerable to SQL Injection via the `sort` parameter in the payments listing en the user-supplied `sort` parameter and lack of sufficient preparation on the existing SQL query in `PaymentRepository.php`, where the sort field is interpolated dir prepared statements do not protect ORDER BY column names. GET requests also skip Amelia's nonce validation entirely. This makes it possible for authenticated a additional SQL queries into already existing queries that can be used to extract sensitive information from the database via time-based blind SQL injection.
CVE-2026-20042	A vulnerability in the configuration backup feature of Cisco Nexus Dashboard could allow an attacker who has the encryption password and access to Full or Config authentication details are included in the encrypted backup files. An attacker with a valid backup file and encryption password from an affected device could decry file to access internal-only APIs on the affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating sy
CVE-2026-30522	A Business Logic vulnerability exists in SourceCodester Loan Management System v1.0 due to improper server-side validation. The application allows administrato frontend interface prevents users from entering negative numbers in the "Monthly Overdue Penalty" field, this constraint is not enforced on the backend. An authe request to submit a negative value for the penalty_rate.
CVE-2026-25834	Mbed TLS v3.3.0 up to 3.6.5 and 4.0.0 allows Algorithm Downgrade.
CVE-2026-2265	An unauthenticated remote code execution (RCE) vulnerability exists in applications that use the Replicator node package manager (npm) version 1.0.5 to deserial
CVE-2026-20097	A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with admin-level privileges to execute arbitrary supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A succ operating system as the root user. Cisco has assigned this vulnerability a SIR of High rather than Medium as the score indicates because additional security implica
CVE-2026-20096	A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with admin-level privileges to perform comman the root user. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted commands to the allow the attacker to execute arbitrary commands on the underlying operating system as the root user. Cisco has assigned this vulnerability a Security Impact Rati security implications could occur once the attacker has become root.
CVE-2026-20095	A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with admin-level privileges to perform comman the root user. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted commands to the allow the attacker to execute arbitrary commands on the underlying operating system as the root user. Cisco has assigned this vulnerability a Security Impact Rati security implications could occur once the attacker has become root.
CVE-2026-35549	An issue was discovered in MariaDB Server before 11.4.10, 11.5.x through 11.8.x before 11.8.6, and 12.x before 12.2.2. If the caching_sha2_password authenticati can crash the server because sha256_crypt_r uses alloca.
CVE-2026-5574	A security vulnerability has been detected in Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30. Affected is the function deletefile of the component FsBrowseClean. may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in a
CVE-2026-4927	Exposure of sensitive information in the users MFA feature in Devolutions Server allows users with user management privileges to obtain other users OTP keys via 2026.1.11.
CVE-2026-3309	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress plugin for WordPress is vulnerable to ar the plugin allowing user-supplied billing field values from the checkout process to be interpolated into shortcode template strings that are subsequently processed unauthenticated attackers to execute arbitrary shortcodes by submitting crafted billing field values during the checkout process.
CVE-2026-35000	ChangeDetection.io versions prior to 0.54.7 contain a protection bypass vulnerability in the SafeXPath3Parser implementation that allows attackers to read arbitrar file-access primitives. Attackers can exploit the incomplete blocklist of dangerous XPath functions to access sensitive data from the local filesystem.
CVE-2026-30523	A Business Logic vulnerability exists in SourceCodester Loan Management System v1.0 due to the lack of proper input validation. The application allows administra However, the backend fails to validate that the duration must be a positive integer. An attacker can submit a negative value for the months parameter. The system
CVE-2026-0552	The Simple Shopping Cart plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpsc_display_product' shortcode in all versions up to, a supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will exe
CVE-2026-33727	Pi-hole is a Linux network-level advertisement and Internet tracker blocking application. Version 6.4 has a local privilege-escalation vulnerability allows code execu account uses nologin, so this is not a direct interactive-login issue. However, nologin does not prevent code from running as UID pihole if a Pi-hole component is co /etc/pihole/versions is sourced by root-run Pi-hole scripts, leading to root code execution. This vulnerability is fixed in 6.4.1.
CVE-2026-0738	The WP Shortcodes Plugin - Shortcodes Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the su_carousel shortcode in all versions up to in the 'su_slide_link' attachment meta field. This makes it possible for authenticated attackers, with author level access and above, to inject arbitrary web scripts in
CVE-2026-	The Royal Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'button_text' parameter in all versions up to, and including

0664	possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses ar
CVE-2025-13368	The Xpro Addons — 140+ Widgets for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Pricing Widget's 'onClick Event' setting in output escaping. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execu
CVE-2026-0737	The WP Shortcodes Plugin - Shortcodes Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 7.4.7. This is d su_lightbox shortcode. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will
CVE-2025-15064	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to Stored C 2.11.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber level access and above, to inje injected page. The vulnerability is only exploitable when "HTML support for user description" is enabled in Ultimate Member settings.
CVE-2018-25249	MyBB My Arcade Plugin 1.3 contains a persistent cross-site scripting vulnerability that allows authenticated users to inject malicious scripts through arcade game s comment field that execute when other users view or edit the comment.
CVE-2026-2437	The WP Travel Engine – Tour Booking Plugin – Tour Operator Software plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wte_trip_tax sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor level access and above, to inject a page.
CVE-2026-2924	The Gutenverse – Ultimate WordPress FSE Blocks Addons & Ecosystem plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'imageLoad' param output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execu
CVE-2026-0626	The WPFunnels – Easy Funnel Builder To Optimize Buyer Journeys And Get More Leads & Sales plugin for WordPress is vulnerable to Stored Cross-Site Scripting via insufficient input sanitization and output escaping of the 'button_icon' parameter. This makes it possible for authenticated attackers, with contributor level access a accesses an injected page.
CVE-2026-5590	A race condition during TCP connection teardown can cause tcp_recv() to operate on a connection that has already been released. If tcp_conn_search() returns NUL passed to tcp_backlog_is_full() and dereferenced without validation, leading to a crash.
CVE-2026-5372	An issue that allowed a SQL injection attack vector related to saved queries (introduced in version 4.0.260123.0). This is an instance of CWE-89: Improper Neutraliz estimated CVSS score of CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H (6.4 Medium). This issue was fixed in version 4.0.260123.1 of the runZero Platform.
CVE-2026-2600	The ElementsKit Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ekit_tab_title' parameter in the Simple sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject a page.
CVE-2026-2949	The Xpro Addons — 140+ Widgets for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Icon Box widget in versions up to, and inc possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses ar
CVE-2026-34809	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark parameter to /cgi-bin/zonefw.cgi. An authenticated attacker can injec page.
CVE-2026-35057	XenForo before 2.3.10 and before 2.2.19 is vulnerable to stored cross-site scripting (XSS) in structured text mentions, primarily affecting legacy profile post conten executed when other users view the content.
CVE-2026-34812	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the mimetypes parameter to /cgi-bin/proxypolicy.cgi. An authenticated attacker c affected page.
CVE-2026-34811	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark parameter to /cgi-bin/xtaccess.cgi. An authenticated attacker can inje page.
CVE-2026-34810	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark parameter to /cgi-bin/vpnfw.cgi. An authenticated attacker can inject page.
CVE-2026-34808	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark parameter to /cgi-bin/outgoingfw.cgi. An authenticated attacker can i affected page.
CVE-2026-34807	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark parameter to /cgi-bin/incoming.cgi. An authenticated attacker can inj page.
CVE-2026-34806	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark parameter to /cgi-bin/snat.cgi. An authenticated attacker can inject a page.
CVE-2026-34805	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark parameter to /cgi-bin/dnat.cgi. An authenticated attacker can inject a page.
CVE-2026-34804	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the dscp parameter to /manage/qos/rules/. An authenticated attacker can inject a page.
CVE-2026-	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the name parameter to /manage/qos/classes/. An authenticated attacker can inje page.

34803	
CVE-2026-34802	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark user ham spam parameter to /cgi-bin/salearn.cgi. An authenticated at view the affected page.
CVE-2026-25601	A vulnerability was identified in MEPIS RM, an industrial software product developed by Metronik. The application contained a hardcoded cryptographic key within t passwords was enabled, this key was used to encrypt user passwords before storing them in the application’s database. An attacker with sufficient privileges to ac embedded key, and gain unauthorized access to the associated ICS/OT environment.
CVE-2026-34800	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the NAME parameter to /cgi-bin/uplinkeditor.cgi. An authenticated attacker can in affected page.
CVE-2025-13535	The King Addons for Elementor plugin for WordPress is vulnerable to multiple Contributor+ DOM-Based Stored Cross-Site Scripting vulnerabilities in all versions up escaping across multiple widgets and features. The plugin uses esc_attr() and esc_url() within JavaScript inline event handlers (onclick attributes), which allows HTM context. Additionally, several JavaScript files use unsafe DOM manipulation methods (template literals, .html(), and window.location.href with unvalidated URLs) wi Contributor-level access and above, to inject arbitrary web scripts via Elementor widget settings that execute when a user accesses the injected page or when an a patched in version 5.1.51.
CVE-2026-34799	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark parameter to /manage/dnsmasq/hosts/. An authenticated attacker ca affected page.
CVE-2026-34798	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark parameter to /cgi-bin/routing.cgi. An authenticated attacker can injec page.
CVE-2026-35507	Shynet before 0.14.0 allows Host header injection in the password reset flow.
CVE-2026-0688	The Webmention plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.6.2 via the 'Tools::read' function. This ma make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.
CVE-2026-34813	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the user parameter to /cgi-bin/proxyuser.cgi. An authenticated attacker can injec page.
CVE-2026-34801	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark parameter to /manage/dhcp/fixed_leases/. An authenticated attacker affected page.
CVE-2026-34820	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark parameter to /manage/ipsec/. An authenticated attacker can inject ar page.
CVE-2026-34823	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark parameter to /manage/password/web/. An authenticated attacker car affected page.
CVE-2026-34822	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the new_cert_name parameter to /manage/ca/certificate/. An authenticated attac the affected page.
CVE-2026-34821	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark parameter to /manage/vpnauthentication/user/. An authenticated atta the affected page.
CVE-2026-34819	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the REMARK parameter to /cgi-bin/openvpnclient.cgi. An authenticated attacker c affected page.
CVE-2026-34818	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the remark parameter to /manage/dnsmasq/localdomains/. An authenticated atta the affected page.
CVE-2026-34817	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the ADDRESS BCC parameter to /cgi-bin/smtprouting.cgi. An authenticated attacl the affected page.
CVE-2026-34816	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the domain parameter to /manage/smtpscan/domainrouting/. An authenticated a view the affected page.
CVE-2026-35054	XenForo before 2.3.9 is vulnerable to stored cross-site scripting (XSS) related to BB code rendering. An attacker can inject malicious scripts through BB code that a
CVE-2026-34815	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the DOMAIN parameter to /cgi-bin/smtpdomains.cgi. An authenticated attacker ca affected page.
CVE-2026-34814	Endian Firewall version 3.3.25 and prior allow stored cross-site scripting (XSS) via the group parameter to /cgi-bin/proxygroup.cgi. An authenticated attacker can in affected page.

CVE-2026-5563	A security flaw has been discovered in AutohomeCorp frostmourne up to 1.0. Affected is the function httpTest of the file /api/monitor-api/alarm/previewData of the launched remotely. The exploit has been released to the public and may be used for attacks.
CVE-2026-5344	A security vulnerability has been detected in Textpattern up to 4.9.1. Affected by this vulnerability is the function mt_uploadImage of the file rpc/TXP_RPCServer.ph leads to path traversal. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor confirmed the issue and
CVE-2026-5556	A security vulnerability has been detected in badlogic pi-mono up to 0.58.4. This vulnerability affects the function discoverAndLoadExtensions of the file packages/ Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but d
CVE-2026-5561	A vulnerability was determined in Campcodes Complete POS Management and Inventory System up to 4.0.6. This affects an unknown function of the file app/Http/ Executing a manipulation can lead to injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.
CVE-2026-5681	A flaw has been found in itsourcecode sanitize or validate this input 1.0. This impacts an unknown function of the file /borrowedequip.php of the component Param attack is possible to be carried out remotely. The exploit has been published and may be used.
CVE-2026-5560	A vulnerability was found in PHPGurukul Online Shopping Portal Project 2.1. The impacted element is an unknown function of the file /payment-method.php of the c results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.
CVE-2026-5578	A vulnerability was found in CodeAstro Online Classroom 1.0. This vulnerability affects unknown code of the file /OnlineClassroom/addassessment.php of the compo in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.
CVE-2026-5579	A vulnerability was determined in CodeAstro Online Classroom 1.0. This issue affects some unknown processing of the file /OnlineClassroom/updatedetailsfromfacu the argument fname can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.
CVE-2026-5559	A vulnerability has been found in AntaresMugisho PyBlade 0.1.8-alpha/0.1.9-alpha. The affected element is the function _is_safe_ast of the file sandbox.py of the co elements used in a template engine. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The project was inf
CVE-2026-5558	A flaw has been found in PHPGurukul PHPGurukul Online Shopping Portal Project up to 2.1. Impacted is an unknown function of the file /pending-orders.php of the c injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.
CVE-2026-5580	A vulnerability was identified in CodeAstro Online Classroom 1.0. Impacted is an unknown function of the file /OnlineClassroom/addvideos.php of the component Pa is possible to initiate the attack remotely. The exploit is publicly available and might be used.
CVE-2026-5557	A vulnerability was detected in badlogic pi-mono up to 0.58.4. This issue affects some unknown processing of the file packages/mom/src/slack.ts of the component channel. The attack can be executed remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respor
CVE-2026-5641	A vulnerability was found in PHPGurukul Online Shopping Portal Project 2.1. The impacted element is an unknown function of the file /admin/update-image1.php of in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.
CVE-2026-5553	A vulnerability was identified in itsourcecode Online Cellphone System 1.0. Affected by this vulnerability is an unknown functionality of the file /cp/available.php of sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.
CVE-2026-5552	A weakness has been identified in PHPGurukul Online Shopping Portal Project 2.1. This issue affects some unknown processing of the file /sub-category.php of the c injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.
CVE-2026-5547	A vulnerability has been found in Tenda AC10 16.03.10.10_multi_TDE01. Affected is the function formAddMacfilterRule of the file /bin/httpd. Such manipulation lead endpoints might be affected.
CVE-2026-5586	A vulnerability was determined in zhongyu09 openchatbi up to 0.2.1. The impacted element is an unknown function of the component Multi-stage Text2SQL Workfl attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not re
CVE-2026-5546	A flaw has been found in Campcodes Complete Online Learning Management System 1.0. This impacts the function add_lesson of the file /application/models/Crud_ attack remotely. The exploit has been published and may be used.
CVE-2026-5543	A vulnerability was identified in PHPGurukul User Registration & Login and User Management System 3.3. The affected element is an unknown function of the file /a injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.
CVE-2026-5719	A flaw has been found in itsourcecode Construction Management System 1.0. This affects an unknown function of the file /borrowedtool.php. Executing a manipula remotely. The exploit has been published and may be used.
CVE-2026-5538	A vulnerability was detected in QingdaoU OnlineJudge up to 1.6.1. Affected by this issue is the function service_url of the file JudgeServer.service_url of the compor forgery. It is possible to launch the attack remotely. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-5537	A security vulnerability has been detected in halex CourseSEL up to 1.1.0. Affected by this vulnerability is the function check_sel of the file Apps/Index/Controller/In manipulation of the argument seid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The

CVE-2026-5317	A security flaw has been discovered in Nothings stb up to 1.22. This affects the function start_decoder of the file stb_vorbis.c. The manipulation results in out-of-bo to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-5532	A vulnerability was found in ScrapeGraphAI scrapegraph-ai up to 1.74.0. The affected element is the function create_sandbox_and_execute of the file scrapegrapha The manipulation results in os command injection. The attack may be launched remotely. The exploit has been made public and could be used. The vendor was co
CVE-2026-5530	A flaw has been found in Ollama up to 18.1. This issue affects some unknown processing of the file server/download.go of the component Model Pull API. Executing remotely. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-5583	A security vulnerability has been detected in PHPGurukul Online Shopping Portal Project 2.1. This affects an unknown part of the file /my-profile.php of the compon injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.
CVE-2026-5352	A security vulnerability has been detected in Trendnet TEW-657BRM 1.00.1. This impacts the function Edit of the file /setup.cgi. Such manipulation of the argument exploit has been disclosed publicly and may be used. The vendor confirms, that "[t]he product in question (...) has been discontinued and end of life since June 23, so we are not able to confirm the vulnerabilities. We will make an announcement on our website's product support page and notify customers who registered their by the maintainer.
CVE-2026-5587	A vulnerability was identified in wbbeyourself MAC-SQL up to 31a9df5e0d520be4769be57a4b9022e5e34a14f4. This affects the function _execute_sql of the file cor Remote exploitation of the attack is possible. The exploit is publicly available and might be used. This product follows a rolling release approach for continuous deli was contacted early about this disclosure but did not respond in any way.
CVE-2025-66483	IBM Aspera Shares 1.9.9 through 1.11.0 does not invalidate session after a password reset which could allow an authenticated user to impersonate another user or
CVE-2026-5639	A flaw has been found in PHPGurukul Online Shopping Portal Project 2.1. Impacted is an unknown function of the file /admin/update-image3.php of the component injection. The attack can be executed remotely. The exploit has been published and may be used.
CVE-2026-5636	A weakness has been identified in PHPGurukul Online Shopping Portal Project 2.1. This affects an unknown part of the file /cancelorder.php of the component Parar may be initiated remotely. The exploit has been made available to the public and could be used for attacks.
CVE-2026-5635	A security flaw has been discovered in PHPGurukul Online Shopping Portal Project 2.1. Affected by this issue is some unknown functionality of the file /categorywise argument cid results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.
CVE-2026-5649	A vulnerability has been found in code-projects Online Application System for Admission 1.0. This issue affects some unknown processing of the file /enrollment/adı attack can be executed remotely. The exploit has been disclosed to the public and may be used.
CVE-2026-5659	A vulnerability was found in pytries datrie up to 0.8.3. The affected element is the function Trie.load/Trie.read/Trie.__setstate__ of the file src/datrie.pyx of the comp launched remotely. 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 respor
CVE-2026-5474	A vulnerability was found in NASA cFS up to 7.0.0. This affects the function CFE_MSG_GetSize of the file apps/to_lab/fsw/src/to_lab_passthru_encode.c of the compo buffer overflow. The attacker must have access to the local network to execute the attack. The project was informed of the problem early through an issue report b
CVE-2026-5660	A vulnerability was determined in itsourcecode Construction Management System 1.0. The impacted element is an unknown function of the file /borrowed_equip.ph causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.
CVE-2026-5623	A vulnerability was identified in hcengineering Huly Platform 0.7.382. This affects an unknown part of the file server/front/src/index.ts of the component Import Enc 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.
CVE-2026-5620	A vulnerability has been found in itsourcecode Construction Management System 1.0. Affected is an unknown function of the file /borrowed_equip_report.php of the injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2026-5670	A vulnerability was found in Cyber-III Student-Management-System up to 1a938fa61e9f735078e9b291d2e6215b4942af3f. This issue affects the function move_upl manipulation of the argument File results in unrestricted upload. The attack can be initiated remotely. The exploit has been made public and could be used. Contin of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.
CVE-2025-43210	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in iOS 18.6 and iPadOS 18.6, iPadOS 17.7.9, macOS Sequoia 15.6 11.6. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.
CVE-2026-5607	A security vulnerability has been detected in imprvhub mcp-browser-agent up to 0.8.0. This impacts the function CallToolRequestSchema of the file src/handlers.ts request.params.name/request.params.arguments leads to server-side request forgery. The attack is possible to be carried out remotely. The exploit has been discl but did not respond in any way.
CVE-2026-5594	A weakness has been identified in premAI-io premsql up to 0.2.1. Affected is the function eval of the file premsql/agents/baseline/workers/followup.py. This manipu out 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 re
CVE-2026-5606	A security flaw has been discovered in PHPGurukul Online Shopping Portal Project 2.1. The affected element is an unknown function of the file /order-details.php of in sql injection. It is possible to launch the attack remotely.
CVE-2026-5355	A vulnerability has been found in Trendnet TEW-657BRM 1.00.1. Affected by this issue is the function vpn_drop of the file /setup.cgi. The manipulation of the argum out remotely. The exploit has been disclosed to the public and may be used. The vendor confirms, that "[t]he product in question (...) has been discontinued and e support for this product, so we are not able to confirm the vulnerabilities. We will make an announcement on our website's product support page and notify custom

	are no longer supported by the maintainer.
CVE-2026-5597	A flaw has been found in griptape-ai griptape 0.19.4. This affects an unknown part of the file griptape\tools\computer\tool.py of the component ComputerTool. Exec possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond
CVE-2026-5596	A vulnerability was detected in griptape-ai griptape 0.19.4. Affected by this issue is some unknown functionality of the file griptape/tools/sql/tool.py of the compone the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-5354	A flaw has been found in Trendnet TEW-657BRM 1.00.1. Affected by this vulnerability is the function vpn_connect of the file /setup.cgi. Executing a manipulation of executed remotely. The exploit has been published and may be used. The vendor confirms, that "[t]he product in question (...) has been discontinued and end of li for this product, so we are not able to confirm the vulnerabilities. We will make an announcement on our website's product support page and notify customers who longer supported by the maintainer.
CVE-2026-5353	A vulnerability was detected in Trendnet TEW-657BRM 1.00.1. Affected is the function ping_test of the file /setup.cgi. Performing a manipulation of the argument c The exploit is now public and may be used. The vendor confirms, that "[t]he product in question (...) has been discontinued and end of life since June 23, 2011, tha not able to confirm the vulnerabilities. We will make an announcement on our website's product support page and notify customers who registered their products maintainer.
CVE-2026-5675	A vulnerability was found in itsourcecode Construction Management System 1.0. This affects an unknown part of the file /borrowed_tool.php of the component Para possible to launch the attack remotely. The exploit has been made public and could be used.
CVE-2026-5640	A vulnerability has been found in PHPGurukul Online Shopping Portal Project 2.1. The affected element is an unknown function of the file /admin/update-image2.ph leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.
CVE-2026-5328	A weakness has been identified in shsuishang modulithshop up to 829bac71f507e84684c782b9b062b8bf3b5585d6. The impacted element is the function listItem src/main/java/com/suisung/shopsuite/pt/service/impl/ProductIndexServiceImpl.java of the component ProductItemDao Interface. Executing a manipulation of the ar The exploit has been made available to the public and could be used for attacks. This product utilizes a rolling release system for continuous delivery, and as such, called 42bcb9463425d1be906c3b290cf29885eb5a2324. A patch should be applied to remediate this issue.
CVE-2026-5327	A security flaw has been discovered in efforthye fast-filesystem-mcp up to 3.5.1. The affected element is the function handleGetDiskUsage of the file src/index.ts. F carried out remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue rep
CVE-2026-5595	A security vulnerability has been detected in griptape-ai griptape 0.19.4. Affected by this vulnerability is the function load_files_from_disk/list_files_from_disk/save_ Such manipulation leads to path traversal. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The vendor was c
CVE-2026-5528	A security vulnerability has been detected in MoussaabBadla code-screenshot-mcp up to 0.1.0. This affects an unknown part of the component HTTP Interface. Suc 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.
CVE-2026-5351	A weakness has been identified in Trendnet TEW-657BRM 1.00.1. This affects the function add_wps_client of the file /setup.cgi. This manipulation of the argument The exploit has been made available to the public and could be used for attacks. The vendor confirms, that "[t]he product in question (...) has been discontinued ar provide support for this product, so we are not able to confirm the vulnerabilities. We will make an announcement on our website's product support page and notif products that are no longer supported by the maintainer.
CVE-2026-34397	Himmelblau is an interoperability suite for Microsoft Azure Entra ID and Intune. From versions 2.0.0-alpha to before 2.3.9 and 3.0.0-alpha to before 3.1.1, there is a Only authenticated himmelblau users whose mapped CN/short name exactly matches a privileged local group name (e.g., "sudo", "wheel", "docker", "adm") can ca system uses NSS results for group-based authorization decisions (sudo, polkit, etc.), this can grant the attacker the privileges of that group. This issue has been pa
CVE-2026-5248	A vulnerability has been found in gougucms 4.08.18. This affects the function reg_submit of the file gougucms-master\app\home\controller\Login.php of the compo dynamically-determined object attributes. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The vendor w
CVE-2026-5259	A vulnerability was determined in AutohomeCorp frostmourne up to 1.0. The affected element is an unknown function of the file frostmourne-monitor/src/main/java Alarm Preview. Executing a manipulation can lead to server-side request forgery. The attack may be performed from remote. The exploit has been publicly disclose
CVE-2026-5273	Use after free in CSS in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Ch
CVE-2026-5472	A flaw has been found in ProjectsAndPrograms School Management System up to 6b6fae5426044f89c08d0dd101c7fa71f9042a59. The affected element is an unkn Handler. This manipulation of the argument File causes unrestricted upload. Remote exploitation of the attack is possible. The exploit has been published and may version details for affected or updated releases are not provided.
CVE-2026-34371	LibreChat is a ChatGPT clone with additional features. Prior to 0.8.4, LibreChat trusts the name field returned by the execute_code sandbox when persisting code-g artifact filename containing traversal sequences (for example, ../../../../../app/client/dist/poc.txt) is concatenated into the server-side destination path and written w execute_code an arbitrary file write primitive as the LibreChat server user. This vulnerability is fixed in 0.8.4.
CVE-2026-5470	A security vulnerability has been detected in mixelpixx Google-Research-MCP 1e062d7bd887bfe5f6e582b6cc288bb897b35cf2/ca613b736ab787bc926932f59cddc6 src/services/content-extractor.service.ts of the component Model Context Protocol Handler. The manipulation of the argument URL leads to server-side request forg may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is n in any way.
CVE-2024-58342	XenForo before 2.2.17 and 2.3.1 allows open redirect via a specially crafted URL. The getDynamicRedirect() function does not adequately validate the redirect targ containing newlines, user credentials, or host mismatches.
CVE-2026-5251	A vulnerability was identified in z-9527 admin 1.0/2.0. This impacts an unknown function of the file /server/routes/user.js of the component User Update Endpoint. S determined object attributes. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early abou
CVE-2026-	A vulnerability was detected in Harvard University IQSS Dataverse up to 6.8. This affects an unknown function of the file /ThemeAndWidgets.xhtml of the compone results in unrestricted upload. Remote exploitation of the attack is possible. The exploit is now public and may be used. Upgrading to version 6.10 mitigates this iss

1879	responded in a very professional manner and quickly released a fixed version of the affected product.
CVE-2018-25240	Watchr 1.1.0.0 contains a denial of service vulnerability that allows local attackers to crash the application by submitting an excessively long string to the search fu trigger a search operation to cause the application to crash.
CVE-2018-25242	One Search 1.1.0.0 contains a denial of service vulnerability that allows local attackers to crash the application by submitting excessively long input strings to the s search bar to trigger an unhandled exception that crashes the application.
CVE-2018-25243	FastTube 1.0.1.0 contains a denial of service vulnerability that allows local attackers to crash the application by submitting an excessively long string to the search trigger a crash when the search operation is executed.
CVE-2019-25666	SpotAuditor 3.6.7 contains a local buffer overflow vulnerability in the Base64 Password Decoder component that allows attackers to crash the application. Attacker denial of service condition.
CVE-2018-25244	Eco Search 1.0.2.0 contains a denial of service vulnerability that allows local attackers to crash the application by submitting an excessively long string to the sear bar and trigger a crash by initiating a search operation.
CVE-2025-43238	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An ap
CVE-2018-25238	VSCO 1.1.1.0 contains a denial of service vulnerability that allows local attackers to crash the application by submitting an excessively long string through the sear and navigate back to trigger an application crash.
CVE-2019-25667	TaskInfo 8.2.0.280 contains a local buffer overflow vulnerability that allows attackers to crash the application by supplying oversized input to registration fields. Att Number textboxes in the Help menu's registration dialog to trigger a denial of service condition.
CVE-2018-25252	FTP Voyager 16.2.0 contains a denial of service vulnerability that allows local attackers to crash the application by injecting oversized buffer data into the site profi repeated characters and paste it into the IP field to trigger a buffer overflow that crashes the FTP Voyager process.
CVE-2018-25253	Termite 3.4 contains a buffer overflow vulnerability in the User interface language settings field that allows local attackers to cause a denial of service by supplying User interface language field to crash the application.
CVE-2019-25683	FileZilla 3.40.0 contains a denial of service vulnerability in the local search functionality that allows local attackers to crash the application by supplying a malforme 384 'A' characters followed by 'BBBB' and 'CCCC' sequences in the search directory field and initiating a local search operation.
CVE-2026-0049	In onHeaderDecoded of LocalImageResolver.java, there is a possible persistent denial of service due to resource exhaustion. This could lead to local denial of servi exploitation.
CVE-2018-25239	Smart VPN 1.1.3.0 contains a denial of service vulnerability that allows local attackers to crash the application by submitting oversized input through the search int trigger an unhandled exception that crashes the application.
CVE-2026-33817	Index out-of-range when encountering a branch page with zero elements in go.etcd.io/bbolt
CVE-2019-25665	River Past Ringtone Converter 2.7.6.1601 contains a local buffer overflow vulnerability that allows attackers to crash the application by supplying oversized input t Activation code textarea via the Help menu's Activate dialog to trigger a denial of service condition.
CVE-2019-25659	ASPRunner Professional 6.0.766 contains a local buffer overflow vulnerability that allows attackers to cause a denial of service by supplying an excessively long pro during project creation to trigger an application crash.
CVE-2026-35406	Aardvark-dns is an authoritative dns server for A/AAAA container records. From 1.16.0 to 1.17.0, a truncated TCP DNS query followed by a connection reset causes vulnerability is fixed in 1.17.1.
CVE-2025-13044	IBM Concert 1.0.0 through 2.2.0 creates temporary files with predictable names, which allows local users to overwrite arbitrary files via a symlink attack.
CVE-2026-31053	A double free vulnerability exists in librz/bin/format/le/le.c in the function le_load_fixup_record(). When processing malformed or circular LE fixup chains, relocation binary can trigger heap corruption and cause the application to crash, resulting in a denial-of-service condition. An attacker with a crafted binary could cause a der
CVE-2019-25677	WinRAR 5.61 contains a denial of service vulnerability that allows local attackers to crash the application by placing a malformed winrar.lng language file in the ins the test button, causing an access violation at memory address 004F1DB8 when the application attempts to read invalid data.
CVE-2025-71280	XenForo before 2.3.7 allows information disclosure via local account page caching on shared systems. On systems where multiple users share a browser or machin
CVE-2016-	NetSchedScan 1.0 contains a buffer overflow vulnerability in the scan Hostname/IP field that allows local attackers to crash the application by supplying an oversiz followed by 4 bytes of EIP overwrite into the Hostname/IP field to trigger a denial of service condition.

20050	
CVE-2019-25660	LanHelper 1.74 contains a local buffer overflow vulnerability that allows attackers to crash the application by sending excessively long input strings. Attackers can Message text field to trigger a denial of service condition.
CVE-2026-3778	The application does not detect or guard against cyclic PDF object references while handling JavaScript in PDF. When pages and annotations are crafted that refere traversal can cause uncontrolled recursion, stack exhaustion, and application crashes.
CVE-2019-25661	Remote Process Explorer 1.0.0.16 contains a local buffer overflow vulnerability that allows attackers to cause a denial of service by sending a crafted payload to th textbox and trigger a crash by connecting to the added computer, overwriting the SEH chain and corrupting exception handlers.
CVE-2026-35480	go-ipld-prime is an implementation of the InterPlanetary Linked Data (IPLD) spec interfaces, a batteries-included codec implementations of IPLD for CBOR and JSON decoder uses collection sizes declared in CBOR headers as Go preallocation hints for maps and lists. The decoder does not cap these size hints or account for their allocation. This vulnerability is fixed in 0.22.0.
CVE-2026-35199	SymCrypt is the core cryptographic function library currently used by Windows. From 103.5.0 to before 103.11.0, The SymCryptXmssSign function passes a 64-bit parameter sets with total tree height >= 32 (which includes standard predefined parameters), this causes silent truncation to zero, resulting in a drastically unders computation. Exploiting this issue would require an application using SymCrypt to perform an XMSS^MT signature using an attacker-controlled parameter set. It is signing, since signing is a private key operation, and private keys must be trusted by definition. Additionally, XMSS(^MT) signing should only be performed in a Ha testing purposes. This is a general rule irrespective of this CVE; XMSS(^MT) and other stateful signature schemes are only cryptographically secure when it is guar cannot be guaranteed by software alone. For this reason, XMSS(^MT) signing is also not FIPS approved when performed outside of an HSM. Fixed in version 103.11
CVE-2026-30526	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Zoo Management System v1.0. The vulnerability is located in the login page, specifica parameter back to the user without proper HTML encoding or sanitization. This allows remote attackers to inject arbitrary web script or HTML via a crafted URL.
CVE-2026-30252	Multiple reflected cross-site scripting (XSS) vulnerabilities in the login.php endpoint of Interzen Consulting S.r.l ZenShare Suite v17.0 allows attackers to execute ar the codice_azienda and red_url parameters.
CVE-2026-30251	A reflected cross-site scripting (XSS) vulnerability in the login_newpwd.php endpoint of Interzen Consulting S.r.l ZenShare Suite v17.0 allows attackers to execute a the codice_azienda parameter.
CVE-2026-20041	A vulnerability in Cisco Nexus Dashboard and Cisco Nexus Dashboard Insights could allow an unauthenticated, remote attacker to conduct a server-side request fo input validation for specific HTTP requests. An attacker could exploit this vulnerability by persuading an authenticated user of the device management interface to network requests that are sourced from the affected device to an attacker-controlled server. The attacker could then execute arbitrary script code in the context of
CVE-2026-35539	An issue was discovered in Roundcube Webmail before 1.5.14 and 1.6.14. XSS exists because of insufficient HTML attachment sanitization in preview mode. A victi
CVE-2026-35466	XSS vulnerability in cveInterface.js allows for inject HTML to be passed to display, as cveInterface trusts input from CVE API services
CVE-2026-34229	Emlog is an open source website building system. Prior to version 2.6.8, there is a stored cross-site scripting (XSS) vulnerability in emlog comment module via URI
CVE-2026-32629	phpMyFAQ is an open source FAQ web application. Prior to version 4.1.1, an unauthenticated attacker can submit a guest FAQ with an email address that is syntac <script>alert(1)</script>"@evil.com. PHP's FILTER_VALIDATE_EMAIL accepts this email as valid. The email is stored in the database without HTML sanitization and bypasses auto-escaping entirely. This issue has been patched in version 4.1.1.
CVE-2026-34729	phpMyFAQ is an open source FAQ web application. Prior to version 4.1.1, there is a stored XSS vulnerability via Regex Bypass in Filter::removeAttributes(). This issu
CVE-2025-61166	An open redirect in Ascertia SigningHub User v10.0 allows attackers to redirect users to a malicious site via a crafted URL.
CVE-2026-3877	A reflected cross-site scripting (XSS) vulnerability in the dashboard search functionality of the VertiGIS FM solution allows attackers to craft a malicious URL, that if context. Such a URL could be delivered through various means, for instance, by sending a link or by tricking victims to visit a page crafted by the attacker.
CVE-2026-35410	Directus is a real-time API and App dashboard for managing SQL database content. Prior to 11.16.1, an open redirect vulnerability exists in the login redirection log URLs as external, allowing attackers to bypass redirect allow-list validation and redirect users to arbitrary external domains upon successful authentication. This vu
CVE-2026-39335	ChurchCRM is an open-source church management system. Prior to 7.1.1, there is Stored XSS in group remove control and family editor state/country. This is prima vulnerability is fixed in 7.1.1.
CVE-2026-39336	ChurchCRM is an open-source church management system. Prior to 7.1.0, a stored cross-site scripting issue affects the Directory Reports form fields set from confi form defaults. This is primarily an admin-to-admin stored XSS path where writable configuration fields are abused. This vulnerability is fixed in 7.1.0.
CVE-2026-34606	Frappe Learning Management System (LMS) is a learning system that helps users structure their content. From version 2.27.0 to before version 2.48.0, Frappe LMS
CVE-2026-34951	Workbench is a suite of tools for administrators and developers to interact with Salesforce.com organizations via the Force.com APIs. Prior to 65.0.0, Workbench co which does not sanitize user-supplied input before rendering it in the page response. Improper neutralization of input during web page generation ('cross-site script fixed in 65.0.0.

CVE-2026-26058	Zulip is an open-source team collaboration tool. From version 1.4.0 to before version 11.6, ./manage.py import reads arbitrary files from the server filesystem via p copy any file the zulip user can read into the uploads directory during import. This issue has been patched in version 11.6.
CVE-2026-35055	XenForo before 2.3.9 and before 2.2.18 is vulnerable to cross-site scripting (XSS) related to lightbox usage in posts. An attacker can inject malicious scripts that ex
CVE-2026-33403	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. From 6.0 to before 6.5, a reflected DO arbitrary HTML into the Pi-hole admin interface by crafting a malicious URL. The file query parameter is interpolated into an innerHTML assignment without escapin <form> elements can exfiltrate credentials to an external origin. This vulnerability is fixed in 6.5.
CVE-2026-34083	Signal K Server is a server application that runs on a central hub in a boat. Prior to version 2.24.0, SignalK Server contains a code-level vulnerability in its OIDC logi the OAuth2 redirect_uri. Because the redirectUri configuration is silently unset by default, an attacker can spoof the Host header to steal OAuth authorization codes the authorization code to whatever domain was injected. This issue has been patched in version 2.24.0.
CVE-2026-20085	A vulnerability in the web-based management interface of Cisco IMC could allow an unauthenticated, remote attacker to conduct a reflected XSS attack against a u attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute based information.
CVE-2026-35390	Bulwark Webmail is a self-hosted webmail client for Stalwart Mail Server. Prior to 1.4.11, the reverse proxy (proxy.ts) set the Content-Security-Policy-Report-Only h scripting (XSS) attacks were logged but not blocked. Any user who could inject script content (e.g., via crafted email HTML) could execute arbitrary JavaScript in th on behalf of the user. This vulnerability is fixed in 1.4.11.
CVE-2018-25247	MyBB Like Plugin 3.0.0 contains a cross-site scripting vulnerability that allows attackers to inject malicious scripts by creating posts or threads with unvalidated sub when other users view the attacker's profile, where liked posts are displayed without sanitization.
CVE-2026-35491	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, Pi-hole FTL supports a CLI passwor only for configuration changes. While /api/config correctly blocks CLI sessions from mutating configuration, /api/teleporter allowed Teleporter imports for CLI sessio (authorization bypass). This vulnerability is fixed in 6.6.
CVE-2026-34765	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.5, 40.8.5, 41.1.0, and 42.0.0-alpha.5, when a named-window lookup to the opener's browsing context group. A renderer could navigate an existing child window that was opened by a different, unrelated rende permissive webPreferences (via setWindowOpenHandler's overrideBrowserWindowOptions), content loaded by the second renderer inherits those permissions. App and use setWindowOpenHandler to grant child windows elevated webPreferences such as a privileged preload script. Apps that do not elevate child window privile grant nodeIntegration: true or sandbox: false to child windows (contrary to the security recommendations) may be exposed to arbitrary code execution. This vulne
CVE-2026-34767	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to versions 38.8.6, 39.8.3, 40.8.3, and 41.0.3, apps th protocol.registerSchemesAsPrivileged() or modify response headers via webRequest.onHeadersReceived may be vulnerable to HTTP response header injection if at who can influence a header value may be able to inject additional response headers, affecting cookies, content security policy, or cross-origin access controls. App has been patched in versions 38.8.6, 39.8.3, 40.8.3, and 41.0.3.
CVE-2026-34830	Rack is a modular Ruby web server interface. Prior to versions 2.2.23, 3.1.21, and 3.2.6, Rack::Sendfile#map_accel_path interpolates the value of the X-Accel-Mapp Accel-Redirect. Because the header value is not escaped, an attacker who can supply X-Accel-Mapping to the backend can inject regex metacharacters and control with x-accel-redirect, this can allow an attacker to cause nginx to serve unintended files from configured internal locations. This issue has been patched in versions
CVE-2025-67805	A non-default configuration in Sage DPW 2025_06_004 allows unauthenticated access to diagnostic endpoints within the Database Monitor feature, exposing sensit all installations and never available in Sage DPW Cloud. It was forcibly disabled again in version 2025_06_003.
CVE-2025-13916	IBM Aspera Shares 1.9.9 through 1.11.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information
CVE-2026-34760	vLLM is an inference and serving engine for large language models (LLMs). From version 0.5.5 to before version 0.18.0, Librosa defaults to using numpy.mean for r a weighted downmixing algorithm. This discrepancy results in inconsistency between audio heard by humans (e.g., through headphones/regular speakers) and auc issue has been patched in version 0.18.0.
CVE-2026-34052	LTI JupyterHub Authenticator is a JupyterHub authenticator for LTI. Prior to version 1.6.3, the LTI 1.1 validator stores OAuth nonces in a class-level dictionary that g with knowledge of a valid consumer key can send repeated requests with unique nonces to gradually exhaust server memory, causing a denial of service. This issu
CVE-2026-5376	An issue that could prevent session inactivity timeouts from triggering due to automatic page reloading has been resolved. This is an instance of CWE-613: Insuffic score of CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:N (5.9 Medium). This issue was fixed in version 4.0.260203.0 of the runZero Platform.
CVE-2026-34610	The leancrypto library is a cryptographic library that exclusively contains only PQC-resistant cryptographic algorithms. Prior to version 1.7.1, lc_x509_extract_name An attacker who crafts a certificate with CN = victim's CN + 256 bytes padding gets cn_size = (uint8_t)(256 + N) = N, where N is the victim's CN length. The first N certificate has an identical CN to the victim's — enabling identity impersonation in PKCS#7 verification, certificate chain matching, and code signing. This issue has
CVE-2026-34380	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. From 3.2.0 to be src/lib/OpenEXRCore/internal_pxr24.c at line 377. The expression (uint64_t)(w * 3) computes w * 3 as a signed 32-bit integer before casting to uint64_t. When w is tested builds (clang/gcc without sanitizers), two's-complement wraparound commonly occurs, and for specific values of w the wrapped result is a small positive int bypassed, the decoding loop proceeds to write pixel data through dout, potentially extending far beyond the allocated output buffer. This vulnerability is fixed in 3.
CVE-2026-34778	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to versions 38.8.6, 39.8.1, 40.8.1, and 41.0.0, a servic used by webContents.executeJavaScript() and related methods, causing the main-process promise to resolve with attacker-controlled data. Apps are only affected webContents.executeJavaScript() (or webFrameMain.executeJavaScript()) in security-sensitive decisions. This issue has been patched in versions 38.8.6, 39.8.1, 40
CVE-2026-35201	Discount is an implementation of John Gruber's Markdown markup language in C. From 1.3.1.1 to before 2.2.7.4, a signed length truncation bug causes an out-of-b truncated to a signed int before entering the native parser, allowing the parser to read past the end of the supplied buffer and crash the process. This vulnerability
CVE-2026-5384	An issue that could allow a credential to be updated and used for a task from outside of the authorized organization scope has been resolved. This is an instance of CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N (5.8 Medium). This issue was fixed in version 4.0.26021.0 of the runZero Platform.

CVE-2026-34981	The whisperX API is a tool for enhancing and analyzing audio content. From 0.3.1 to 0.5.0, FileService.download_from_url() in app/services/file_service.py calls requ request is already made, and can be bypassed by appending .mp3 to any internal URL. The /speech-to-text-url endpoint is unauthenticated. This vulnerability is fix
CVE-2026-34772	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to versions 38.8.6, 39.8.0, 40.7.0, and 41.0.0-beta.8, to a use-after-free. If a session is torn down while a native save-file dialog is open for a download, dismissing the dialog dereferences freed memory, which may lea that do not permit downloads, are not affected. This issue has been patched in versions 38.8.6, 39.8.0, 40.7.0, and 41.0.0-beta.8.
CVE-2026-34761	Ella Core is a 5G core designed for private networks. Prior to version 1.8.0, Ella Core panics when processing a NGAP handover failure message. An attacker able to process, causing service disruption for all connected subscribers. This issue has been patched in version 1.8.0.
CVE-2026-5374	An issue that allowed MCP agents to access remediation and asset information from outside of the authorized organization scope has been resolved. This is an inst CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N (5.8 Medium). This issue was fixed in version 4.0.260202.0 of the runZero Platform.
CVE-2026-5378	An issue that allowed administrators to create and update users outside of their authorized organization scope has been resolved. This is an instance of CWE-863: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:H/A:N (5.8 Medium). This issue was fixed in version 4.0.260203.0 of the runZero Platform.
CVE-2025-24819	Nokia MantaRay NM is vulnerable to a Relative Path Traversal vulnerability due to improper validation of input parameter on the file system in Software Manager a
CVE-2026-30867	CocoaMQTT is a MQTT 5.0 client library for iOS and macOS written in Swift. Prior to version 2.2.2, a vulnerability exists in the packet parsing logic of CocoaMQTT th host iOS/macOS/tvOS application. If an attacker publishes the 4-byte malformed payload to a shared topic with the RETAIN flag set to true, the MQTT broker will pe the broker will automatically push the malformed packet. The app will instantly crash in the background before the user can even interact with it. This effectively " manually wiped from the broker database. This issue has been patched in version 2.2.2.
CVE-2026-5245	A vulnerability was found in Cesanta Mongoose up to 7.20. This impacts the function handle_mdns_record of the file mongoose.c of the component mDNS Record H overflow. Remote exploitation of the attack is possible. A high degree of complexity is needed for the attack. The exploitability is said to be difficult. The exploit has The patch is named 0d882f1b43ff2308b7486a56a9d60cd6dba8a3f1. You should upgrade the affected component. The vendor was contacted early, responded in a
CVE-2026-5618	A vulnerability was detected in kalcaddle kodbox up to 1.64. This affects an unknown function of the component shareMake/shareCheck. Performing a manipulation possible to be carried out remotely. The complexity of an attack is rather high. The exploitability is reported as difficult. The exploit is now public and may be used.
CVE-2026-5246	A vulnerability was determined in Cesanta Mongoose up to 7.20. Affected is the function mg_tls_verify_cert_signature of the file mongoose.c of the component P-38 attack can be executed remotely. Attacks of this nature are highly complex. The exploitability is told to be difficult. The exploit has been publicly disclosed and may called 0d882f1b43ff2308b7486a56a9d60cd6dba8a3f1. The affected component should be upgraded. The vendor was contacted early, responded in a very profess
CVE-2026-5673	A flaw was found in libtheora. This heap-based out-of-bounds read vulnerability exists within the AVI (Audio Video Interleave) parser, specifically in the avi_parse_in specially crafted AVI file containing a truncated header sub-chunk. This could lead to a denial-of-service (application crash) or potentially leak sensitive information
CVE-2026-5683	A vulnerability was found in Tenda CX12L 16.03.53.12. Affected by this vulnerability is the function fromP2pListFilter of the file /goform/P2pListFilter. Performing a must originate from the local network. The exploit has been made public and could be used.
CVE-2026-3776	The application does not validate the presence of required appearance (AP) data before accessing stamp annotation resources. When a PDF contains a stamp annc without a prior null or validity check, which allows a crafted document to trigger a null pointer dereference and crash the application, resulting in denial of service.
CVE-2026-34933	Avahi is a system which facilitates service discovery on a local network via the mDNS/DNS-SD protocol suite. Prior to version 0.9-rc4, any unprivileged local user ca flags. This issue has been patched in version 0.9-rc4.
CVE-2019-25657	AnyBurn 4.3 x86 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long string to the image c image file fields and click Convert Now to trigger a crash.
CVE-2019-25658	a-Mac Address Change 5.4 contains a local buffer overflow vulnerability that allows local attackers to crash the application by supplying oversized input to registrat Company', or 'Register Code' fields and click the Register button to trigger a denial of service crash.
CVE-2026-5475	A vulnerability was determined in NASA cFS up to 7.0.0. This impacts the function CFE_SB_TransmitMsg of the file cfe_sb_priv.c of the component CCSDS Header Si informed of the problem early through an issue report but has not responded yet.
CVE-2025-66484	IBM Aspera Shares 1.9.9 through 1.11.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI within a trusted session.
CVE-2026-5745	A flaw was found in libarchive. A NULL pointer dereference vulnerability exists in the ACL parsing logic, specifically within the archive_acl_from_text_nl() function. W subsequent fields), the function fails to perform adequate validation before advancing the pointer. An attacker can exploit this by providing a maliciously crafted ar resulting in a Denial of Service (DoS).
CVE-2026-34447	Open Neural Network Exchange (ONNX) is an open standard for machine learning interoperability. Prior to version 1.21.0, there is a symlink traversal vulnerability been patched in version 1.21.0.
CVE-2018-25256	IP TOOLS 2.50 contains a local buffer overflow vulnerability in the SNMP Scanner component that allows local attackers to crash the application by supplying oversi and trigger the crash by clicking the Start button, causing denial of service and SEH overwrite.
CVE-2026-34730	Copier is a library and CLI app for rendering project templates. Prior to version 9.14.1, Copier's _external_data feature allows a template to load YAML files using te read attacker-chosen YAML-parseable local files that are accessible to the user running Copier and expose their contents in rendered output. This issue has been p

CVE-2025-65116	Buffer Overflow Vulnerability in JP1/IT Desktop Management 2 - Manager on Windows, JP1/IT Desktop Management 2 - Operations Director on Windows, Job Manage Management - Manager on Windows, Job Management Partner 1/IT Desktop Management - Manager on Windows, JP1/NETM/DM Manager on Windows, JP1/NETM/DM Windows, Job Management Partner 1/Software Distribution Client on Windows.This issue affects JP1/IT Desktop Management 2 - Manager: from 13-50 before 13-50- 01-07, from 13-00 before 13-00-05, from 12-60 before 12-60-12, from 10-50 through 12-50-11; JP1/IT Desktop Management 2 - Operations Director: from 13-50 bef before 13-01-07, from 13-00 before 13-00-05, from 12-60 before 12-60-12, from 10-50 through 12-50-11; Job Management Partner 1/IT Desktop Management 2 - M 09-50 through 10-10-16; Job Management Partner 1/IT Desktop Management - Manager: from 09-50 through 10-10-16; JP1/NETM/DM Manager: from 09-00 through 1/Software Distribution Manager: from 09-00 through 09-51-13; Job Management Partner 1/Software Distribution Client: from 09-00 through 09-51-13.
CVE-2026-3777	The application does not properly validate the lifetime and validity of internal view cache pointers after JavaScript changes the document zoom and page state. Wh view object may be destroyed while stale pointers are still kept and later dereferenced, which under crafted JavaScript and document structures can lead to a use-
CVE-2026-5679	A security vulnerability has been detected in Totolink A3300R 17.0.0cu.557_B20221024. The impacted element is the function vsetTr069Cfg of the file /cgi-bin/cste The exploit has been disclosed publicly and may be used.
CVE-2026-31313	An authenticated stored cross-site scripting (XSS) vulnerability in the creation/editing module of Feehi CMS v2.1.1 allows attackers to execute arbitrary web scripts
CVE-2026-34903	Missing Authorization vulnerability in OceanWP Ocean Extra allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ocean Extra:
CVE-2026-33406	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. From 6.0 to before 6.5, configuration v without escaping in settings-advanced.js, enabling HTML attribute injection. A double quote in any config value breaks out of the attribute context. JavaScript exec element styling for UI redressing. The primary attack vector is importing a malicious teleporter backup, which bypasses per-field server-side validation. This vulner
CVE-2026-34749	Payload is a free and open source headless content management system. Prior to version 3.79.1, a Cross-Site Request Forgery (CSRF) vulnerability exists in the au bypassed, allowing cross-site requests to be made. This issue has been patched in version 3.79.1.
CVE-2026-34848	hoppscotch is an open source API development ecosystem. Prior to version 2026.3.0, there is a stored XSS vulnerability in the team member overflow tooltip via di
CVE-2017-20233	Hirschmann HiLCOS products OpenBAT, BAT450, WLC, BAT867 contains a firewall filtering vulnerability that fails to correctly filter IPv4 multicast and broadcast traf to be bypassed. Attackers with network access can inject or observe multicast and broadcast packets that should have been blocked by the firewall.
CVE-2026-31350	An authenticated stored cross-site scripting (XSS) vulnerability in Feehi CMS v2.1.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted
CVE-2026-31153	A stored cross-site scripting (XSS) vulnerability in Bynder v0.1.394 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.
CVE-2025-66485	IBM Aspera Shares 1.9.9 through 1.11.0 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an at scripting, cache poisoning or session hijacking.
CVE-2026-32712	Open Source Point of Sale is a web based point-of-sale application written in PHP using CodeIgniter framework. Prior to 3.4.3, a Stored Cross-Site Scripting (XSS) vu configured with escape: false in the bootstrap-table column configuration, causing customer names to be rendered as raw HTML. An attacker with customer manag last_name field, which executes in the browser of any user viewing the Daily Sales page. This vulnerability is fixed in 3.4.3.
CVE-2026-31352	An authenticated stored cross-site scripting (XSS) vulnerability in the Role Management module of Feehi CMS v2.1.1 allows attackers to execute arbitrary web scrip
CVE-2026-29598	Multiple stored cross-site scripting (XSS) vulnerabilities in the submit_add_user.asp endpoint of DDSN Interactive Acora CMS v10.7.1 allow attackers to execute arb Name parameters.
CVE-2026-31353	An authenticated stored cross-site scripting (XSS) vulnerability in the Category module of Feehi CMS v2.1.1 allows attackers to execute arbitrary web scripts or HTM
CVE-2026-22675	OCS Inventory NG Server version 2.12.3 and prior contain a stored cross-site scripting vulnerability that allows unauthenticated attackers to execute arbitrary Java Attackers can register rogue agents or craft requests with malicious User-Agent values that are stored without sanitation and rendered with insufficient encoding in authenticated users viewing the statistics dashboard.
CVE-2026-34777	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to versions 38.8.6, 39.8.1, 40.8.1, and 41.0.0, when a permissions, the origin passed to session.setPermissionRequestHandler() was the top-level page's origin rather than the requesting iframe's origin. Apps that grant inadvertently grant permissions to embedded third-party content. The correct requesting URL remains available via details.requestingUrl. Apps that already check 39.8.1, 40.8.1, and 41.0.0.
CVE-2026-31354	Multiple authenticated stored cross-site scripting (XSS) vulnerabilities in the Permissions module of Feehi CMS v2.1.1 allows attackers to execute arbitrary web scri parameters.
CVE-2026-34425	OpenClaw versions prior to commit 8aceaf5 contain a preflight validation bypass vulnerability in shell-bleed protection that allows attackers to execute blocked scr recognize. Attackers can craft commands such as piped execution, command substitution, or subshell invocation to bypass the validateScriptFileForShellBleed() va
CVE-2026-4364	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 throug listings retrieved via a browser session to return a JSON payload while incorrectly specifying the response Content-Type as text/html. Because the content is delive script under certain conditions. This creates an opportunity for JavaScript injection, potentially leading to cross-site scripting (XSS).

CVE-2026-35046	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. Prior to 2.6.4, Tandoor Recipes allows authenticated users to i explicitly whitelists the <style> tag, causing the backend to persist and serve unsanitized CSS payloads via the API. Any client consuming instructions_markdown f attacker-controlled CSS — enabling UI redressing, phishing overlays, visual defacement, and CSS-based data exfiltration. This vulnerability is fixed in 2.6.4.
CVE-2026-35508	Shynet before 0.14.0 allows XSS in urldisplay and iconify template filters,
CVE-2026-35200	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 8.6.73 and 9.7.1-alpha.4, a file can be uploaded w Content-Type header that differs from the extension (e.g., text/html). The Content-Type is passed to the storage adapter without consistency validation. Storage ad file with the mismatched Content-Type. The default GridFS adapter is not affected because it derives Content-Type from the filename at serving time. This vulneral
CVE-2026-34590	Postiz is an AI social media scheduling tool. Prior to version 2.21.4, the POST /webhooks/ endpoint for creating webhooks uses WebhooksDto which validates the ur blocks internal/private network addresses. The update (PUT /webhooks/) and test (POST /webhooks/send) endpoints correctly apply @IsSafeWebhookUrl. When a p validation, enabling blind SSRF against internal services. This issue has been patched in version 2.21.4.
CVE-2026-34584	listmonk is a standalone, self-hosted, newsletter and mailing list manager. From version 4.1.0 to before version 6.1.0, bugs in list permission checks allows users in different scenarios. This only affects multi-user environments with untrusted users. This issue has been patched in version 6.1.0.
CVE-2026-34974	phpMyFAQ is an open source FAQ web application. Prior to version 4.1.1, the regex-based SVG sanitizer in phpMyFAQ (SvgSanitizer.php) can be bypassed using HT edit_faq permission can upload a malicious SVG that executes arbitrary JavaScript when viewed, enabling privilege escalation from editor to full admin takeover. Th
CVE-2026-39380	Open Source Point of Sale is a web based point-of-sale application written in PHP using CodeIgniter framework. Prior to 3.4.3, a Stored Cross-Site Scripting (XSS) vu properly sanitize user input supplied through the stock_location parameter, allowing attackers to inject malicious JavaScript code that is stored in the database and 3.4.3.
CVE-2026-4065	The Smart Slider 3 plugin for WordPress is vulnerable to unauthorized access and modification of data due to missing capability checks on multiple wp_ajax_smart- display_admin_ajax() method does not call checkForCap() (which requires unfiltered_html capability), and several controller actions only validate the nonce (validat authenticated attackers, with Contributor-level access and above, to enumerate slider metadata and create, modify, and delete image storage records by obtaining
CVE-2026-33978	Notesnook is a note-taking app focused on user privacy & ease of use. Prior to version 3.3.17, a stored XSS vulnerability exists in the mobile share / web clip flow b and then rendered with innerHTML inside the mobile share editor WebView. An attacker can control the shared title metadata (for example through Android/iOS sh HTML such as <img src=x onerror=...>. When the victim opens the Notesnook share flow and selects Web clip, the payload is inserted into the generated HTI 3.3.17.
CVE-2026-4829	Improper authentication in the external OAuth authentication flow in Devolutions Server 2026.1.11 and earlier allows an authenticated user to authenticate as othe authentication flow.
CVE-2026-35540	An issue was discovered in Roundcube Webmail 1.6.0 before 1.6.14. Insufficient Cascading Style Sheets (CSS) sanitization in HTML e-mail messages may lead to SS
CVE-2026-1243	IBM Content Navigator 3.0.15, 3.1.0, and 3.2.0 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript co credentials disclosure within a trusted session.
CVE-2026-34753	vLLM is an inference and serving engine for large language models (LLMs). From 0.16.0 to before 0.19.0, a server-side request forgery (SSRF) vulnerability in down vLLM batch runner issue arbitrary HTTP/HTTPS requests from the server, without any URL validation or domain restrictions. This can be used to target internal serv host. This vulnerability is fixed in 0.19.0.
CVE-2025-15611	The Popup Box WordPress plugin before 5.5.0 does not properly validate nonces in the add_or_edit_popupbox() function before saving popup data, allowing unauth authenticated admin visits a malicious page, the attacker can create or modify popups with arbitrary JavaScript that executes in the admin panel and frontend.
CVE-2026-39367	WWBN AVideo is an open source video platform. In versions 26.0 and prior, AVideo's EPG (Electronic Program Guide) feature parses XML from user-controlled URLs A user with upload permission can set a video's epg_link to a malicious XML file whose <title> elements contain JavaScript. This payload executes in the browser o account takeover.
CVE-2026-2696	The Export All URLs WordPress plugin before 5.1 generates CSV filenames containing posts URLS (including private posts) in a predictable pattern using a random directory. As a result, any unauthenticated user can brute-force the filenames to gain access to sensitive data contained within the exported files.
CVE-2026-26895	User enumeration vulnerability in /pwreset.php in osTicket v1.18.2 allows remote attackers to enumerate valid usernames registered in the platform.
CVE-2026-35483	text-generation-webui is an open-source web interface for running Large Language Models. Prior to 4.3, an unauthenticated path traversal vulnerability in load_tem on the server filesystem. For .jinja files the content is returned verbatim; for .yaml files a parsed key is extracted. This vulnerability is fixed in 4.3.
CVE-2026-5666	A vulnerability was detected in code-projects Online FIR System 1.0. Affected by this issue is some unknown functionality of the file /complaints.sql of the compone sensitive information. The attack may be performed from remote. The exploit is now public and may be used.
CVE-2026-5619	A flaw has been found in Braffolk mcp-summarization-functions up to 0.1.5. This impacts an unknown function of the file src/server/mcp-server.ts of the component to os command injection. The attack requires local access. The exploit has been published and may be used. The vendor was contacted early about this disclosure
CVE-2026-1491	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 throug could allow a remote attacker to access sensitive information due to an inconsistent interpretation of an HTTP request by a reverse proxy.
CVE-2026-5621	A vulnerability was found in ChrisChinchilla Vale-MCP up to 0.1.0. Affected by this vulnerability is an unknown functionality of the file src/index.ts of the component injection. Attacking locally is a requirement. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not

CVE-2026-25742	Zulip is an open-source team collaboration tool. Prior to version 11.6, Zulip is an open-source team collaboration tool. From version 1.4.0 to before version 11.6, ev WEB_PUBLIC_STREAMS_ENABLED) is disabled, attachments originating from web-public streams can still be retrieved anonymously. As a result, file contents remai spectator access is disabled, the /users/me/<stream_id>/topics endpoint remains reachable anonymously, allowing retrieval of topic history for web-public streams 11.6.
CVE-2025-14938	The Listeo Core plugin for WordPress is vulnerable to unauthenticated arbitrary media upload in all versions up to, and including, 2.0.27 via the "listeo_core_handle on the AJAX endpoint handling file uploads. This makes it possible for unauthenticated attackers to upload arbitrary media to the site's media library, without achie
CVE-2026-34776	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to versions 38.8.6, 39.8.1, 40.8.1, and 41.0.0, on mac out-of-bounds heap read when parsing a crafted second-instance message. Leaked memory could be delivered to the app's second-instance event handler. This iss not call app.requestSingleInstanceLock() are not affected. Windows is not affected by this issue. This issue has been patched in versions 38.8.6, 39.8.1, 40.8.1, and
CVE-2026-34523	SillyTavern is a locally installed user interface that allows users to interact with text generation large language models, image generation engines, and text-to-spee route handler allows any unauthenticated user to determine whether files exist anywhere on the server's filesystem. by sending percent-encoded "../" sequences (' of files. This issue has been patched in version 1.17.0.
CVE-2026-28767	A specific administrative endpoint notifications is accessible without proper authentication.
CVE-2026-34511	OpenClaw before 2026.4.2 reuses the PKCE verifier as the OAuth state parameter in the Gemini OAuth flow, exposing it through the redirect URL. Attackers who ca defeating PKCE protection and enabling token redemption.
CVE-2026-34715	ewe is a Gleam web server. Prior to version 3.0.6, the encode_headers function in src/ewe/internal/encoder.gleam directly interpolates response header keys and v application that passes user-controlled data into response headers (e.g., setting a Location redirect header from a request parameter) allows an attacker to inject a possible cross-site scripting. Notably, ewe does validate CRLF in incoming request headers via validate_field_value() in the HTTP/1.1 parser — but provides no equi patched in version 3.0.6.
CVE-2026-35452	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the plugin/CloneSite/client.log.php endpoint serves the clone operation log file without User::isAdmin(). The log contains internal filesystem paths, remote server URLs, and SSH connection metadata.
CVE-2026-32662	Development and test API endpoints are present that mirror production functionality.
CVE-2024-53828	Ericsson Packet Core Controller (PCC) versions prior to 1.38 contain a vulnerability where an attacker sending a large volume of specially crafted messages may ca
CVE-2026-35413	Directus is a real-time API and App dashboard for managing SQL database content. Prior to 11.16.1, when GRAPHQL_INTROSPECTION=false is configured, Directus the server_specs_graphql resolver on the /graphql/system endpoint returns an equivalent SDL representation of the schema and was not subject to the same restri structure (collection names, field names, types, and relationships) to unauthenticated users at the public permission level, and to authenticated users at their perm
CVE-2026-39373	JWCrypto implements JWK, JWS, and JWE specifications using python-cryptography. Prior to 1.5.7, an unauthenticated attacker can exhaust server memory by send limits input token size to 250KB but does not validate the decompressed output size. An unauthenticated attacker can cause memory exhaustion on memory-const 100MB. This vulnerability is fixed in 1.5.7.
CVE-2026-5638	A vulnerability was detected in HerikLyma CPPWebFramework up to 3.1. This issue affects some unknown processing. Performing a manipulation results in path tra may be used. The project was informed of the problem early through an issue report but has not responded yet.
CVE-2016-20051	Snews CMS 1.7 contains a cross-site request forgery vulnerability that allows attackers to change administrator credentials without authentication by crafting malic containing a hidden form that submits POST requests to the changeup action, modifying the admin username and password parameters to gain unauthorized acce
CVE-2026-35484	text-generation-webui is an open-source web interface for running Large Language Models. Prior to 4.3, an unauthenticated path traversal vulnerability in load_pre pairs (including passwords, API keys, connection strings) are returned in the API response. This vulnerability is fixed in 4.3.
CVE-2016-20053	Redaxo CMS 5.2 contains a cross-site request forgery vulnerability that allows unauthenticated attackers to create administrative user accounts by tricking authen targeting the users endpoint with hidden fields containing admin credentials and account parameters to add new administrator accounts without user consent.
CVE-2026-5549	A vulnerability was determined in Tenda AC10 16.03.10.10_multi_TDE01. Affected by this issue is some unknown functionality of the file /webroot_ro/pem/privkeyS can lead to use of hard-coded cryptographic key . The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.
CVE-2026-2862	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 throug could allow a remote attacker to access sensitive information due to an inconsistent interpretation of an HTTP request by a reverse proxy.
CVE-2026-35449	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the install/test.php diagnostic script has its CLI-only access guard disabled by comment exposing video viewer statistics including IP addresses, session IDs, and user agents to unauthenticated visitors.
CVE-2026-5380	An issue that could allow an authorized user to view the clear-text secrets for a subset of credential types and fields has been resolved. This is an instance of CWE- CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N (5.3 Medium). This issue was fixed in version 4.0.260204.2 of the runZero Platform.
CVE-2026-5312	A weakness has been 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, DN 05 and DNS-1550-04 up to 20260205. Affected by this vulnerability is the function FMT_restart/Status_HDInfo/SMART_List/ScanDisk_info/ScanDisk/volume_status/Get_Volume_Mapping/FMT_check_disk_remount_state/FMT_rebuildinfo/FMT_result_lis of the file /cgi-bin/dsk_mgr.cgi. Executing a manipulation can lead to improper access controls. It is possible to launch the attack remotely. The exploit has been ma
CVE-	

2026-33617	An unauthenticated remote attacker can access a configuration file containing database credentials. This can result in a some loss of confidentiality, but there is no
CVE-2026-5484	A weakness has been identified in BookStackApp BookStack up to 26.03. Affected is the function chapterToMarkdown of the file app/Exports/ExportFormatter.php c pages can lead to improper access controls. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for at 8a59895ba063040cc8dafd82e94024c406df3d04. It is advisable to upgrade the affected component. The vendor was contacted early, responded in a very professi
CVE-2026-5414	A security flaw has been discovered in Newgen OmniDocs up to 12.0.00. Affected by this issue is some unknown functionality of the file /omnidocs/WebApiRequest of resource identifiers. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. The vendor was conta
CVE-2026-4325	A flaw was found in Keycloak. The SingleUseObjectProvider, a global key-value store, lacks proper type and namespace isolation. This vulnerability allows an attack action tokens, such as password reset links. This could lead to unauthorized access or account compromise.
CVE-2026-5531	A vulnerability has been found in SourceCodester Student Result Management System 1.0. Impacted is an unknown function of the file /login_credentials.txt of the a file or on disk. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2026-35179	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the SocialMediaPublisher plugin exposes a publishInstagram.json.php endpoint that act accepts user-controlled parameters including an access token, container ID, and Instagram account ID, and passes them directly to the Graph API via InstagramUp arbitrary Graph API calls through the server, potentially using stolen tokens or abusing the platform's own credentials.
CVE-2026-35542	An issue was discovered in Roundcube Webmail before 1.5.14 and 1.6.14. The remote image blocking feature can be bypassed via a crafted background attribute access-control bypass.
CVE-2026-5661	A vulnerability was identified in Free5GC 4.2.0. This affects an unknown function of the component NGSetupRequest Handler. Such manipulation leads to denial of might be used.
CVE-2026-34510	OpenClaw before 2026.3.22 contains a path traversal vulnerability in Windows media loaders that accepts remote-host file URLs and UNC-style paths before local-p are treated as local content, bypassing intended access restrictions.
CVE-2026-5585	A vulnerability was found in Tencent AI-Infra-Guard 4.0. The affected element is an unknown function of the file common/websocket/task_manager.go of the compo disclosure. The attack may be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but di
CVE-2026-35543	An issue was discovered in Roundcube Webmail before 1.5.14 and 1.6.14. The remote image blocking feature can be bypassed via SVG content (with animate attri bypass.
CVE-2026-34973	phpMyFAQ is an open source FAQ web application. Prior to version 4.1.1, the searchCustomPages() method in phpmyfaq/src/phpMyFAQ/Search.php uses real_escap clauses. However, real_escape_string() does not escape SQL LIKE metacharacters % (match any sequence) and _ (match any single character). An unauthenticated unintended records — including content that was not meant to be surfaced — resulting in information disclosure. This issue has been patched in version 4.1.1.
CVE-2026-35468	nimiq/core-rs-albatross is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. Prior to version 1.3.0, two peer-t and call blockchain.history_store.history_index().unwrap() directly. That assumption is false by construction. HistoryStoreProxy::history_index() explicitly returns No otherwise running without the history index, a remote peer can send RequestTransactionsProof or RequestTransactionReceiptsByAddress and trigger an Option::un
CVE-2026-35544	An issue was discovered in Roundcube Webmail before 1.5.14 and 1.6.14. Insufficient Cascading Style Sheets (CSS) sanitization in HTML e-mail messages may lead
CVE-2026-5323	A vulnerability was found in priyankark a11y-mcp up to 1.0.5. This vulnerability affects the function A11yServer of the file src/index.js. The manipulation results in s exploit has been made public and could be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version resolve this issue. The patch is identified as e3e11c9e8482bd06b82fd9fced67be4856f0dffc. It is recommended to upgrade the affected component. The vendor ac a local stdio MCP server - it has no HTTP endpoint and is not network-accessible. The caller is always the local user or an LLM acting on their behalf with user appro
CVE-2026-35545	An issue was discovered in Roundcube Webmail before 1.5.15 and 1.6.15. The remote image blocking feature can be bypassed via SVG content in an e-mail messa animate element with attributeName=fill/filter/stroke.
CVE-2026-5326	A vulnerability was identified in SourceCodester Leave Application System 1.0. Impacted is an unknown function of the file /index.php?page=manage_user of the c authorization bypass. The attack can be executed remotely. The exploit is publicly available and might be used.
CVE-2026-34826	Rack is a modular Ruby web server interface. Prior to versions 2.2.23, 3.1.21, and 3.2.6, Rack::Utils.get_byte_ranges parses the HTTP Range header without limiting rejects ranges whose total byte coverage exceeds the file size, it does not restrict the count of ranges. An attacker can supply many small overlapping ranges such consumption per request. This results in a denial of service condition in Rack file-serving paths that process multipart byte range responses. This issue has been pa
CVE-2026-5571	A vulnerability was identified in Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30. The impacted element is an unknown function of the file /fs of the component Co disclosure. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure bu
CVE-2026-35592	pyLoad is a free and open-source download manager written in Python. Prior to 0.5.0b3.dev97, the _safe_extractall() function in src/pyload/plugins/extractors/UnTa character-level string comparison rather than path-level comparison. This allows a specially crafted tar archive to write files outside the intended extraction directo 2026-32808 fix (commit 5f4f0fa) but was never applied to _safe_extractall(), making this an incomplete fix. This vulnerability is fixed in 0.5.0b3.dev97.
CVE-2026-22680	OpenViking versions prior to 0.3.3 contain a missing authorization vulnerability in the task polling endpoints that allows unauthorized attackers to enumerate or ret /api/v1/tasks and /api/v1/tasks/{task_id} routes without authentication to expose task type, task status, resource identifiers, archive URIs, result payloads, and erro deployments.
CVE-2026-3177	The Charitable – Donation Plugin for WordPress – Fundraising with Recurring Donations & More plugin for WordPress is vulnerable to Insufficient Verification of Data cryptographic verification of incoming Stripe webhook events. This makes it possible for unauthenticated attackers to forge payment_intent.succeeded webhook pa

CVE-2026-5311	A security flaw has been discovered 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 1200-05 and DNS-1550-04 up to 20260205. Affected is the function Webdav_Access_List of the file /cgi-bin/file_center.cgi. Performing a manipulation of the argum remotely. The exploit has been released to the public and may be used for attacks.
CVE-2026-5601	A vulnerability was found in Acrel Electrical Prepaid Cloud Platform 1.0. This issue affects some unknown processing of the file /bin.rar of the component Backup Fil 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.
CVE-2026-25043	Budibase is an open-source low-code platform. Prior to version 3.23.25, a business logic vulnerability exists in Budibase's password reset functionality due to the a Password" endpoint. An unauthenticated attacker can repeatedly trigger password reset requests for the same email address, resulting in hundreds of password re user harassment, denial of service (DoS) against user inboxes, and potential financial and reputational impact for Budibase. This issue has been patched in version
CVE-2026-34979	OpenPrinting CUPS is an open source printing system for Linux and other Unix-like operating systems. In versions 2.4.16 and prior, there is a heap-based buffer ov time of publication, there are no publicly available patches.
CVE-2026-5342	A flaw has been found in LibRaw up to 0.22.0. This affects the function LibRaw::nikon_load_padded_packed_raw of the file src/decoders/decoders_libraw.cpp of the can lead to out-of-bounds read. It is possible to launch the attack remotely. The exploit has been published and may be used. Upgrading to version 0.22.1 mitigate advisable to upgrade the affected component.
CVE-2026-34999	OpenViking versions 0.2.5 prior to 0.2.14 contain a missing authentication vulnerability in the bot proxy router that allows remote unauthenticated attackers to acc and POST /bot/v1/chat/stream endpoints. Attackers can bypass authentication checks and interact directly with the upstream bot backend through the OpenViking
CVE-2026-35487	text-generation-webui is an open-source web interface for running Large Language Models. Prior to 4.3, an unauthenticated path traversal vulnerability in load_pro verbatim in the API response. This vulnerability is fixed in 4.3.
CVE-2026-35450	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the plugin/API/check.ffmpeg.json.php endpoint probes the FFmpeg remote server confi management endpoints (kill.ffmpeg.json.php, list.ffmpeg.json.php, ffmpeg.php) require User::isAdmin().
CVE-2026-5603	A vulnerability was identified in elgentos magento2-dev-mcp up to 1.0.2. The affected element is the function executeMagerun2Command of the file src/index.ts. S locally. The exploit is publicly available and might be used. The name of the patch is aa1ffcc0aea1b212c69787391783af27df15ae9d. A patch should be applied to
CVE-2026-5602	A vulnerability was determined in Nor2-io heim-mcp up to 0.1.3. Impacted is the function registerTools of the file src/tools.ts of the component new_heim_applicati causes os command injection. The attack requires local access. The exploit has been publicly disclosed and may be utilized. Patch name: c321d8af25f77668781e6 vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.
CVE-2026-34230	Rack is a modular Ruby web server interface. Prior to versions 2.2.23, 3.1.21, and 3.2.6, Rack::Utils.select_best_encoding processes Accept-Encoding values with q this method is used by Rack::Deflater to choose a response encoding, an unauthenticated attacker can send a single request with a crafted Accept-Encoding heade This results in a denial of service condition for applications using Rack::Deflater. This issue has been patched in versions 2.2.23, 3.1.21, and 3.2.6.
CVE-2026-5527	A weakness has been identified in Tenda 4G03 Pro 1.0/1.0re/01.bin/04.03.01.53. Affected by this issue is some unknown functionality of the file /etc/www/pem/serv use of hard-coded cryptographic key . It is possible to initiate the attack remotely.
CVE-2026-34736	Open edX Platform enables the authoring and delivery of online learning at any scale. From the maple release to before the ulmo release, an unauthenticated atta OAuth2 password grant issuing tokens to inactive users (documented behavior) and the activation_key being exposed in the REST API response at /api/user/v1/acc
CVE-2026-34786	Rack is a modular Ruby web server interface. Prior to versions 2.2.23, 3.1.21, and 3.2.6, Rack::Static#applicable_rules evaluates several header_rules types agains before the file is served. As a result, a request for a URL-encoded variant of a static path can serve the same file without the headers that header_rules were intend response headers to static content, this can allow an attacker to bypass those headers by requesting an encoded form of the path. This issue has been patched in
CVE-2026-34763	Rack is a modular Ruby web server interface. Prior to versions 2.2.23, 3.1.21, and 3.2.6, Rack::Directory interpolates the configured root path directly into a regula metacharacters such as +, *, or ., the prefix stripping can fail and the generated directory listing may expose the full filesystem path in the HTML output. This issue
CVE-2025-14944	The Backup Migration plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 2.0.0. This is due to a missing capability check endpoint only validates against hardcoded tokens which are publicly exposed in the plugin's JavaScript. This makes it possible for unauthenticated attackers to trig transfers to configured cloud storage targets and resource exhaustion.
CVE-2026-35583	Emissary is a P2P based data-driven workflow engine. Prior to 8.39.0, the configuration API endpoint (/api/configuration/{name}) validated configuration names usi bypassed using URL-encoded variants, double-encoding, or Unicode normalization to achieve path traversal and read configuration files outside the intended direct
CVE-2026-5650	A vulnerability was found in code-projects Online Application System for Admission 1.0. Impacted is an unknown function of the file /enrollment/database/oas.sql. P attack is possible to be carried out remotely. The exploit has been made public and could be used.
CVE-2026-34899	Missing Authorization vulnerability in Eniture technology LTL Freight Quotes – Worldwide Express Edition allows Exploiting Incorrectly Configured Access Control Se n/a through 5.2.1.
CVE-2025-66442	In Mbed TLS through 4.0.0, there is a compiler-induced timing side channel (in RSA and CBC/ECB decryption) that only occurs with LLVM's select-optimize feature.
CVE-2026-35613	coursevault-preview is a utility for previewing course material files from a configured directory. coursevault-preview versions prior to 0.1.1 contain a path traversal String.prototype.startsWith(baseDir) on a normalized path, which does not enforce a directory boundary. An attacker who controls the relativePath argument to aff baseDir when a sibling directory exists whose name shares the same string prefix. This vulnerability is fixed in 0.1.1.
CVE-2026-35516	LinkAce is a self-hosted archive to collect website links. Prior to 2.5.4, LinkRepository::update and CheckLinksCommand::checkLink do not check for private IPs. An metadata, internal APIs) by creating a link with a public URL and then updating it to a private IP. The links:check cron job makes the request server-side without IP topology. This vulnerability is fixed in 2.5.4.

CVE-2026-34589	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. From 3.2.0 to be component block pointers using signed 32-bit arithmetic. For a large enough width, the calculation overflows and later decoder stores operate on a wrapped pointe 3.3.9, and 3.4.9.
CVE-2026-34972	OpenFGA is a high-performance and flexible authorization/permission engine built for developers and inspired by Google Zanzibar. From 1.8.0 to 1.13.1, under spe relation, and user combination can result in improper policy enforcement. This vulnerability is fixed in 1.14.0.
CVE-2026-34526	SillyTavern is a locally installed user interface that allows users to interact with text generation large language models, image generation engines, and text-to-spee checked against /^\d+\.\d+\.\d+\.\d+$/. This only matches literal dotted-quad IPv4 (e.g. 127.0.0.1, 10.0.0.1). It does not catch: localhost (hostname, not dotted-qu localtest.me -> 127.0.0.1). A separate port check (urlObj.port !== '') limits exploitation to services on default ports (80/443), making this lower severity than a fully
CVE-2026-5704	A flaw was found in tar. A remote attacker could exploit this vulnerability by crafting a malicious archive, leading to hidden file injection with fully attacker-controlle an attacker to introduce malicious files onto a system without detection.
CVE-2026-4925	Improper access control in the users MFA feature in Devolutions Server allows an authenticated user to bypass administrator-enforced restrictions and remove thei affects Server: from 2026.1.6 through 2026.1.11.
CVE-2026-5175	Improper access control in the multi-factor authentication (MFA) management API in Devolutions Server allows an authenticated attacker to delete their own config crafted HTTP requests. This issue affects Server: from 2026.1.6 through 2026.1.11.
CVE-2026-35461	Papra is a minimalistic document management and archiving platform. Prior to 26.4.0, the Papra webhook system allows authenticated users to register arbitrary U makes outbound HTTP POST requests to registered URLs, including localhost, internal network ranges, and cloud provider metadata endpoints, on every document
CVE-2026-34061	nimiq/core-rs-albatross is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. Prior to version 1.3.0, an elected match the canonical next interlink. Honest validators accept that proposal in verify_macro_block_proposal() because the proposal path validates header shape, suc for election blocks. The same finalized block is later rejected by verify_block() during push with InvalidInterlink. Because validators prevote and precommit the mal before voting. This issue has been patched in version 1.3.0.
CVE-2026-20174	A vulnerability in the Metadata update feature of Cisco Nexus Dashboard Insights could allow an authenticated, remote attacker to write arbitrary files to an affecte file. An attacker could exploit this vulnerability by crafting a metadata update file and manually uploading it to an affected device. A successful exploit could allow the root user. To exploit this vulnerability, the attacker must have valid administrative credentials. Note: Manual uploading of metadata files is typical for Air manual upload option exists for both deployments.
CVE-2026-34608	NanoMQ MQTT Broker (NanoMQ) is an all-around Edge Messaging Platform. Prior to version 0.24.10, in NanoMQ's webhook_inproc.c, the hook_work_cb() function p body is obtained from nng_msg_body(msg), which is a binary buffer without a guaranteed null terminator. This leads to an out-of-bounds read (OOB read) as cJSON buffer (e.g., nng_msg metadata or adjacent heap/stack). The issue is often masked by nng's allocation padding (extra 32 bytes of zeros for non-power-of-two sizes length is a power-of-two >=1024 (no padding added). This issue has been patched in version 0.24.10.
CVE-2026-31351	An authenticated stored cross-site scripting (XSS) vulnerability in the creation/editing module of Feehi CMS v2.1.1 allows attackers to execute arbitrary web scripts
CVE-2026-20087	A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with administrative privileges to conduct a stor validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could al access sensitive, browser-based information.
CVE-2026-34831	Rack is a modular Ruby web server interface. Prior to versions 2.2.23, 3.1.21, and 3.2.6, Rack::Files#fail sets the Content-Length response header using String#siz characters, the declared Content-Length is smaller than the number of bytes actually sent on the wire. Because Rack::Files reflects the requested path in 404 resp containing percent-encoded UTF-8 characters. This results in incorrect HTTP response framing and may cause response desynchronization in deployments that rely 2.2.23, 3.1.21, and 3.2.6.
CVE-2026-20088	A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with administrative privileges to conduct a stor validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could al access sensitive, browser-based information.
CVE-2026-35571	Emissary is a P2P based data-driven workflow engine. Prior to 8.39.0, Mustache navigation templates interpolated configuration-controlled link values directly into navItems configuration could inject javascript: URIs, enabling stored cross-site scripting (XSS) against other authenticated users viewing the Emissary web interfac
CVE-2025-66486	IBM Aspera Shares 1.9.9 through 1.11.0 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be execute
CVE-2026-20089	A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with administrative privileges to conduct a stor validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could al access sensitive, browser-based information.
CVE-2026-32762	Rack is a modular Ruby web server interface. From versions 3.0.0.beta1 to before 3.1.21 and 3.2.0 to before 3.2.6, Rack::Utils.forwarded_values parses the RFC 72 Because quoted values may legally contain semicolons, a header can be interpreted by Rack as multiple Forwarded directives rather than as a single quoted for va preserves quoted Forwarded values differently, this discrepancy can allow an attacker to smuggle host, proto, for, or by parameters through a single header value.
CVE-2026-20090	A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with administrative privileges to conduct a stor validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could al access sensitive, browser-based information.
CVE-2026-34835	Rack is a modular Ruby web server interface. From versions 3.0.0.beta1 to before 3.1.21, and 3.2.0 to before 3.2.6, Rack::Request parses the Host header using ar compliant hostnames, including /, ?, #, and @. Because req.host returns the full parsed value, applications that validate hosts using naive prefix or suffix checks ca req.host, req.url, or req.base_url for link generation, redirects, or origin validation. This issue has been patched in versions 3.1.21 and 3.2.6.
CVE-2026-26962	Rack is a modular Ruby web server interface. From version 3.2.0 to before version 3.2.6, Rack::Multipart::Parser unfolds folded multipart part headers incorrectly. V CRLF in parsed parameter values such as filename or name instead of removing the folded line break during unfolding. As a result, applications that later reuse tho injection or response splitting. This issue has been patched in version 3.2.6.

CVE-2026-27447	OpenPrinting CUPS is an open source printing system for Linux and other Unix-like operating systems. In versions 2.4.16 and prior, CUPS daemon (cupsd) contains during authorization checks. The vulnerability allows an unprivileged user to gain unauthorized access to restricted operations by using a user with a username tha publicly available patches.
CVE-2026-24147	NVIDIA Triton Inference Server contains a vulnerability in triton server where an attacker may cause an information disclosure by uploading a model configuration. service.
CVE-2026-5338	A security vulnerability has been detected in Tenda G103 1.0.0.5. The affected element is the function action_set_system_settings of the file system.lua of the com injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.
CVE-2026-3774	The application allows PDF JavaScript and document/print actions (such as WillPrint/DidPrint) to update form fields, annotations, or optional content groups (OCGs) updates are not fully covered by the existing redaction, encryption, and printing logic, which, under specific document structures and user workflows, may cause a or result in printed output that slightly differs from what was reviewed on screen.
CVE-2026-35404	Open edX Platform enables the authoring and delivery of online learning at any scale. he view_survey endpoint accepts a redirect_url GET parameter that is passed survey name is provided, the server issues an immediate HTTP 302 redirect to the attacker-controlled URL. Additionally, the same unvalidated URL is embedded in client-side JavaScript performs location.href = url. This enables phishing and credential theft attacks against authenticated Open edX users. This vulnerability is fix
CVE-2026-34773	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to versions 38.8.6, 39.8.1, 40.8.1, and 41.0.0, on Win before writing to the registry. Apps that pass untrusted input as the protocol name may allow an attacker to write to arbitrary subkeys under HKCU\Software\Classe app.setAsDefaultProtocolClient() with a protocol name derived from external or untrusted input. Apps that use a hardcoded protocol name are not affected. This iss
CVE-2026-27456	util-linux is a random collection of Linux utilities. Prior to version 2.41.4, a TOCTOU (Time-of-Check-Time-of-Use) vulnerability has been identified in the SUID binary validates the source file path with user privileges via fork() + setuid() + realpath(), but subsequently re-canonicalizes and opens it with root privileges (euid=0) wit O_NOFOLLOW, nor inode comparison, nor post-open fstat() are employed. This allows a local unprivileged user to replace the source file with a symlink pointing to and mount it as root. Exploitation requires an /etc/fstab entry with user,loop options whose path points to a directory where the attacker has write permission, and distributions). The impact is unauthorized read access to root-protected files and block devices, including backup images, disk volumes, and any file containing a v
CVE-2026-27101	Dell Secure Connect Gateway (SCG) 5.0 Appliance and Application version(s) 5.28.00.xx to 5.32.00.xx, contain(s) an Improper Limitation of a Pathname to a Restric management network could potentially exploit this vulnerability, leading to remote execution.
CVE-2026-5576	A flaw has been found in SourceCodester/jkev Record Management System 1.0. Affected by this issue is some unknown functionality of the file save_emp.php of th Remote exploitation of the attack is possible. The exploit has been published and may be used.
CVE-2026-5339	A vulnerability was detected in Tenda G103 1.0.0.5. The impacted element is the function action_set_net_settings of the file gpon.lua of the component Setting Har authLoid/authLoidPassword/authPassword/authSerialNo/authType/oltType/usVlanId/usVlanPriority results in command injection. It is possible to initiate the attack r
CVE-2026-5417	A vulnerability was determined in Dataease SQLbot up to 1.6.0. This issue affects the function get_es_data_by_http of the file backend/apps/db/es_engine.py of the server-side request forgery. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 1.7.0 is capabl was contacted early about this disclosure.
CVE-2026-34561	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 Settings – Social Media Management. Multiple configuration fields, including Social Media and Social Media Link, accept attacker-controlled input that is stored serv patched in version 0.31.0.0.
CVE-2026-34562	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 Settings – Company Information. Several administrative configuration fields accept attacker-controlled input that is stored server-side and later rendered without p
CVE-2025-67807	The login mechanism of Sage DPW 2025_06_004 displays distinct responses for valid and invalid usernames, allowing enumeration of existing accounts in versions versions.
CVE-2026-34446	Open Neural Network Exchange (ONNX) is an open standard for machine learning interoperability. Prior to version 1.21.0, there is an issue in onnx.load, the code c a hardlink looks exactly like a regular file on the filesystem. This issue has been patched in version 1.21.0.
CVE-2026-5331	A vulnerability was determined in OpenCart 4.1.0.3. This affects an unknown part of the file installer.php of the component Extension Installer Page. Executing a m exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-5469	A weakness has been identified in Casdoor 2.356.0. This vulnerability affects unknown code of the component Webhook URL Handler. Executing a manipulation ca was contacted early about this disclosure but did not respond in any way.
CVE-2026-34847	hoppscotch is an open source API development ecosystem. Prior to version 2026.3.0, the /enter page contains a DOM-based open redirect vulnerability. The redire proper validation. This issue has been patched in version 2026.3.0.
CVE-2026-5476	A vulnerability was identified in NASA cFS up to 7.0.0 on 32-bit. Affected is the function CFE_TBL_ValidateCodecLoadSize of the file cfe/modules/tbl/fsw/src/cfe_tbl_p attack is rather high. The exploitability is told to be difficult. A fix is planned for the upcoming version milestone of the project.
CVE-2026-30613	An information disclosure vulnerability exists in AZIOT 1 Node Smart Switch (16amp)- WiFi/Bluetooth Enabled Software Version: 1.1.9 due to improper access contr UART interface and obtain sensitive information from the serial console without authentication.
CVE-2026-5473	A vulnerability has been found in NASA cFS up to 7.0.0. The impacted element is the function pickle.load of the component Pickle Module. Such manipulation leads high level of complexity. The exploitability is regarded as difficult. The exploit has been disclosed to the public and may be used. The project was informed of the p
CVE-2026-	UTT Aggressive HiPER 810G v3v1.7.7-171114 was discovered to contain a buffer overflow in the notes parameter of the formGroupConfig function. This vulnerabilit

31060	
CVE-2026-31066	UTT Aggressive HiPER 810G v3v1.7.7-171114 was discovered to contain a buffer overflow in the selDateType parameter of the formTaskEdit function. This vulneral
CVE-2026-31058	UTT Aggressive HiPER 1200GW v2.5.3-170306 was discovered to contain a buffer overflow in the timeRangeName parameter of the formConfigDnsFilterGlobal func crafted input.
CVE-2026-31061	UTT Aggressive HiPER 810G v3v1.7.7-171114 was discovered to contain a buffer overflow in the timestart parameter of the ConfigAdvideo function. This vulnerabil
CVE-2026-31062	UTT Aggressive 520W v3v1.7.7-180627 was discovered to contain a buffer overflow in the filename parameter of the formFtpServerDirConfig function. This vulnera
CVE-2026-31063	UTT Aggressive HiPER 1200GW v2.5.3-170306 was discovered to contain a buffer overflow in the pools parameter of the formArpBindConfig function. This vulnerab
CVE-2026-31065	UTT Aggressive 520W v3v1.7.7-180627 was discovered to contain a buffer overflow in the addCommand parameter of the formConfigCliForEngineerOnly function. input.
CVE-2026-28265	PowerStore, contains a Path Traversal vulnerability in the Service user. A low privileged attacker with local access could potentially exploit this vulnerability, leadin
CVE-2026-34726	Copier is a library and CLI app for rendering project templates. Prior to version 9.14.1, Copier's _subdirectory setting is documented as the subdirectory to use as th traversal such as .. and uses it directly when selecting the template root. As a result, a template can escape its own directory and make Copier render files from th
CVE-2026-5383	An issue that could allow access to Explorer groups from outside of the authorized organization scope has been resolved. This is an instance of CWE-863: Incorrect CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:L/A:L (4.4 Medium). This issue was fixed in version 4.0.260208.0 of the runZero Explorer.
CVE-2026-5625	A weakness has been identified in assafelovic gpt-researcher up to 3.4.3. This issue affects some unknown processing of the file gpt_researcher/skills/researcher.py task can lead to cross site scripting. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. The pr responded yet.
CVE-2026-5542	A vulnerability was determined in code-projects Simple Laundry System 1.0. Impacted is an unknown function of the file /modstaffinfo.php of the component Param scripting. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.
CVE-2026-3831	The Database for Contact Form 7, WPforms, Elementor forms plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check o makes it possible for authenticated attackers, with Contributor-level access and above, to extract all form submissions - including names, emails, phone numbers.
CVE-2026-5321	A flaw has been found in vanna-ai vanna up to 2.0.2. Affected by this issue is some unknown functionality of the component FastAPI/Flask Server. Executing a man attack can be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in ar
CVE-2026-35411	Directus is a real-time API and App dashboard for managing SQL database content. Prior to 11.16.1, Directus is vulnerable to an open redirect via the redirect quer configured Two-Factor Authentication (2FA) visits a crafted URL, they are presented with the legitimate Directus 2FA setup page. After completing the setup proces redirect parameter without any validation. This vulnerability could be used in phishing attacks targeting Directus administrators, as the initial interaction occurs on
CVE-2026-5240	A security vulnerability has been detected in code-projects BloodBank Managing System 1.0. This affects an unknown part of the file /admin_state.php. The manipu the attack remotely. The exploit has been disclosed publicly and may be used.
CVE-2026-5671	A vulnerability was determined in Cyber-III Student-Management-System up to 1a938fa61e9f735078e9b291d2e6215b4942af3f. Impacted is an unknown function o Deletion Endpoint. Executing a manipulation of the argument batch can lead to cross site scripting. The attack can be launched remotely. The exploit has been pub information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded
CVE-2019-25682	CMSsite 1.0 contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized administrative actions by crafting malicious HTML form submit POST requests to the users.php endpoint with parameters like source=add_user, source=edit_user, or del=1 to create, modify, or delete admin accounts.
CVE-2026-5541	A vulnerability was found in code-projects Simple Laundry System 1.0. This issue affects some unknown processing of the file /modmemberinfo.php of the compon cross site scripting. The attack may be initiated remotely. The exploit has been made public and could be used.
CVE-2026-2826	The Kadence Blocks — Page Builder Toolkit for Gutenberg Editor plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.6. capability in the `process_pattern` REST API endpoint. This makes it possible for authenticated attackers, with contributor level access and above, to upload image downloads and creates as media attachments.
CVE-2026-5255	A vulnerability was detected in code-projects Simple Laundry System 1.0. This affects an unknown part of the file /delstaffinfo.php of the component Parameter Ha attack may be launched remotely. The exploit is now public and may be used.
CVE-2026-35462	Papra is a minimalistic document management and archiving platform. Prior to 26.4.0, API keys with an expiresAt date are never validated against the current time indefinitely, allowing a user whose key has expired to continue accessing all protected endpoints as if the key were still valid. This vulnerability is fixed in 26.4.0.
CVE-2026-	A flaw has been found in assafelovic gpt-researcher up to 3.4.3. The impacted element is an unknown function of the file backend/server/app.py of the component carried out 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 respond

5630	
CVE-2026-35460	Papra is a minimalistic document management and archiving platform. Prior to 26.4.0, transactional email templates in Papra interpolate user.name directly into H containing HTML tags will have those tags injected into the verification and password reset email bodies. Since emails are sent from the legitimate domain (e.g: au from official Papra notifications. This vulnerability is fixed in 26.4.0.
CVE-2026-5313	A vulnerability has been found in Nothings stb up to 2.30. This issue affects the function stbi__gif_load_next in the library stb_image.h of the component GIF Decod 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.
CVE-2026-5319	A security vulnerability has been detected in itsourcecode Payroll Management System up to 1.0. Affected is an unknown function of the file /navbar.php. Such ma the attack remotely. The exploit has been disclosed publicly and may be used.
CVE-2026-5615	A weakness has been identified in givanz Vvvebjs up to 2.0.5. The affected element is an unknown function of the file upload.php of the component File Upload Enc scripting. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. Patch name: 8cac22cff99b this issue. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.
CVE-2026-22662	prompts.chat prior to commit 1464475 contains a blind server-side request forgery vulnerability in the Wiro media generator that allows authenticated users to per exploit this vulnerability by sending POST requests to the /api/media-generate endpoint to probe internal networks, access internal services, and exfiltrate data thr
CVE-2026-5624	A security flaw has been discovered in ProjectSend r2002. This vulnerability affects unknown code of the file upload.php. Performing a manipulation results in cross released to the public and may be used for attacks. Upgrading to version r2029 is able to resolve this issue. The patch is named 2c0d25824ab571b6c219ac1a188a
CVE-2026-5572	A security flaw has been discovered in Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30. This affects an unknown function. Performing a manipulation results in cro 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.
CVE-2026-5539	A flaw has been found in code-projects Simple Laundry System 1.0. This affects an unknown part of the file /modifymember.php of the component Parameter Hand attack can be initiated remotely. The exploit has been published and may be used.
CVE-2026-5467	A vulnerability was identified in Casdoor 2.356.0. Affected by this issue is some unknown functionality of the component OAuth Authorization Request Handler. Suc launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any wa
CVE-2026-5318	A weakness has been identified in LibRaw up to 0.22.0. This impacts the function HuffTable::initval of the file src/decompressors/losslessjpeg.cpp of the component write. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 0.22.1 wil advisable to upgrade the affected component.
CVE-2016-20054	Nodcms contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized administrative actions by crafting malicious forms. Attack admin/user_manipulate and admin/settings/generall endpoints to create users or modify application settings without explicit consent.
CVE-2026-33227	Improper validation and restriction of a classpath path name vulnerability in Apache ActiveMQ Client, Apache ActiveMQ Broker, Apache ActiveMQ All. In two instanc console) an authenticated user provided "key" value could be constructed to traverse the classpath due to path concatenation. As a result, the application is expos together with another attack to lead to exploit.This issue affects Apache ActiveMQ Client: before 5.19.3, from 6.0.0 before 6.2.2; Apache ActiveMQ Broker: before 5 6.2.2. Users are recommended to upgrade to version 5.19.4 or 6.2.3, which fixes the issue. Note: 5.19.3 and 6.2.2 also fix this issue, but that is limited to non-Wind
CVE-2026-5529	A vulnerability was detected in Dromara lamp-cloud up to 5.8.1. This vulnerability affects the function pageUser of the file /defUser/pageUser of the component De attack can be initiated remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not res
CVE-2026-5314	A vulnerability was found in Nothings stb up to 1.26. Impacted is the function stbtt_InitFont_internal in the library stb_truetype.h of the component TTF File Handler 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.
CVE-2026-35181	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the player skin configuration endpoint at admin/playerUpdate.json.php does not validat security check via ignoreTableSecurityCheck(), removing the only other layer of defense. Combined with SameSite=None cookies, a cross-origin POST can modify t
CVE-2026-35180	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the site customization endpoint at admin/customize_settings_nativeUpdate.json.php lac domain-based security check executes. Combined with SameSite=None cookie policy, a cross-origin POST can overwrite the platform's logo with attacker-controlle
CVE-2026-31150	Incorrect access control in Kaleris YMS v7.2.2.1 allows authenticated attackers with only the shipping/receiving role to view the truck's dashboard resources.
CVE-2026-5533	A vulnerability was determined in badlogic pi-mono 0.58.4. The impacted element is an unknown function of the file packages/web-ui/src/tools/artifacts/SvgArtifact scripting. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disc
CVE-2026-39395	Cosign provides code signing and transparency for containers and binaries. Prior to 3.0.6 and 2.6.3, cosign verify-blob-attestation may erroneously report a "Verifie For old-format bundles and detached signatures, this was due to a logic flaw in the error handling of the predicate type validation. For new-format bundles, the pre 2.6.3.
CVE-2026-4989	Improper input validation in the gateway health check feature in Devolutions Server allows a low-privileged authenticated user to perform server-side request forg issue affects Server: from 2026.1.1 through 2026.1.11, from 2025.3.1 through 2025.3.17.
CVE-2026-5315	A vulnerability was determined in Nothings stb up to 1.26. The affected element is the function stbtt__buf_get8 in the library stb_truetype.h of the component TTF I be executed remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in an
CVE-2026-	In sec boot, there is a possible out of bounds write due to an integer overflow. This could lead to local denial of service, if an attacker has physical access to the de

20446	exploitation. Patch ID: ALPS09963054; Issue ID: MSV-3899.
CVE-2026-5316	A vulnerability was identified in Nothings stb up to 1.22. The impacted element is the function setup_free of the file stb_vorbis.c. The manipulation leads to allocati publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-5535	A security flaw has been discovered in FedML-AI FedML up to 0.8.9. This impacts an unknown function of the file FileUtils.java of the component MQTT Message Ha attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this d
CVE-2026-28736	** UNSUPPORTED WHEN ASSIGNED ** Focalboard version 8.0 fails to validate file ownership when serving uploaded files. This allows an authenticated attacker wh standalone product is not maintained and no fix will be issued.
CVE-2026-5705	A vulnerability was identified in code-projects Online Hotel Booking 1.0. Affected by this vulnerability is an unknown functionality of the file /booknow.php of the co cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used.
CVE-2026-4820	IBM Maximo Application Suite 9.1, 9.0, 8.11, and 8.10 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get th user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic.
CVE-2026-35541	An issue was discovered in Roundcube Webmail before 1.5.14 and 1.6.14. Incorrect password comparison in the password plugin could lead to type confusion that
CVE-2026-35414	OpenSSH before 10.3 mishandles the authorized_keys principals option in uncommon scenarios involving a principals list in conjunction with a Certificate Authority
CVE-2026-32602	Homarr is an open-source dashboard. Prior to 1.57.0, the user registration endpoint (/api/trpc/user.register) is vulnerable to a race condition that allows an attacke performs three sequential database operations without a transaction: CHECK, CREATE, and DELETE. Because these operations are not atomic, concurrent requests This allows multiple accounts to be registered using a single invite token that was intended to be single-use. This vulnerability is fixed in 1.57.0.
CVE-2026-35177	Vim is an open source, command line text editor. Prior to 9.2.0280, a path traversal bypass in Vim's zip.vim plugin allows overwriting of arbitrary files when openin This vulnerability is fixed in 9.2.0280.
CVE-2025-36373	IBM DataPower Gateway 10.6CD 10.6.1.0 through 10.6.5.0 and IBM DataPower Gateway 10.5.0 10.5.0.0 through 10.5.0.20 and IBM DataPower Gateway 10.6.0 10. information from other domains to an administrative user.
CVE-2026-39314	OpenPrinting CUPS is an open source printing system for Linux and other Unix-like operating systems. In versions 2.4.16 and prior, an integer underflow vulnerabili crash the cupsd root process by supplying a negative job-password-supported IPP attribute. The bounds check only caps the upper bound, so a negative value pass argument to memset() on a 33-byte stack buffer. This causes an immediate SIGSEGV in the cupsd root process. Combined with systemd's Restart=on-failure, an at
CVE-2026-21767	HCL BigFix Platform is affected by insufficient authentication. The application might allow users to access sensitive areas of the application without proper authent
CVE-2026-2625	A flaw was found in rust-rpm-sequoia. An attacker can exploit this vulnerability by providing a specially crafted Red Hat Package Manager (RPM) file. During the RP signature parsing code, leading to an unconditional termination of the rpm process. This issue results in an application level denial of service, making the system u
CVE-2026-39316	OpenPrinting CUPS is an open source printing system for Linux and other Unix-like operating systems. In versions 2.4.16 and prior, a use-after-free vulnerability ex cupsdDeleteTemporaryPrinters() in scheduler/printers.c calls cupsdDeletePrinter() without first expiring subscriptions that reference the printer, leaving cupsd_subs subsequently dereferenced at multiple code sites, causing a crash (denial of service) of the cupsd daemon. With heap grooming, this can be leveraged for code ex
CVE-2026-34768	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to versions 38.8.6, 39.8.1, 40.8.0, and 41.0.0-beta.8, path to the Run registry key without quoting. If the app is installed to a path containing spaces, an attacker with write access to an ancestor directory may be able default Windows install, standard system directories are protected against writes by standard users, so exploitation typically requires a non-standard install locatio
CVE-2026-5682	A vulnerability has been found in Meesho Online Shopping App up to 27.3 on Android. Affected is an unknown function of the file /api/endpoint of the component co attack may be performed from remote. The attack requires a high level of complexity. The exploitability is told to be difficult. The exploit has been disclosed to the
CVE-2026-5360	A vulnerability has been found in Free5GC 4.2.0. The affected element is an unknown function of the component aper. Such manipulation leads to type confusion. T The exploitability is described as difficult. The exploit has been disclosed to the public and may be used. The name of the patch is 26205eb01705754b7b902ad6c4
CVE-2026-35537	An issue was discovered in Roundcube Webmail before 1.5.14 and 1.6.14. Unsafe deserialization in the redis/memcache session handler may lead to arbitrary file v
CVE-2025-67806	The login mechanism of Sage DPW 2021_06_004 displays distinct responses for valid and invalid usernames, allowing enumeration of existing accounts in versions versions.
CVE-2026-37977	A flaw was found in Keycloak. A remote attacker can exploit a Cross-Origin Resource Sharing (CORS) header injection vulnerability in Keycloak's User-Managed Acc supplied JSON Web Token (JWT) is used to set the `Access-Control-Allow-Origin` header before the JWT signature is validated. When a specially crafted JWT with an origin, even if the grant is later rejected. This can lead to the exposure of low-sensitivity information from authorization server error responses, weakening origin is
CVE-2026-3184	A flaw was found in util-linux. Improper hostname canonicalization in the `login(1)` utility, when invoked with the `-h` option, can modify the supplied remote hostn specially crafted hostname, potentially bypassing host-based Pluggable Authentication Modules (PAM) access control rules that rely on fully qualified domain name
CVE-2026-	Rack is a modular Ruby web server interface. Prior to versions 2.2.23, 3.1.21, and 3.2.6, Rack::Multipart::Parser extracts the boundary parameter from multipart/fo multiple boundary parameters, Rack selects the last one rather than the first. In deployments where an upstream proxy, WAF, or intermediary interprets the first b

26961	past upstream inspection and have Rack parse a different body structure than the intermediary validated. This issue has been patched in versions 2.2.23, 3.1.21, a
CVE-2026-5413	A vulnerability was identified in Newgen OmniDocs up to 12.0.00. Affected by this vulnerability is an unknown functionality of the file /omnidocs/GetWebApiConfigu disclosure. The attack is possible to be carried out remotely. The attack is considered to have high complexity. The exploitation appears to be difficult. The exploit disclosure but did not respond in any way.
CVE-2026-35448	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the BlockonomicsYPT plugin's check.php endpoint returns payment order data for any E AJAX polling helper for the authenticated invoice.php page, but it performs no access control checks of its own. Since Bitcoin addresses are publicly visible on the b platform.
CVE-2026-5622	A vulnerability was determined in hcengineering Huly Platform 0.7.382. Affected by this issue is some unknown functionality of the file foundations/core/packages/t argument SERVER_SECRET with the input secret causes use of hard-coded cryptographic key . The attack can be initiated remotely. The attack is considered to hav early about this disclosure but did not respond in any way.
CVE-2026-35386	In OpenSSH before 10.3, command execution can occur via shell metacharacters in a username within a command line. This requires a scenario where the usernar % in ssh_config.
CVE-2026-5370	A vulnerability was identified in krayin laravel-crm up to 2.2. Impacted is the function composeMail of the file packages/Webkul/Admin/tests/e2e-pw/tests/mail/inbo cross site scripting. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The identifier of the patch is 73ed28d466bf14
CVE-2026-5254	A security vulnerability has been detected in welovemedia FFmate up to 2.0.15. Affected by this issue is some unknown functionality of the file /ui/app/components cross site scripting. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disc
CVE-2026-5468	A security flaw has been discovered in Casdoor 2.356.0. This affects the function dangerouslySetInnerHTML. Performing a manipulation of the argument formCss/fc 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
CVE-2026-5325	A vulnerability was determined in SourceCodester Simple Customer Relationship Management System 1.0. This issue affects some unknown processing of the file / Description causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.
CVE-2026-5253	A weakness has been identified in bufanyun HotGo 1.0/2.0. Affected by this vulnerability is an unknown functionality of the file /web/src/layout/components/Header lead to cross site scripting. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. The vendor was
CVE-2026-5332	A vulnerability was identified in Xiaopi Panel 1.0.0. This vulnerability affects unknown code of the file /demo.php of the component WAF Firewall. The manipulation is possible. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-5568	A vulnerability has been found in Akaunting up to 3.1.21. This issue affects some unknown processing of the component Invoice/Billing. The manipulation of the arg 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.
CVE-2026-35679	Zcash zcashd before 6.12.0 allows invalid transactions to be accepted under certain conditions, which potentially could have resulted in the draining of user funds
CVE-2026-5249	A vulnerability was found in gougucms 4.08.18. This impacts an unknown function of the file \gougucms-master\app\admin\view\user\record.html of the componen cross site scripting. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this di
CVE-2026-5252	A security flaw has been discovered in z-9527 admin 1.0/2.0. Affected is an unknown function of the file /server/routes/message.js of the component Message Crea 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 re
CVE-2026-33404	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. From 6.0 to before 6.5, client hostnam escaping in network.js (Network page) and charts.js/index.js (Dashboard chart tooltips). While upstream validation in dnsmasq and FTL blocks HTML characters via with other fields in the same file that are properly escaped. This vulnerability is fixed in 6.5.
CVE-2026-5456	A vulnerability was identified in Align Technology My Invisalign App 3.12.4 on Android. The impacted element is an unknown function of the file com/aligntech/myir manipulation of the argument CDAACCESS_TOKEN leads to use of hard-coded cryptographic key . The attack must be carried out locally. The exploit is publicly ava not respond in any way.
CVE-2026-5453	A vulnerability has been found in Rico só vantagem pra investir App up to 4.58.32.12421 on Android. This issue affects some unknown processing of the file br/com Such manipulation of the argument SEGMENT_WRITE_KEY leads to use of hard-coded cryptographic key . The attack can only be performed from a local environme contacted early about this disclosure but did not respond in any way.
CVE-2026-35094	A flaw was found in libinput. An attacker capable of deploying a Lua plugin file in specific system directories can exploit a dangling pointer vulnerability. This occurs be printed to system logs. This could potentially expose sensitive data if the memory location is re-used, leading to information disclosure. For this exploit to work,
CVE-2026-5455	A vulnerability was determined in Dialogue App up to 4.3.2 on Android. The affected element is an unknown function of the file file res/raw/config.json of the compo SEGMENT_WRITE_KEY can lead to use of hard-coded cryptographic key . The attack is restricted to local execution. The exploit has been publicly disclosed and may in any way.
CVE-2026-5462	A vulnerability was identified in Wahoo Fitness SYSTM App up to 7.2.1 on Android. Impacted is an unknown function of the file com/WahooFitness/SYSTM/BuildConfi argument SEGMENT_WRITE_KEY leads to use of hard-coded cryptographic key . Local access is required to approach this attack. The exploit is publicly available an respond in any way.
CVE-2026-5457	A security flaw has been discovered in PropertyGuru AgentNet Singapore App up to 23.7.10 on Android. This affects an unknown function of the file com/allproperty com.allproperty.android.agentnet. The manipulation of the argument SEGMENT_ANDROID_WRITE_KEY/SEGMENT_TOS_WRITE_KEY results in use of hard-coded cryp 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.
CVE-2026-	A weakness has been identified in Noelse Individuals & Pro App up to 2.1.7 on Android. This impacts an unknown function of the file com/reactnative/antelop/BuildC SEGMENT_WRITE_KEY causes use of hard-coded cryptographic key . The attack needs to be launched locally. The exploit has been made available to the public and

5458	did not respond in any way.
CVE-2026-5452	A flaw has been found in UCC CampusConnect App up to 14.3.5 on Android. This vulnerability affects unknown code of the file campusconnect/BuildConfig.java of t cryptographic key . The attack can only be executed locally. The exploit has been published and may be used.
CVE-2026-34766	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to versions 38.8.6, 39.8.0, 40.7.0, and 41.0.0-beta.8, filtered list that was presented to the handler. An app whose handler could be influenced to select a device ID outside the filtered set would grant access to a devic The WebUSB security blocklist remained enforced regardless, so security-sensitive devices on the blocklist were not affected. The practical impact is limited to app 39.8.0, 40.7.0, and 41.0.0-beta.8.
CVE-2026-5454	A vulnerability was found in GRID Organiser App up to 1.0.5 on Android. Impacted is an unknown function of the file file res/raw/app.json of the component co.grida use of hard-coded cryptographic key . The attack is only possible with local access. The exploit has been made public and could be used.
CVE-2026-5471	A vulnerability was detected in Investory Toy Planet Trouble App up to 1.5.5 on Android. Impacted is an unknown function of the file assets/google-services-desktop current_key results in use of hard-coded cryptographic key . The attack must be initiated from a local position. The exploit is now public and may be used.
CVE-2025-43236	A type confusion issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7.
CVE-2026-2475	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 throug attacker to conduct phishing attacks, caused by an open redirect vulnerability. An attacker could exploit this vulnerability using a specially crafted request to redire
CVE-2026-35538	An issue was discovered in Roundcube Webmail before 1.5.14 and 1.6.14. Unsanitized IMAP SEARCH command arguments could lead to IMAP injection or CSRF byp
CVE-2026-35387	OpenSSH before 10.3 can use unintended ECDSA algorithms. Listing of any ECDSA algorithm in PubkeyAcceptedAlgorithms or HostbasedAcceptedAlgorithms is mis
CVE-2026-33405	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. From 6.0 to before 6.5, the formatInfo HTML without escaping when a user expands a query row in the Query Log, enabling stored HTML injection. JavaScript execution is blocked by the server's CSP (scr confirming the omission was an oversight. This vulnerability is fixed in 6.5.
CVE-2026-5382	An issue that could expose records outside of the authorized organization scope through the MCP endpoints has been resolved. This is an instance of CWE-863: Inc CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:N/A:N (3.0 Low). This issue was fixed in version 4.0.260206.0 of the runZero Platform.
CVE-2026-5379	An issue that allowed MCP agents to access certificate information from outside of their authorized organization scope has been resolved. This is an instance of CW CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:N/A:N (3.0 Low). This issue was fixed in version 4.0.260203.0 of the runZero Platform.
CVE-2026-34781	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.5, 40.8.5, 41.1.0, and 42.0.0-alpha.5, apps tha clipboard contains image data that fails to decode, the resulting null bitmap is passed unchecked to image construction, triggering a controlled abort and crashing read images from the clipboard are not affected. This issue does not allow memory corruption or code execution. This vulnerability is fixed in 39.8.5, 40.8.5, 41.1.0
CVE-2026-34762	Ella Core is a 5G core designed for private networks. Prior to version 1.8.0, the PUT /api/v1/subscriber/{imsi} API accepts an IMSI identifier from both the URL path NetworkManager to modify any subscriber's policy while the audit trail records a fabricated or unrelated subscriber IMSI. This issue has been patched in version 1.8
CVE-2026-4292	An issue was discovered in 6.0 before 6.0.4, 5.2 before 5.2.13, and 4.2 before 4.2.30. Admin changelist forms using `ModelAdmin.list_editable` incorrectly allowed series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Cantina for reporting this issue.
CVE-2025-66487	IBM Aspera Shares 1.9.9 through 1.11.0 does not properly rate limit the frequency that an authenticated user can send emails, which could result in email flooding
CVE-2026-5375	An issue that could allow a user with access to a credential to view sensitive fields through an API response has been resolved. This is an instance of CWE-200: Exp score of CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N (2.7 Low). This issue was fixed in version 4.0.260203.0 of the runZero Platform.
CVE-2026-35388	OpenSSH before 10.3 omits connection multiplexing confirmation for proxy-mode multiplexing sessions.
CVE-2026-5420	A security flaw has been discovered in Shinrays Games Goods Triple App up to 1.200. The affected element is an unknown function of the file jRwTX.java of the cor AES_IV/AES_PASSWORD results in use of hard-coded cryptographic key . Attacking locally is a requirement. The complexity of an attack is rather high. The exploita used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2026-5310	A vulnerability was identified in Enter Software Iperius Backup up to 8.7.2. This impacts an unknown function of the file IperiusAccounts.ini. Such manipulation lead attack is characterized by high complexity. The exploitability is said to be difficult. The exploit is publicly available and might be used. Upgrading to version 8.7.4 w contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.
CVE-2026-5643	A vulnerability was identified in Cyber-III Student-Management-System up to 1a938fa61e9f735078e9b291d2e6215b4942af3f. This impacts an unknown function of manipulation of the argument $_SERVER['PHP_SELF'] leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and r delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but
CVE-2026-5644	A security flaw has been discovered in Cyber-III Student-Management-System up to 1a938fa61e9f735078e9b291d2e6215b4942af3f. Affected is an unknown functi argument $_SERVER['PHP_SELF'] results in cross site scripting. The attack can be initiated remotely. The exploit has been released to the public and may be used f no version details of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet
CVE-	A vulnerability was detected in code-projects Online Shoe Store 1.0. This affects an unknown part of the file /admin/admin_feature.php of the component Add Produ

2026-5647	scripting. The attack may be launched remotely. The exploit is now public and may be used.
CVE-2026-5668	A flaw has been found in Cyber-III Student-Management-System up to 1a938fa61e9f735078e9b291d2e6215b4942af3f. This affects an unknown part of the file /adr $_SERVER['PHP_SELF'] causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been published and may be used. This product is usi affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.
CVE-2026-34764	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. From 33.0.0-alpha.1 to before 39.8.5, 40.8.5, 41.1.0, and 4 vulnerable to a use-after-free. Under certain conditions, the release() callback provided on a paint event texture can outlive its backing native state, and invoking i crash or memory corruption. Apps are only affected if they use offscreen rendering with webPreferences.offscreen: { useSharedTexture: true }. Apps that do not e ensure texture.release() is called promptly after the texture has been consumed, before the texture object becomes unreachable. This vulnerability is fixed in 39.8
CVE-2026-5381	An issue that could expose task information outside of the authorized organization scope has been resolved. This is an instance of CWE-863: Incorrect Authorizatio (2.2 Low). This issue was fixed in version 4.0.260205.0 of the runZero Platform.
CVE-2026-27949	Plane is an an open-source project management tool. Prior to 1.3.0, a vulnerability was identified in Plane's authentication flow where a user's email address is incl magic code is submitted). Transmitting personally identifiable information (PII) via GET request query strings is classified as an insecure design practice. The affect (packages/utils/src/auth.ts). This vulnerability is fixed in 1.3.0.
CVE-2026-32588	Authenticated DoS over CQL in Apache Cassandra 4.0, 4.1, 5.0 allows authenticated user to raise query latencies via repeated password changes. Users are recom
CVE-2026-27315	Sensitive Information Leak in cqlsh in Apache Cassandra 4.0 allows access to sensitive information, like passwords, from previously executed cqlsh command via ~ version 4.0.20, which fixes this issue. -- Description: Cassandra's command-line tool, cqlsh, provides a command history feature that allows users to recall previous in the ~/.cassandra/cqlsh_history file in the user's home directory. However, cqlsh does not redact sensitive information when saving command history. This means users) within cqlsh, these passwords are permanently stored in cleartext in the history file on the disk.
CVE-2026-23459	In the Linux kernel, the following vulnerability has been resolved: ip_tunnel: adapt iptunnel_xmit_stats() to NETDEV_PCPU_STAT_DSTATS Blamed commits forgot th iptunnel_xmit_stats() was assuming tunnels were only using NETDEV_PCPU_STAT_TSTATS. @syncp offset in pcpu_sw_netstats and pcpu_dstats is different. 32bit ke This patch also moves pcpu_stat_type closer to dev->{t,d}stats to avoid a potential cache line miss since iptunnel_xmit_stats() needs to read it.
CVE-2026-23458	In the Linux kernel, the following vulnerability has been resolved: netfilter: ctnetlink: fix use-after-free in ctnetlink_dump_exp_ct() ctnetlink_dump_exp_ct() stores a ctnetlink_exp_ct_dump_table(), but drops the conntrack reference immediately after netlink_dump_start(). When the dump spans multiple rounds, the second recv nfct_help(ct), leading to a use-after-free on ct->ext. The bug is that the netlink_dump_control has no .start or .done callbacks to manage the conntrack reference a ctnetlink_get_conntrack) properly use .start/.done callbacks for this purpose. Fix this by adding .start and .done callbacks that hold and release the conntrack refer early-return check in the dump callback to avoid dereferencing ct->ext unnecessarily. BUG: KASAN: slab-use-after-free in ctnetlink_exp_ct_dump_table+0x4f/0x2e(133 Comm: ctnetlink_poc Not tainted 7.0.0-rc2+ #3 PREEMPTLAZY Call Trace: <TASK> ctnetlink_exp_ct_dump_table+0x4f/0x2e0 netlink_dump+0x333/0x880 netl Allocated by task 133: kmem_cache_alloc_noprof+0x134/0x440 __nf_conntrack_alloc+0xa8/0x2b0 ctnetlink_create_conntrack+0xa1/0x900 ctnetlink_new_conntrac nfnetlink_rcv+0xdb/0x220 netlink_unicast+0x3ec/0x590 netlink_sendmsg+0x397/0x690 __sys_sendmsg+0xf4/0x180 Freed by task 0: slab_free_after_rcu_debug+
CVE-2026-39324	Rack::Session is a session management implementation for Rack. From 2.0.0 to before 2.1.2, Rack::Session::Cookie incorrectly handles decryption failures when cc default decoder instead of rejecting the cookie. This allows an unauthenticated attacker to supply a crafted session cookie that is accepted as valid session data wi session state, an attacker can manipulate session contents and potentially gain unauthorized access. This vulnerability is fixed in 2.1.2.
CVE-2026-39321	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.8.0-alpha.6 and 8.6.74, he login endpoint respor exists in the database. When a user is not found, the server responds immediately. When a user exists but the password is wrong, a bcrypt comparison runs first, a enumerate valid usernames. This vulnerability is fixed in 9.8.0-alpha.6 and 8.6.74.
CVE-2026-23460	In the Linux kernel, the following vulnerability has been resolved: net/rose: fix NULL pointer dereference in rose_transmit_link on reconnect syzkaller reported a bug values: TCP_CLOSE, TCP_LISTEN, TCP_SYN_SENT, and TCP_ESTABLISHED. rose_connect() already rejects calls for TCP_ESTABLISHED (-EISCONN) and TCP_CLOSE wit rose_connect() is called a second time while the first connection attempt is still in progress (TCP_SYN_SENT), it overwrites rose->neighbour via rose_get_neigh(). If >neighbour == NULL. When the socket is subsequently closed, rose_release() sees ROSE_STATE_1 and calls rose_write_internal() -> rose_transmit_link(skb, NULL), connection is already in progress should return -EALREADY. Add this missing check for TCP_SYN_SENT to complete the state validation in rose_connect(). [1] https:/ https://gist.github.com/mrpre/9e6779e0d13e2c66779b1653fef80516
CVE-2026-21630	Improperly built order clauses lead to a SQL injection vulnerability in the articles webservice endpoint.
CVE-2026-23456	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_h323: fix OOB read in decode_int() CONS case In decode_int(), the CONS c checking that len bytes remain in the buffer. The existing boundary check only validates the 2 bits for get_bits(), not the subsequent 1-4 bytes that get_uint() reads read. Add a boundary check for len bytes after get_bits() and before get_uint().
CVE-2025-70844	yaffa v2.0.0 is vulnerable to Cross Site Scripting (XSS). An attacker can inject malicious JavaScript into the "Add Account Group" function on the account-group pag page.
CVE-2026-21629	The ajax component was excluded from the default logged-in-user check in the administrative area. This behavior was potentially unexpected by 3rd party develop
CVE-2026-23457	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_sip: fix Content-Length u32 truncation in sip_help_tcp() sip_help_tcp() pars but stores the result in unsigned int clen. On 64-bit systems, values exceeding UINT_MAX are silently truncated before computing the SIP message boundary. For e parser to miscalculate where the current message ends. The loop then treats trailing data in the TCP segment as a second SIP message and processes it through th simple_strtoul(), and reject Content-Length values that exceed the remaining TCP payload length.
CVE-2026-21632	Lack of output escaping for article titles leads to XSS vectors in various locations.
CVE-2024-36058	The Send Basket functionality in Koha Library before 23.05.10 is susceptible to Time-Based SQL Injection because it fails to sanitize the POST parameter bib_list in database.
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_h323: check for zero length in DecodeQ931() In DecodeQ931(), the UserUs the protocol discriminator byte before passing it to DecodeH323_UserInformation(). If the encoded length is 0, the decrement wraps to -1, which is then passed as

23455	len is positive after the decrement.
CVE-2026-33709	JupyterHub is software that allows one to create a multi-user server for Jupyter notebooks. Prior to version 5.4.4, an open redirect vulnerability in JupyterHub allows page, after which they are sent to an arbitrary attacker-controlled site outside JupyterHub instead of a JupyterHub page, bypassing JupyterHub's check to prevent t
CVE-2026-5359	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this car
CVE-2026-25044	Budibase is an open-source low-code platform. Prior to version 3.33.4, the bash automation step executes user-provided commands using execSync without proper allows template interpolation, potentially allowing arbitrary command execution. This issue has been patched in version 3.33.4.
CVE-2026-23409	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix differential encoding verification Differential encoding allows loops to be created if terminates. Unfortunately the differential encode verification had two bugs. 1. it conflated states that had gone through check and already been marked, with state chain being verified are treated as a chain that has already been verified. 2. the order bailout on already checked states compared current chain check iterators j,k current chain verification was being mistaken for moving to an already verified state. Move to a double mark scheme where already verified states get a different m verification check that was the cause of the second error as any already verified state is already marked.
CVE-2026-23405	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix: limit the number of levels of policy namespaces Currently the number of policy nar namespaces aren't strictly tied to user namespaces and it is possible to create them and nest them arbitrarily deep which can be used to exhaust system resource
CVE-2026-4931	Smart contract Marginal v1 performs unsafe downcast, allowing attackers to settle a large debt position for a negligible asset cost.
CVE-2026-21631	Lack of output escaping leads to a XSS vector in the multilingual associations component.
CVE-2026-35615	PraisonAI is a multi-agent teams system. Prior to 1.5.113, _validate_path() calls os.path.normpath() first, which collapses .. sequences, then checks for '..' in norma completely useless and allows trivial path traversal to any file on the system. This vulnerability is fixed in 1.5.113.
CVE-2026-23898	Lack of input validation leads to an arbitrary file deletion vulnerability in the autoupdate server mechanism.
CVE-2026-23461	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix use-after-free in l2cap_unregister_user After commit ab4eedb790ca ("Bluet protect access to conn->users. However, l2cap_register_user() and l2cap_unregister_user() don't use conn->lock, creating a race condition where these functions c lead to use-after-free and list corruption bugs, as reported by syzbot. Fix this by changing l2cap_register_user() and l2cap_unregister_user() to use conn->lock inste
CVE-2026-35614	Frappe is a full-stack web application framework. Prior to 16.14.0 and 15.104.0, Frappe has a SQL injection in bulk_update. This vulnerability is fixed in 16.14.0 and
CVE-2026-23467	In the Linux kernel, the following vulnerability has been resolved: drm/i915/dmc: Fix an unlikely NULL pointer deference at probe intel_dmc_update_dc6_allowed_co the case when the call path is intel_power_domains_init_hw() -> {skl,bxt,icl}_display_core_init() -> gen9_set_dc_state() -> intel_dmc_update_dc6_allowed_count(), gen9_set_dc_state() calls intel_dmc_update_dc6_allowed_count() conditionally, depending on the current and target DC states. At probe, the target is disabled, but unlikely that DC6 is enabled at probe, as we haven't seen this failure mode before. It is also strange to have DC6 enabled at boot, since that would require the DMC stopping / reprogramming the firmware is a poorly specified sequence and as such unlikely an intentional BIOS behaviour. It's more likely that BIOS is leaving an un DMC firmware for this). The tracking of the DC6 allowed counter only works if starting / stopping the counter depends on the _SW_ DC6 state vs. the current _HW_ counter was started). Thus, using the HW DC6 state is incorrect and it also leads to the above oops. Fix both issues by using the SW DC6 state for the tracking. This below. (cherry picked from commit 2344b93af8eb5da5d496b4e0529d35f0f559eaf0)
CVE-2026-23466	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Open-code GGTT MMIO access protection GGTT MMIO access is currently protected by ho is later unbound or unloaded. However, if driver load fails, this protection is insufficient because drm_dev_unplug() is never called. Additionally, devm release funct GGTT MMIO region is removed, as some BOs may be freed asynchronously by worker threads. To address this, introduce an open-coded flag, protected by the GGT devm release function to ensure MMIO access is disabled once teardown begins. (cherry picked from commit 4f3a998a173b4325c2efd90bdadc6ccd3ad9a431)
CVE-2026-23404	In the Linux kernel, the following vulnerability has been resolved: apparmor: replace recursive profile removal with iterative approach The profile removal code use and system crashes. Reproducer: $ pf='a'; for ((i=0; i<1024; i++)); do echo -e "profile $pf { \n }" \| apparmor_parser -K -a; pf="$pf//x"; done $ echo -n a > /sys/ker approach with an iterative approach in __remove_profile(). The function repeatedly finds and removes leaf profiles until the entire subtree is removed, maintaining
CVE-2026-23465	In the Linux kernel, the following vulnerability has been resolved: btrfs: log new dentries when logging parent dir of a conflicting inode If we log the parent director we finish we have the parent directory's inode marked as logged but we did not log its new dentries. As a consequence if the parent directory is explicitly fsynced l after a power failure the new dentries are missing. Example scenario: $ mkdir foo $ sync $rmdir foo $ mkdir dir1 $ mkdir dir2 # A file with the same name and pare deleted directory's # inode is a conflicting inode of this new file's inode. $ touch foo $ ln foo dir2/link # The fsync on dir2 will log the parent directory (".") because not log its new dentries (dir1). $ xfs_io -c "fsync" dir2 # This fsync on the parent directory is no-op, since the previous fsync # logged it (but without logging its new this by ensuring we log new dir dentries whenever we log the parent directory of a no longer existing conflicting inode. A test case for fstests will follow soon.
CVE-2026-23468	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Limit BO list entry count to prevent resource exhaustion Userspace can pass an arb multiplication overflow check prevents out-of-bounds allocation, a large number of entries could still cause excessive memory allocation (up to potentially gigabyte per BO list, which is more than sufficient for any realistic use case (e.g., a single list containing all buffers in a large scene). This prevents memory exhaustion attac exceeds the limit (cherry picked from commit 688b87d39e0aa8135105b40dc167d74b5ada5332)
CVE-2026-23469	In the Linux kernel, the following vulnerability has been resolved: drm/imagination: Synchronize interrupts before suspending the GPU The runtime PM suspend cal doesn't wait for it to finish. Depending on timing, the IRQ handler could be running while the GPU is suspended, leading to kernel crashes when trying to access GP runtime PM suspend callback, wait for any IRQ handlers in progress on other CPU cores to finish, by calling synchronize_irq(). At the same time, remove the runtim approach to begin with, and being at the wrong place as they should have wrapped all GPU register accesses, the driver would hit a deadlock between synchronize and the resume callback requiring the same. Example crash signature on a TI AM68 SK platform: [337.241218] SError Interrupt on CPU0, code 0x00000000bf0000 6.17.7-B2C-00005-g9c7bbe4ea16c #2 PREEMPT [337.241246] Tainted: [M]=MACHINE_CHECK [337.241249] Hardware name: Texas Instruments AM68 SK (DT) [3 337.241256] pc : pvr_riscv_irq_pending+0xc/0x24 [337.241277] lr : pvr_device_irq_thread_handler+0x64/0x310 [337.241282] sp : ffff800085b0bd30 [337.24128 337.241291] x26: ffff000806e48f80 x25: ffff0008070d9eac x24: 0000000000000000 [337.241296] x23: ffff0008068e9bf0 x22: ffff0008068e9bd0 x21: ffff800085b 0000000000000001 [337.241305] x17: 637365645f656c70 x16: 0000000000000000 x15: ffff000b7df9ff40 [337.241310] x14: 0000a585fe3c0d0e x13: 0000009 0000000000000af0 x9 : ffff800085b0bd00 [337.241318] x8 : ffff0008071175d0 x7 : 000000000000b955 x6 : 0000000000000003 [337.241323] x5 : 0000000000

	ffff800080e39d20 x1 : ffff800080e3fc48 x0 : 0000000000000000 [337.241333] Kernel panic - not syncing: Asynchronous SError Interrupt [337.241337] CPU: 0 UI PREEMPT [337.241342] Tainted: [M]=MACHINE_CHECK [337.241343] Hardware name: Texas Instruments AM68 SK (DT) [337.241345] Call trace: [337.241348] s dump_stack+0x18/0x24 [337.241368] vpanic+0x124/0x2ec [337.241373] abort+0x0/0x4 [337.241377] add_taint+0x0/0xbc [337.241384] arm64_serror_panic+ el1h_64_error_handler+0x30/0x48 [337.241400] el1h_64_error+0x6c/0x70 [337.241404] pvr_riscv_irq_pending+0xc/0x24 (P) [337.241410] irq_thread_fn+0x2c/ 337.241428] ret_from_fork+0x10/0x20 [337.241434] SMP: stopping secondary CPUs [337.241451] Kernel Offset: disabled [337.241453] CPU features: 0x040000 end Kernel panic - not syncing: Asynchronous SError Interrupt]---
CVE-2026-35608	QuickDrop is an easy-to-use file sharing application. Prior to 1.5.3, a stored XSS vulnerability exists in the file preview endpoint. The application allows SVG files to crafted SVG file containing a JavaScript payload. When any user views the file preview, the script executes in the context of the application's domain. This vulnerab
CVE-2026-23470	In the Linux kernel, the following vulnerability has been resolved: drm/imagination: Fix deadlock in soft reset sequence The soft reset sequence is currently execut waits for IRQ handlers, i.e. itself, to complete. Use disable_irq_nosync() during a soft reset instead.
CVE-2026-35606	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Prior to 2.63.1, the resourceGe Perm.Download permission flag. All three other content-serving endpoints (/api/raw, /api/preview, /api/subtitle) correctly verify this permission before serving conte bypass paths. This vulnerability is fixed in 2.63.1.
CVE-2026-23471	In the Linux kernel, the following vulnerability has been resolved: drm: Fix use-after-free on framebuffers and property blobs when calling drm_dev_unplug When tr desktop environment and game running I noticed a few OOPSes when dereferencing freed pointers, related to framebuffers and property blobs after the compositc immediately put the references from struct drm_file objects during drm_dev_unplug(). Related warnings for framebuffers on the subtest: [739.713076] ----------[c WARNING: drivers/gpu/drm/drm_mode_config.c:584 at drm_mode_config_cleanup+0x30b/0x320 [drm], CPU#12: xe_module_load/13145 .... [739.713328] Call Trac [xe] [739.713574] ? intel_atomic_global_obj_cleanup+0xe4/0x1a0 [xe] [739.713794] intel_display_driver_remove_noirq+0x51/0xb0 [xe] [739.714041] xe_display 739.714294] devres_release_all+0xad/0xf0 [739.714301] device_unbind_cleanup+0x12/0xa0 [739.714305] device_release_driver_internal+0x1b7/0x210 [739.7 739.714319] drv_attr_store+0x21/0x30 [739.714322] sysfs_kf_write+0x48/0x60 [739.714328] kernfs_fop_write_iter+0x16b/0x240 [739.714333] vfs_write+0x26 __x64_sys_write+0x19/0x20 [739.714347] x64_sys_call+0xa15/0xa30 [739.714355] do_syscall_64+0xd8/0xab0 [739.714361] entry_SYSCALL_64_after_hwframe 0000:67:00.0: [drm] drm_WARN_ON(!list_empty(&fb->filp_head)) [739.714464] WARNING: drivers/gpu/drm/drm_framebuffer.c:833 at drm_framebuffer_free+0x6c 0010:drm_framebuffer_free+0x7a/0x90 [drm] ... [739.714869] Call Trace: [739.714871] <TASK> [739.714876] drm_mode_config_cleanup+0x26a/0x320 [drm] [drm_mode_config_cleanup+0x207/0x320 [drm] [739.715235] intel_display_driver_remove_noirq+0x51/0xb0 [xe] [739.715576] xe_display_fini_early+0x33/0x50 [devres_release_all+0xad/0xf0 [739.715843] device_unbind_cleanup+0x12/0xa0 [739.715850] device_release_driver_internal+0x1b7/0x210 [739.715856] device drv_attr_store+0x21/0x30 [739.715868] sysfs_kf_write+0x48/0x60 [739.715873] kernfs_fop_write_iter+0x16b/0x240 [739.715878] vfs_write+0x266/0x520 [739 739.715893] x64_sys_call+0xa15/0xa30 [739.715900] do_syscall_64+0xd8/0xab0 [739.715905] entry_SYSCALL_64_after_hwframe+0x4b/0x53 and then finally fi canonical address 0xdead000000000122: 0000 [#1] SMP [743.186535] CPU: 3 UID: 1000 PID: 3453 Comm: kwin_wayland Tainted: G W 7.0.0-rc1-valkyria+ #110 name: Gigabyte Technology Co., Ltd. X299 AORUS Gaming 3/X299 AORUS Gaming 3-CF, BIOS F8n 12/06/2021 [743.186539] RIP: 0010:drm_framebuffer_cleanup+ 50 07 00 00 31 f6 e8 3a 80 d3 e1 49 8b 44 24 10 49 8d 7c 24 08 49 8b 54 24 08 <48> 3b 38 0f 85 95 7f 02 00 48 3b 7a 08 0f 85 8b 7f 02 00 48 89 42 [743.1865
CVE-2026-35605	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Prior to 2.63.1, the Matches() f when matching paths against access rules. A rule for /uploads also matches /uploads_backup/, granting or denying access to unintended directories. This vulnerabi
CVE-2026-35604	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Prior to 2.63.1, when an admin that user remain fully accessible to unauthenticated users. The public share download handler does not re-check the share owner's current permissions. This vulne
CVE-2026-23464	In the Linux kernel, the following vulnerability has been resolved: soc: microchip: mpfs: Fix memory leak in mpfs_sys_controller_probe() In mpfs_sys_controller_prol freeing the allocated memory for sys_controller, leading to a memory leak. Fix this by jumping to the out_free label to ensure the memory is properly freed. Also, c same label.
CVE-2026-35585	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. From 2.0.0 through 2.63.1, the on file events such as upload, rename, and delete — is vulnerable to OS command injection. Variable substitution for values like $FILE and $USERNAME is performe malicious filename containing shell metacharacters, causing the server to execute arbitrary OS commands when the hook fires. This results in Remote Code Execu onwards, including for existent installations.
CVE-2026-23472	In the Linux kernel, the following vulnerability has been resolved: serial: core: fix infinite loop in handle_tx() for PORT_UNKNOWN uart_write_room() and uart_write(ports that were never properly initialized): - uart_write_room() returns kfifo_avail() which can be > 0 - uart_write() checks xmit_buf and returns 0 if NULL This incon they can write: while (tty_write_room(tty) > 0) { written = tty->ops->write(...); // written is always 0, loop never exits } For example, caif_serial's handle_tx() enter Fix by making uart_write_room() also check xmit_buf and return 0 if it's NULL, consistent with uart_write(). Reproducer: https://gist.github.com/mrpre/d9a694cc0e1
CVE-2026-34228	Emlog is an open source website building system. Prior to version 2.6.8, the backend upgrade interface accepts remote SQL and ZIP URLs via GET parameters. The extracts it directly into the web root directory. This process does not validate a CSRF token. Therefore, an attacker only needs to trick an authenticated administrat write. This issue has been patched in version 2.6.8.
CVE-2026-23473	In the Linux kernel, the following vulnerability has been resolved: io_uring/poll: fix multishot recv missing EOF on wakeup race When a socket send and shutdown() to run. The first wake gets poll ownership (poll_refs=1), and the second bumps it to 2. When io_poll_check_events() runs, it calls io_poll_issue() which does a recv th (atomic_sub_return(2) -> 0) and exits, even though only the first event was consumed. Since the shutdown is a persistent state change, no further wakeups will ha loop, and ensure that another loop is done to check for status if more than a single poll activation is pending. This ensures we don't lose the shutdown event.
CVE-2026-35584	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Prior to 1.8.212, the endpoint GET /thread/read/{conversation_id}/{thread_id} c belongs to the given conversation_id. This allows any unauthenticated attacker to mark any thread as read by passing arbitrary IDs, enumerate valid thread IDs via conversations (IDOR). This vulnerability is fixed in 1.8.212.
CVE-2026-23474	In the Linux kernel, the following vulnerability has been resolved: mtd: Avoid boot crash in RedBoot partition table parser Given CONFIG_FORTIFY_SOURCE=y and a when available") produces the warning below and an oops. Searching for RedBoot partition table in 50000000.flash at offset 0x7e0000 ----------[cut here]---------- detected buffer overflow: 15 byte read of buffer size 14 Modules linked in: CPU: 0 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.19.0 #1 NONE As Kees said, "'name basically any length at all. This fortify warning looks legit to me -- this code used to be reading beyond the end of the allocation." Since the size of the dynamic allo within bounds.
CVE-2026-23463	In the Linux kernel, the following vulnerability has been resolved: soc: fsl: qbman: fix race condition in qman_destroy_fq When QMAN_FQ_FLAG_DYNAMIC_FQID is s the pool and WARN_ON(fq_table[fq->idx]) in qman_create_fq() gets triggered. Indeed, we can have: Thread A Thread B qman_destroy_fq() qman_create_fq() qman_ available again -- qman_alloc_fqid() -- so, we can get the just-freed fqid in thread B -- fq->fqid = fqid; fq->idx = fqid * 2; WARN_ON(fq_table[fq->idx]); fq_table[fq-> qman_release_fqid() and fq_table[fq->idx] = NULL makes the WARN_ON() trigger a lot more. To prevent that, ensure that fq_table[fq->idx] is set to NULL before ge
CVE-2026-23475	In the Linux kernel, the following vulnerability has been resolved: spi: fix statistics allocation The controller per-cpu statistics is not allocated until after the controll sysfs attributes can trigger a NULL-pointer dereference. Fix this by moving the statistics allocation to controller allocation while tying its lifetime to that of the contr
	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: HIDP: Fix possible UAF This fixes the following trace caused by not dropping l2cap_con

CVE-2026-23462	freeing conn ffff88810a171c00 [97.809907] CPU: 1 UID: 0 PID: 1419 Comm: repro_standalon Not tainted 7.0.0-rc1-dirty #14 PREEMPT(lazy) [97.809935] Hardwar 04/01/2014 [97.809947] Call Trace: [97.809954] <TASK> [97.809961] dump_stack_lvl (lib/dump_stack.c:122) [97.809990] l2cap_conn_free (net/bluetooth/l2cap net/bluetooth/l2cap_core.c:1821 net/bluetooth/l2cap_core.c:1798) [97.810055] l2cap_disconn_cfm (net/bluetooth/l2cap_core.c:7347 (discriminator 1) net/bluetooth (net/bluetooth/l2cap_core.c:7341) [97.810117] hci_conn_hash_flush (./include/net/bluetooth/hci_core.h:2152 (discriminator 2) net/bluetooth/hci_conn.c:2644 (discr 97.810180] ? __pfx_hci_dev_close_sync (net/bluetooth/hci_sync.c:5285) [97.810212] ? srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) [97.810242] ? up_wri ./include/linux/atomic/atomic-arch-fallback.h:2852 (discriminator 5) ./include/linux/atomic/atomic-long.h:268 (discriminator 5) ./include/linux/atomic/atomic-instrum kernel/locking/rwsem.c:1643 (discriminator 5)) [97.810267] ? srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) [97.810290] ? rcu_is_watching (./arch/x86/incl ./include/linux/context_tracking.h:128 kernel/rcu/tree.c:752) [97.810320] hci_unregister_dev (net/bluetooth/hci_core.c:504 net/bluetooth/hci_core.c:2716) [97.810 (drivers/bluetooth/hci_vhci.c:678) [97.810404] __fput (fs/file_table.c:470) [97.810430] task_work_run (kernel/task_work.c:235) [97.810451] ? __pfx_task_work_run (arch/x86/lib/retpoline.S:221) [97.810495] ? do_raw_spin_unlock (./include/asm-generic/qspinlock.h:128 (discriminator 5) kernel/locking/spinlock_debug.c:142 (disc srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) [97.810574] ? __pfx_do_exit (kernel/exit.c:897) [97.810594] ? lock_acquire (kernel/locking/lockdep.c:470 (di kernel/locking/lockdep.c:5825 (discriminator 6)) [97.810616] ? srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) [97.810639] ? do_raw_spin_lock (kernel/locki (discriminator 4)) [97.810664] ? srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) [97.810688] ? find_held_lock (kernel/locking/lockdep.c:5350 (discriminator (kernel/signal.c:3007 (discriminator 1)) [97.810772] ? security_file_permission (./arch/x86/include/asm/jump_label.h:37 security/security.c:2366) [97.810803] ? srs (fs/read_write.c:555) [97.810854] ? __pfx_get_signal (kernel/signal.c:2800) [97.810880] ? srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) [97.810905] ? __p (arch/x86/lib/retpoline.S:221) [97.810960] arch_do_signal_or_restart (arch/ ---truncated---
CVE-2026-34980	OpenPrinting CUPS is an open source printing system for Linux and other Unix-like operating systems. In versions 2.4.16 and prior, in a network-exposed cupsd wit PostScript queue without authentication. The server accepts a page-border value supplied as textWithoutLanguage, preserves an embedded newline through optio trusted scheduler control record. A follow-up raw print job can therefore make the server execute an attacker-chosen existing binary such as /usr/bin/vim as lp. At t
CVE-2026-31271	megagao production_ssm v1.0 contains an authorization bypass vulnerability in the user addition functionality. The insert() method in UserController.java lacks aut accounts by directly accessing the /user/insert endpoint. This leads to complete system compromise.
CVE-2026-31272	MRCMS 3.1.2 contains an access control vulnerability. The save() method in src/main/java/org/marker/mushroom/controller/UserController.java lacks proper author authentication.
CVE-2026-35572	ChurchCRM is an open-source church management system. Prior to 6.5.3, it is possible to trigger server-side HTTP/HTTPS requests to arbitrary hosts (SSRF) by sup outbound request to the attacker-controlled domain, confirmed via OAST. This vulnerability is fixed in 6.5.3.
CVE-2026-34947	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 befor pages without email verification. This issue has been patched in versions 2026.1.3, 2026.2.2, and 2026.3.0.
CVE-2026-23899	An improper access check allows unauthorized access to webservice endpoints.
CVE-2026-35578	ChurchCRM is an open-source church management system. Prior to 7.0.0, it was possible in many places across the ChurchCRM application to create a link that, wh attacker if they clicked 'Cancel' button on the page. For this write-up the DonatedItemEditor.php will be used as an example, however wherever all instances of 'lin
CVE-2025-14857	An improper access control vulnerability exists in Semtech LoRa LR11xxx transceivers running early versions of firmware where the memory write command acces stack. An attacker with physical access to the SPI interface can overwrite stack memory to hijack program control flow and achieve limited arbitrary code execution mechanism prevents persistent firmware modification, the crypto engine isolates cryptographic keys from direct firmware access, and all modifications are lost upo
CVE-2026-23403	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix memory leak in verify_header The function sets `*ns = NULL` on every call, leaking unpacked. This also breaks namespace consistency checking since *ns is always NULL when the comparison is made. Remove the incorrect assignment. The caller
CVE-2026-3566	Rejected reason: After further discussion, the issue was determined to not meet the criteria for CVE assignment.
CVE-2026-39400	Cronicle is a multi-server task scheduler and runner, with a web based front-end UI. Prior to 0.9.111, a non-admin user with create_events and run_events privilege table.header, table.rows, table.caption). The server stores this data without sanitization, and the client renders it via innerHTML on the Job Details page. This vulne
CVE-2026-34080	xdg-dbus-proxy is a filtering proxy for D-Bus connections. Prior to 0.1.7, a policy parser vulnerability allows bypassing eavesdrop restrictions. The proxy checks for before the equals sign) and similar cases. Clients can intercept D-Bus messages they should not have access to. This vulnerability is fixed in 0.1.7.
CVE-2026-31404	In the Linux kernel, the following vulnerability has been resolved: NFSD: Defer sub-object cleanup in export put callbacks svc_export_put() calls path_put() and auth period. RCU readers in e_show() and c_show() access both ex_path (via seq_path/d_path) and ex_client->name (via seq_escape) without holding a reference. If cac are freed while still in use, producing a NULL pointer dereference in d_path. Commit 2530766492ec ("nfsd: fix UAF when access ex_uuid or ex_stats") moved kfree auth_domain_put() running before the grace period because both may sleep and call_rcu callbacks execute in softirq context. Replace call_rcu/kfree_rcu with queue it in process context where sleeping is permitted. This allows path_put() and auth_domain_put() to be moved into the deferred callback alongside the other resourc ek_path and ek_client. A dedicated workqueue scopes the shutdown drain to only NFSD export release work items; flushing the shared system_unbound_wq would rcu_barrier() followed by flush_workqueue() to ensure all deferred release callbacks complete before the export caches are destroyed. Reviwed-by: Jeff Layton <jla
CVE-2026-33439	Open Access Management (OpenAM) is an access management solution. Prior to 16.0.6, OpenIdentityPlatform OpenAM is vulnerable to pre-authentication Remote parameter. This bypasses the WhitelistObjectInputStream mitigation that was applied to the jato.pageSession parameter after CVE-2021-35464. An unauthenticate crafted serialized Java object as the jato.clientSession GET/POST parameter to any JATO ViewBean endpoint whose JSP contains <jato:form> tags (e.g., the Passwo
CVE-2026-31403	In the Linux kernel, the following vulnerability has been resolved: NFSD: Hold net reference for the lifetime of /proc/fs/nfs/exports fd The /proc/fs/nfs/exports proc e exports_proc_open() captures the caller's current network namespace and stores its svc_export_cache in seq->private, but takes no reference on the namespace. I opener does setns() to a different namespace), nfsd_net_exit() calls nfsd_export_shutdown() which frees the cache. Subsequent reads on the still-open fd dereferer net for the lifetime of the open file descriptor. This prevents nfsd_net_exit() from running -- and thus prevents nfsd_export_shutdown() from freeing the cache -- wh cache_create_net()), so exports_release() can retrieve it without additional per-file storage.
CVE-2026-2394	Buffer Over-read vulnerability in RTI Connext Professional (Core Libraries) allows Overread Buffers.This issue affects Connext Professional: from 7.4.0 before 7.7.0, before 5.3.*, from 4.3x before 5.2.*.
	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix heap overflow in NFSv4.0 LOCK replay cache The NFSv4.0 replay cache uses a fixed 112

CVE-2026-31402	responses. This size was calculated based on OPEN responses and does not account for LOCK denied responses, which include the conflicting lock owner as a varia denied due to a conflict with an existing lock that has a large owner, nfsd4_encode_operation() copies the full encoded response into the undersized replay buffer v bounds write of up to 944 bytes past the end of the buffer, corrupting adjacent heap memory. This can be triggered remotely by an unauthenticated attacker with other requests a conflicting lock to provoke the denial. We could fix this by increasing NFSD4_REPLAY_ISIZE to allow for a full opaque, but that would increase the s checking the encoded response length against NFSD4_REPLAY_ISIZE before copying into the replay buffer. If the response is too large, set rp_buflen to 0 to skip ca correct response on the original request.
CVE-2026-39841	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in Wikimedia Foundation Mediawiki - Cargo Extension allows Stored XS
CVE-2026-28386	Issue summary: Applications using AES-CFB128 encryption or decryption on systems with AVX-512 and VAES support can trigger an out-of-bounds read of up to 15 read may trigger a crash which leads to Denial of Service for an application if the input buffer ends at a memory page boundary and the following page is unmappe The vulnerable code path is only reached when processing partial blocks (when a previous call left an incomplete block and the current call provides fewer bytes th boundary with the following page unmapped. CFB mode is not used in TLS/DTLS protocols, which use CBC, GCM, CCM, or ChaCha20-Poly1305 instead. For these re x86-64 systems with AVX-512 and VAES instruction support are affected. Other architectures and systems without VAES support use different code paths that are n
CVE-2026-39840	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Wikimedia Foundation Mediawiki - Cargo Extension allows XSS T 3.8.7.
CVE-2026-39839	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in Wikimedia Foundation Mediawiki - Cargo Extension allows Stored XS
CVE-2026-39838	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Wikimedia Foundation MediaWiki - ProofreadPage Extension allo
CVE-2026-39837	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in WikiWorks Mediawiki - Cargo Extension allows Stored XSS.This issue
CVE-2026-39382	dbt enables data analysts and engineers to transform their data using the same practices that software engineers use to build applications. Inside the reusable wo job uses peter-evans/find-comment to search for an existing comment indicating that a docs issue has already been opened. The output steps.issue_comment.outp comment-body is attacker-controlled text and is inserted into shell syntax without escaping, a malicious comment body can break out of the quoted string and inje bbed8d28354e9c644c5a7df13946a3a0451f9ab9.
CVE-2026-39381	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.8.0-alpha.7 and 8.6.75, the GET /sessions/me en protected via the protectedFields server option. Any authenticated user can retrieve their own session's protected fields with a single request. The equivalent GET vulnerability is fixed in 9.8.0-alpha.7 and 8.6.75.
CVE-2026-31401	In the Linux kernel, the following vulnerability has been resolved: HID: bpf: prevent buffer overflow in hid_hw_request right now the returned value is considered to arbitrary big, because it's the return value of dispatch_hid_bpf_raw_requests(), which calls the struct_ops and we have no guarantees that the value makes sense.
CVE-2026-39401	Cronicle is a multi-server task scheduler and runner, with a web based front-end UI. Prior to 0.9.111, jb child processes can include an update_event key in their JS without any authorization check. A low-privilege user who can create and run events can modify any event property, including webhook URLs and notification emai
CVE-2026-28387	Issue summary: An uncommon configuration of clients performing DANE TLSA-based server authentication, when paired with uncommon server DANE TLSA record A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, the issue only af certificate usages and the DANE-TA(2) certificate usage. By far the most common deployment of DANE is in SMTP MTAs for which RFC7672 recommends that client SMTP (or other similar) clients are not vulnerable to this issue. Conversely, any clients that support only the PKIX usages, and ignore the DANE-TA(2) usage are also publishes a TLSA RRset with both types of TLSA records. No FIPS modules are affected by this issue, the problem code is outside the FIPS module boundary.
CVE-2026-31399	In the Linux kernel, the following vulnerability has been resolved: nvdimm/bus: Fix potential use after free in asynchronous initialization Dingisoul with KASAN repo b6eae0f61db2 ("libnvdimm: Hold reference on parent while scheduling async init") correctly added a reference on the parent device to be held until asynchronous ref count of the device drops to 0 prior to the parent pointer being accessed. Thus resulting in use after free. The bug bot AI correctly identified the fix. Save a refe outcome of device_add().
CVE-2026-35568	MCP Java SDK is the official Java SDK for Model Context Protocol servers and clients. Prior to 1.0.0, the java-sdk contains a DNS rebinding vulnerability. This vulnera a victims browser that is either local, or network adjacent. This allows an attacker to make any tool call to the server as if they were a locally running MCP connecte
CVE-2026-39936	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in The Wikimedia Foundation Mediawiki - Score Extension allows Cr
CVE-2026-39935	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in The Wikimedia Foundation Mediawiki - CampaignEvents Extensio Extension: 1.43.7, 1.44.4, 1.45.2.
CVE-2025-20628	An insufficient granularity of access control vulnerability exists in PingIDM (formerly ForgeRock Identity Management) where administrators cannot properly configu means attackers can spoof a client-mode RCS (if one exists) to intercept and/or modify an identity's security-relevant properties, such as passwords and account re client mode.
CVE-2026-0545	In mlflow/mlflow, the FastAPI job endpoints under `/ajax-api/3.0/jobs/*` are not protected by authentication or authorization when the `basic-auth` app is enabled. (`MLFLOW_SERVER_ENABLE_JOB_EXECUTION=true`) and any job function is allowlisted, any network client can submit, read, search, and cancel jobs without crede execution if allowed jobs perform privileged actions such as shell execution or filesystem changes. Even if jobs are deemed safe, this still constitutes an authentica in job results.
CVE-2026-39937	Improper removal of sensitive information before storage or transfer vulnerability in The Wikimedia Foundation Mediawiki - CentralAuth Extension allows Resource
CVE-2026-	Loop with unreachable exit condition ('infinite loop') vulnerability in The Wikimedia Foundation Mediawiki - GrowthExperiments Extension allows Leveraging Time-o

39934	GrowthExperiments Extension: 1.45.2, 1.44.4, 1.43.7.
CVE-2026-39933	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in The Wikimedia Foundation Mediawiki - GlobalWatchlist Extensior
CVE-2026-34582	Botan is a C++ cryptography library. Prior to version 3.11.1, the TLS 1.3 implementation allowed ApplicationData records to be processed prior to the Finished mes certificates can by bypassed by a client which entirely omits Certificate, CertificateVerify, and the Finished message and instead sends application data records. Th
CVE-2026-28388	Issue summary: When a delta CRL that contains a Delta CRL Indicator extension is processed a NULL pointer dereference might happen if the required CRL Numbe crash which leads to a Denial of Service for an application. When CRL processing and delta CRL processing is enabled during X.509 certificate verification, the delta dereferencing it. When a malformed delta CRL file is being processed, this parameter can be NULL, causing a NULL pointer dereference. Exploiting this issue requir certificate being verified to contain a freshestCRL extension or the base CRL to have the EXFLAG_FRESHEST flag set, and an attacker to provide a malformed CRL t cannot be escalated to achieve code execution or memory disclosure. For that reason the issue was assessed as Low severity according to our Security Policy. The affected code is outside the OpenSSL FIPS module boundary.
CVE-2026-34580	Botan is a C++ cryptography library. In 3.11.0, the function Certificate_Store::certificate_known had a misleading name; it would return true if any certificate in the did not check that the cert it found and the cert it was passed were actually the same certificate. In 3.11.0 an extension of path validation logic was made which as identical. The impact is that if an end entity certificate is presented, and its DN (and subject key identifier, if set) match that of any trusted root, the end entity cert fixed in 3.11.1.
CVE-2026-34079	Flatpak is a Linux application sandboxing and distribution framework. Prior to 1.16.4, the caching for ld.so removes outdated cache files without properly checking allows Flatpak apps to delete arbitrary files on the host. This vulnerability is fixed in 1.16.4.
CVE-2026-34078	Flatpak is a Linux application sandboxing and distribution framework. Prior to 1.16.4, the Flatpak portal accepts paths in the sandbox-expose options which can be host path in the sandbox. This gives apps access to all host files and can be used as a primitive to gain code execution in the host context. This vulnerability is fixe
CVE-2026-31790	Issue summary: Applications using RSASVE key encapsulation to establish a secret encryption key can send contents of an uninitialized memory buffer to a malicio the previous execution of the application process which leads to sensitive data leakage to an attacker. RSA_public_encrypt() returns the number of bytes written or zero. As a result, if RSA encryption fails, encapsulation can still return success to the caller, set the output lengths, and leave the caller to use the contents of the c EVP_PKEY_encapsulate() with RSA/RSASVE on an attacker-supplied invalid RSA public key without first validating that key, then this may cause stale or uninitialized place of the KEM ciphertext. As a workaround calling EVP_PKEY_public_check() or EVP_PKEY_public_check_quick() before EVP_PKEY_encapsulate() will mitigate the i
CVE-2026-31789	Issue summary: Converting an excessively large OCTET STRING value to a hexadecimal string leads to a heap buffer overflow on 32 bit platforms. Impact summary execution or other undefined behavior. If an attacker can supply a crafted X.509 certificate with an excessively large OCTET STRING value in extensions such as th converted to hex, the size of the buffer needed for the result is calculated as multiplication of the input length by 3. On 32 bit platforms, this multiplication may ov Applications and services that print or log contents of untrusted X.509 certificates are vulnerable to this issue. As the certificates would have to have sizes of over 32 bit platforms are affected, this issue was assigned Low severity. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the affected cod
CVE-2026-28390	Issue summary: During processing of a crafted CMS EnvelopedData message with KeyTransportRecipientInfo a NULL pointer dereference can happen. Impact sumr authentication or cryptographic operations occur resulting in Denial of Service. When a CMS EnvelopedData message that uses KeyTransportRecipientInfo with RSA algorithm identifier is examined without checking for its presence. This results in a NULL pointer dereference if the field is missing. Applications and services that c are vulnerable. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.
CVE-2026-28389	Issue summary: During processing of a crafted CMS EnvelopedData message with KeyAgreeRecipientInfo a NULL pointer dereference can happen. Impact summary authentication or cryptographic operations occur resulting in Denial of Service. When a CMS EnvelopedData message that uses KeyAgreeRecipientInfo is processed without checking for its presence. This results in a NULL pointer dereference if the field is missing. Applications and services that call CMS_decrypt() on untrusted in modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.
CVE-2026-31400	In the Linux kernel, the following vulnerability has been resolved: sunrpc: fix cache_request leak in cache_release When a reader's file descriptor is closed while in the request's readers count but never checks whether it should free the request. In cache_read(), when readers drops to 0 and CACHE_PENDING is clear, the cache reference. cache_release() lacks this cleanup. The only other path that frees requests with readers == 0 is cache_dequeue(), but it runs only when CACHE_PENDIN still non-zero, cache_dequeue() will have skipped the request, and no subsequent call will clean it up. Add the same cleanup logic from cache_read() to cache_relea and if so, dequeue and free the cache_request.
CVE-2026-31398	In the Linux kernel, the following vulnerability has been resolved: mm/rmap: fix incorrect pte restoration for lazyfree folios We batch unmap anonymous lazyfree fo we may end up setting the entire batch writable. Fix this by respecting writable bit during batching. Although on a successful unmap of a lazyfree folio, the soft-dirt make the fix consistent w.r.t both writable bit and soft-dirty bit. I was able to write the below reproducer and crash the kernel. Explanation of reproducer (set 64K r MADV_DONTFORK. fork() - parent points to the folio with 8 writable ptes and 8 non-writable ptes. Merge the VMAs with MADV_DOFORK so that folio_unmap_pte_bat the folio as lazyfree. Write to the memory to dirty the pte, eventually rmap will dirty the folio. Then trigger reclaim, we will hit the pte restoration path, and the kerr BUG_ON(atomic_inc_return(&ptc->anon_map_count) > 1 && rw); The code path is asking for anonymous page to be mapped writable into the pagetable. The BUG_ more than one process, which breaks anonymous memory/CoW semantics. [21.134473] kernel BUG at mm/page_table_check.c:118! [21.134497] Internal error: C CPU: 1 UID: 0 PID: 1735 Comm: dup-lazyfree Not tainted 7.0.0-rc1-00116-g018018a17770 #1028 PREEMPT [21.136858] Hardware name: linux,dummy-virt (DT) [21.137308] pc : page_table_check_set+0x28c/0x2a8 [21.137607] lr : page_table_check_set+0x134/0x2a8 [21.137885] sp : ffff80008a3b3340 [21.138124] x29: f 0040000000000040 x25: ffffd1a55f7dd000 x24: 0000000000000001 [21.139045] x23: 0000000000000001 x22: 0000000000000001 x21: ffffd1a55f217f30 [21.1 21.140027] x17: 0001400000000000 x16: 0001700000000000 x15: 000000000000ffff [21.140578] x14: 000000000000000c x13: 005c006000000000 x12: 0000(ffffd1a55c079ee0 [21.141077] x8 : 0000000000000001 x7 : 005c03e000040000 x6 : 000000004000ffff [21.141490] x5 : ffff00017fffce00 x4 : 000000000000000 0000000000000000 x0 : ffff0000c08228c0 [21.141991] Call trace: [21.142093] page_table_check_set+0x28c/0x2a8 (P) [21.142265] __page_table_check_ptes_se 21.142766] contpte_set_ptes+0xe8/0x140 [21.142907] try_to_unmap_one+0x10c4/0x10d0 [21.143177] rmap_walk_anon+0x100/0x250 [21.143315] try_to_unm shrink_lruvec+0x664/0xbf0 [21.144043] shrink_node+0x218/0x878 [21.144285] __node_reclaim.constprop.0+0x98/0x338 [21.144763] user_proactive_reclaim+ dev_attr_store+0x20/0x40 [21.145585] sysfs_kf_write+0x84/0xa8 [21.145835] kernfs_fop_write_iter+0x130/0x1c8 [21.145994] vfs_write+0x2b8/0x368 [21.146 21.146380] invoke_syscall+0x50/0x120 [21.146513] el0_svc_common.constprop.0+0x48/0xf8 [21.146679] do_el0_svc+0x28/0x40 [21.146798] el0_svc+0x34/0
CVE-2026-23402	In the Linux kernel, the following vulnerability has been resolved: KVM: x86/mmu: Only WARN in direct MMUs when overwriting shadow-present SPTE Adjust KVM's different target PFN to only apply to direct MMUs, i.e. only to MMUs without shadowed gPTEs. While it's impossible for KVM to overwrite a shadow-present SPTE in r userspace, aren't detected by KVM's write tracking and so can break KVM's shadow paging rules. ------------[cut here]------------ pfn != spte_to_pfn(*sptep) WARNING vmx_ept_stale_r/872 Modules linked in: kvm_intel kvm irqbypass CPU: 0 UID: 1000 PID: 872 Comm: vmx_ept_stale_r Not tainted 7.0.0-rc2-eafebd2d2ab0-sink-vm # 02/06/2015 RIP: 0010:mmu_set_spte+0x1e4/0x440 [kvm] Call Trace: <TASK> ept_page_fault+0x535/0x7f0 [kvm] kvm_mmu_do_page_fault+0xee/0x1f0 [kvm] kvr kvm_arch_vcpu_ioctl_run+0xc55/0x1c20 [kvm] kvm_vcpu_ioctl+0x2d5/0x980 [kvm] __x64_sys_ioctl+0x8a/0xd0 do_syscall_64+0xb5/0x730 entry_SYSCALL_64_aft
CVE-2025-71058	Dual DHCP DNS Server 8.01 improperly accepts and caches UDP DNS responses without validating that the response originates from a legitimate configured upstre results into the cache, enabling a remote attacker to inject forged responses and poison the DNS cache, potentially redirecting victims to attacker-controlled destir

CVE-2026-39351	Frappe is a full-stack web application framework. Prior to 16.14.0 and 15.104.0, Frappe allows unrestricted Doctype access via API exploit.
CVE-2026-39349	OrangeHRM is a comprehensive human resource management (HRM) system. From 5.0 to 5.8, OrangeHRM Open Source encrypts certain sensitive fields with AES enables pattern disclosure against stored data. This vulnerability is fixed in 5.8.1.
CVE-2026-39348	OrangeHRM is a comprehensive human resource management (HRM) system. From 5.0 to 5.8, OrangeHRM Open Source omits authorization on job specification ar to read attachments via direct reference to attachment identifiers. This vulnerability is fixed in 5.8.1.
CVE-2026-39347	OrangeHRM is a comprehensive human resource management (HRM) system. From 5.0 to 5.8, OrangeHRM Open Source accepts changes to self-appraisal submiss breaking integrity of finalized appraisal records. This vulnerability is fixed in 5.8.1.
CVE-2026-39346	OrangeHRM is a comprehensive human resource management (HRM) system. From 5.0 to 5.8, OrangeHRM Open Source allowed authenticated users to bypass dis of modules disabled by an administrator. This vulnerability is fixed in 5.8.1.
CVE-2026-39345	OrangeHRM is a comprehensive human resource management (HRM) system. From 5.0 to 5.8, OrangeHRM Open Source fails to restrict email template file resoluti influence the template path to read arbitrary local files. This vulnerability is fixed in 5.8.1.
CVE-2026-22711	Improper neutralization of alternate XSS syntax vulnerability in The Wikimedia Foundation Mediawiki - Wikilove Extension allows Cross-Site Scripting (XSS).This issu
CVE-2026-39344	ChurchCRM is an open-source church management system. Prior to 7.1.0, there is a Reflected Cross-Site Scripting (XSS) vulnerability on the login page, which is ca the URL. The username parameter value is directly displayed in the login page input element without filter, allowing attackers to insert malicious JavaScript scripts. data such as session cookies or replacing the display to show the attacker's login form. This vulnerability is fixed in 7.1.0.
CVE-2026-39360	RustFS is a distributed object storage system built in Rust. Prior to alpha.90, RustFS contains a missing authorization check in the multipart copy path (UploadPartC exfiltrate victim objects by copying them into an attacker-controlled multipart upload and completing the upload. This breaks tenant isolation in multi-user / multi-t
CVE-2026-39342	ChurchCRM is an open-source church management system. Prior to 7.1.0, the searchwhat parameter via QueryView.php with the QueryID=15 is vulnerable to a SQ access to the "Advanced Search" query. This vulnerability is fixed in 7.1.0.
CVE-2026-31390	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix memory leak in xe_vm_madvise_ioctl When check_bo_args_are_sane() validation fails This ensures proper cleanup in this error path. (cherry picked from commit 29bd06faf727a4b76663e4be0f7d770e2d2a7965)
CVE-2026-39338	ChurchCRM is an open-source church management system. Prior to 7.1.0, a Blind Reflected Cross-Site Scripting vulnerability exists in the search parameter accept supplied input prior to rendering it within the browser's DOM. Although the application ultimately returns an HTTP 500 error due to the malformed API request caus <script> tags before the error response is returned — resulting in successful code execution regardless of the server-side error. This vulnerability is fixed in 7.1.0.
CVE-2026-31389	In the Linux kernel, the following vulnerability has been resolved: spi: fix use-after-free on controller registration failure Make sure to deregister from driver core als registration to avoid use-after-free (of driver resources) and unclocked register accesses.
CVE-2026-27124	FastMCP is the standard framework for building MCP applications. Prior to version 3.2.0, while testing the GitHubProvider OAuth integration, which allows authentic discovered that the FastMCP OAuthProxy does not properly validate the user's consent upon receiving the authorization code from GitHub. In combination with GitH introduces a Confused Deputy vulnerability. This issue has been patched in version 3.2.0.
CVE-2026-25118	immich is a high performance self-hosted photo and video management solution. Prior to version 2.6.0, the Immich application is vulnerable to credential disclosur application transmits the album password within the URL query parameters in a GET request to /api/shared-links/me. This exposes the password in browser history authentication credentials. The impact of this vulnerability is the potential compromise of shared album access and unauthorized exposure of sensitive user data. T
CVE-2026-23401	In the Linux kernel, the following vulnerability has been resolved: KVM: x86/mmu: Drop/zap existing present SPTE even when creating an MMIO SPTE When installir shadow-present). While commit a54aa15c6bda3 was right about it being impossible to convert a shadow-present SPTE to an MMIO SPTE due to a _guest_ write, it f host userspace modifies a shadowed gPTE to switch from a memslot to emulted MMIO and then the guest hits a relevant page fault, KVM will install the MMIO SPTE is_shadow_present_pte(*sptep) WARNING: arch/x86/kvm/mmu/mmu.c:484 at mark_mmio_spte+0xb2/0xc0 [kvm], CPU#0: vmx_ept_stale_r/4292 Modules linked in: tainted 7.0.0-rc2-eafebd2d2ab0-sink-vm #319 PREEMPT Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 0.0.0 02/06/2015 RIP: 0010:mark_mmio_sp ept_page_fault+0x535/0x7f0 [kvm] kvm_mmu_do_page_fault+0xee/0x1f0 [kvm] kvm_mmu_page_fault+0x8d/0x620 [kvm] vmx_handle_exit+0x18c/0x5a0 [kvm_in [kvm] __x64_sys_ioctl+0x8a/0xd0 do_syscall_64+0xb5/0x730 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x47fa3f </TASK> ---[end trace 0000000(
CVE-2026-27634	Piwigo is an open source photo gallery application for the web. Prior to version 16.3.0, the four date filter parameters (f_min_date_available, f_max_date_available, concatenated directly into SQL without any escaping or type validation. This could result in an unauthenticated attacker reading the full database, including user pa
CVE-2026-27481	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 befor unauthorized users to view hidden (staff-only) tags and its associated data. All Discourse instances with tagging enabled and staff-only tag groups configured are in
CVE-2026-31397	In the Linux kernel, the following vulnerability has been resolved: mm/huge_memory: fix use of NULL folio in move_pages_huge_pmd() move_pages_huge_pmd() ha page path, src_folio is explicitly set to NULL, and is used as a sentinel to skip folio operations like lock and rmap. In the huge zero page branch, src_folio is NULL, so SPARSEMEM_VMEMMAP this silently produces a bogus PFN, installing a PMD pointing to non-existent physical memory. On other memory models it is a NULL derefe which was obtained from pmd_page() and remains valid throughout. After commit d82d09e48219 ("mm/huge_memory: mark PMD mappings of the huge zero folio continues to treat them as special mappings. move_pages_huge_pmd() currently reconstructs the destination PMD in the huge zero page branch, which drops PMD As a result, vm_normal_page_pmd() can treat the moved huge zero PMD as a normal page and corrupt its refcount. Instead of reconstructing the PMD from the foli handle the PMD metadata the same way move_huge_pmd() does for moved entries by marking it soft-dirty and clearing uffd-wp.
CVE-2026-39363	Vite is a frontend tooling framework for JavaScript. From 6.0.0 to before 6.4.2, 7.3.2, and 8.0.5, if it is possible to connect to the Vite dev server's WebSocket witho event vite:invoke and combine file://... with ?raw (or ?inline) to retrieve the contents of arbitrary files on the server as a JavaScript string (e.g., export default "..."). applied to this WebSocket-based execution path. This vulnerability is fixed in 6.4.2, 7.3.2, and 8.0.5.

CVE-2026-31396	In the Linux kernel, the following vulnerability has been resolved: net: macb: fix use-after-free access to PTP clock PTP clock is registered on every opening of the i ethtool call which is possible while the interface is just present in the kernel. BUG: KASAN: use-after-free in ptp_clock_index+0x47/0x50 drivers/ptp/ptp_clock.c:426 syz.0.6 Not tainted 6.1.164+ #109 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.16.1-0-g3208b098f51a-prebuilt.qemu.org 04/01/2014 Call T lib/dump_stack.c:106 print_address_description mm/kasan/report.c:316 [inline] print_report+0x17f/0x496 mm/kasan/report.c:420 kasan_report+0xd9/0x180 mm/k gem_get_ts_info+0x138/0x1e0 drivers/net/ethernet/cadence/macb_main.c:3349 macb_get_ts_info+0x68/0xb0 drivers/net/ethernet/cadence/macb_main.c:3371 __e net/ethtool/ioctl.c:2367 [inline] __dev_ethtool net/ethtool/ioctl.c:3017 [inline] dev_ethtool+0x2b05/0x6290 net/ethtool/ioctl.c:3095 dev_ioctl+0x637/0x1070 net/cor sock_ioctl+0x577/0x6d0 net/socket.c:1320 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:870 [inline] __se_sys_ioctl fs/ioctl.c:856 [inline] __x64_sys_ioctl+0x1 do_syscall_64+0x35/0x80 arch/x86/entry/common.c:76 entry_SYSCALL_64_after_hwframe+0x6e/0xd8 </TASK> Allocated by task 457: kmalloc include/linux/slab.h drivers/ptp/ptp_clock.c:235 gem_ptp_init+0x46f/0x930 drivers/net/ethernet/cadence/macb_ptp.c:375 macb_open+0x901/0xd10 drivers/net/ethernet/cadence/macb __dev_change_flags+0x56a/0x740 net/core/dev.c:8651 dev_change_flags+0x92/0x170 net/core/dev.c:8722 do_setlink+0xaf8/0x3a80 net/core/rtnetlink.c:2833 __rt net/core/rtnetlink.c:3655 rtnetlink_rcv_msg+0x3c6/0xed0 net/core/rtnetlink.c:6150 netlink_rcv_skb+0x15d/0x430 net/netlink/af_netlink.c:2511 netlink_unicast_kern net/netlink/af_netlink.c:1344 netlink_sendmsg+0x97e/0xeb0 net/netlink/af_netlink.c:1872 sock_sendmsg_nosec net/socket.c:718 [inline] __sock_sendmsg+0x14b/0 net/socket.c:2164 [inline] __se_sys_sendto net/socket.c:2160 [inline] __x64_sys_sendto+0xdc/0x1b0 net/socket.c:2160 do_syscall_x64 arch/x86/entry/common.c:46 entry_SYSCALL_64_after_hwframe+0x6e/0xd8 Freed by task 938: kasan_slab_free include/linux/kasan.h:177 [inline] slab_free_hook mm/slub.c:1729 [inline] slab_fr __kmem_cache_free+0xbc/0x320 mm/slub.c:3700 device_release+0xa0/0x240 drivers/base/core.c:2507 kobject_cleanup lib/kobject.c:681 [inline] kobject_release kobject_put+0x1cd/0x350 lib/kobject.c:729 put_device+0x1b/0x30 drivers/base/core.c:3805 ptp_clock_unregister+0x171/0x270 drivers/ptp/ptp_clock.c:391 gem_p macb_close+0x1c8/0x270 drivers/net/ethernet/cadence/macb_main.c:2966 __dev_close_many+0x1b9/0x310 net/core/dev.c:1585 __dev_close net/core/dev.c:1597 truncated---
CVE-2026-31395	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: fix OOB access in DBG_BUF_PRODUCER async event handler The ASYNC_EVENT_CMPL_E firmware-supplied 'type' field directly as an index into bp->bs_trace[] without bounds validation. The 'type' field is a 16-bit value extracted from DMA-mapped com compromised NIC can supply any value from 0 to 65535, causing an out-of-bounds access into kernel heap memory. The bnxt_bs_trace_check_wrap() call then der >wrapped, leading to kernel memory corruption or a crash. Fix by adding a bounds check and defining BNXT_TRACE_MAX as DBG_LOG_BUFFER_FLUSH_REQ_TYPE_ 0xc).
CVE-2026-31394	In the Linux kernel, the following vulnerability has been resolved: mac80211: fix crash in ieee80211_chan_bw_change for AP_VLAN stations ieee80211_chan_bw_ch >link[link_id]. For stations on AP_VLAN interfaces (e.g. 4addr WDS clients), sta->sdata points to the VLAN sdata, whose link never participates in chanctx reservatio NULL pointer dereference in __ieee80211_sta_cap_rx_bw() when accessing chandef->chan->band during CSA. Resolve the VLAN sdata to its parent AP sdata using even if it doesn't matter]
CVE-2026-31393	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Validate L2CAP_INFO_RSP payload length before access l2cap_information_rsp but then reads rsp->data without verifying that the payload is present: - L2CAP_IT_FEAT_MASK calls get_unaligned_le32(rsp->data), which reads 4 bytes past the h the header (needs cmd_len >= 5). A truncated L2CAP_INFO_RSP with result == L2CAP_IR_SUCCESS triggers an out-of-bounds read of adjacent skb data. Guard eac the read and let the state machine complete with safe defaults (feat_mask and remote_fixed_chan remain zero from kzalloc), so the info timer cleanup and l2cap_c
CVE-2026-31392	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix krb5 mount with username option Customer reported that some of their krb5 mou with wrong credentials. It turned out the client was reusing SMB session from first mount to try mounting the other shares, even though a different username= opt with sec=krb5 to search for principals from keytab is supported by cifs.upcall(8) since cifs-utils-4.8. So fix this by matching username mount option in match_sessio ENOKEY as there is no 'foobar' principal in keytab (/etc/krb5.keytab). The client ends up reusing SMB session from first mount to perform the second one, which is for testuser@ZELDA.TEST: ktutil: write_kt /etc/krb5.keytab ktutil: quit $ klist -ke Keytab name: FILE:/etc/krb5.keytab KVNO Principal ---- ---------- //w22-root2/scratch /mnt/1 -o sec=krb5,username=testuser $ mount.cifs //w22-root2/scratch /mnt/2 -o sec=krb5,username=foobar $ mount -t cifs | grep -Po 'usern
CVE-2026-39365	Vite is a frontend tooling framework for JavaScript. From 6.0.0 to before 6.4.2, 7.3.2, and 8.0.5, the dev server's handling of .map requests for optimized dependen a result, it is possible to bypass the server.fs.strict allow list and retrieve .map files located outside the project root, provided they can be parsed as valid source m
CVE-2026-39364	Vite is a frontend tooling framework for JavaScript. From 7.1.0 to before 7.3.2 and 8.0.5, on the Vite dev server, files that should be blocked by server.fs.deny (e.g., ?raw, ?import&raw, or ?import&url&inline are appended. This vulnerability is fixed in 7.3.2 and 8.0.5.
CVE-2026-4374	Improper Restriction of XML External Entity Reference vulnerability in RTI Connext Professional (Routing Service,Observability Collector,Recording Service,Queuein Serializat...
CVE-2026-5762	Allocation of resources without limits or throttling vulnerability in Wikimedia Foundation MediaWiki - ReportIncident Extension allows HTTP DoS.This issue affects M
CVE-2026-39322	PolarLearn is a free and open-source learning program. In 0-PRERELEASE-15 and earlier, POST /api/v1/auth/sign-in creates a valid session for banned accounts befo authenticated /api routes, enabling account data access and authenticated actions as the banned user.
CVE-2026-31391	In the Linux kernel, the following vulnerability has been resolved: crypto: atmel-sha204a - Fix OOM ->tfm_count leak If memory allocation fails, decrement ->tfm_c
CVE-2025-69515	An issue in JXL 9 Inch Car Android Double Din Player Android v12.0 allows attackers to force the infotainment system into accepting falsified GPS signals as legitima
CVE-2025-56015	In GenieACS 1.2.13, an unauthenticated access vulnerability exists in the NBI API endpoint.
CVE-2025-14859	The Semtech LR11xx LoRa transceivers implement secure boot functionality using digital signatures to authenticate firmware. However, the implementation uses a attacks. An attacker with physical access to the device can exploit this weakness to generate a malicious firmware image with a hash collision, bypassing the secu device.
CVE-2025-14858	The Semtech LR11xx LoRa transceivers running early versions of firmware contains an information disclosure vulnerability in its firmware validation functionality. W decrypts the provided encrypted firmware package block-by-block to validate its integrity. However, the last decrypted firmware block remains uncleared in memo can subsequently issue memory read commands to retrieve the decrypted firmware contents from this residual memory, effectively bypassing the firmware encryp interface.
CVE-2026-23453	In the Linux kernel, the following vulnerability has been resolved: net: ti: icssg-prueth: Fix memory leak in XDP_DROP for non-zero-copy mode Page recycling was r zero-copy mode, which uses xsk_buff_free() instead. However, this causes a memory leak when running XDP programs that drop packets in non-zero-copy mode (s OOM conditions. Fix this by handling cleanup in the caller, emac_rx_packet(). When emac_run_xdp() returns ICSSG_XDP_CONSUMED for XDP_DROP, the caller now already handles cleanup correctly with xsk_buff_free().

CVE-2026-23454	In the Linux kernel, the following vulnerability has been resolved: net: mana: fix use-after-free in mana_hwc_destroy_channel() by reordering teardown A potential before the HWC's Completion Queue (CQ) and Event Queue (EQ) are destroyed. This allows an in-flight CQ interrupt handler to dereference freed memory, leading mana_smc_teardown_hwc() signals the hardware to stop but does not synchronize against IRQ handlers already executing on other CPUs. The IRQ synchronization mana_gd_deregister_irq(). Since this runs after kfree(hwc->caller_ctx), a concurrent mana_hwc_rx_event_handler() can dereference freed caller_ctx (and rxq->msg creation order: destroy the TX/RX work queues and CQ/EQ before freeing hwc->caller_ctx. This ensures all in-flight interrupt handlers complete before the memory
CVE-2026-35481	Rejected reason: Further research determined the issue does not satisfy the assignment rules.
CVE-2026-35566	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-39319. Reason: This candidate is a duplicate of CVE-2026-39319. Not references and descriptions in this candidate have been removed to prevent accidental usage.another CVE.
CVE-2026-32145	Allocation of Resources Without Limits or Throttling vulnerability in gleam-wisp wisp allows a denial of service via multipart form body parsing. The multipart_body multipart boundary is not present in a chunk, the parser takes the MoreRequiredForBody path, which appends the chunk to the output but passes the quota uncha decrement_quota. The same pattern exists in multipart_headers, where MoreRequiredForHeaders recurses without calling decrement_body_quota. An unauthentica form submissions in a single HTTP request. This issue affects wisp: from 0.2.0 before 2.2.2.
CVE-2026-35393	goshs is a SimpleHTTPServer written in Go. Prior to 2.0.0-beta.3, the POST multipart upload directory not sanitized. This vulnerability is fixed in 2.0.0-beta.3.
CVE-2026-35392	goshs is a SimpleHTTPServer written in Go. Prior to 2.0.0-beta.3, PUT upload in httpserver/updown.go has no path sanitization. This vulnerability is fixed in 2.0.0-be
CVE-2026-35391	Bulwark Webmail is a self-hosted webmail client for Stalwart Mail Server. Prior to 1.4.11, the getClientIP() function in lib/admin/session.ts trusted the first (leftmost) attacker could forge their source IP address to bypass IP-based rate limiting (enabling brute-force attacks against the admin login) or forge audit log entries (makin is fixed in 1.4.11.
CVE-2026-35389	Bulwark Webmail is a self-hosted webmail client for Stalwart Mail Server. Prior to 1.4.11, S/MIME signature verification did not validate the certificate trust chain (ch displayed as having a valid signature. This vulnerability is fixed in 1.4.11.
CVE-2026-35213	@hapi/content provided HTTP Content-* headers parsing. All versions of @hapi/content through 6.0.0 are vulnerable to Regular Expression Denial of Service (ReDo Type and Content-Disposition headers contain patterns susceptible to catastrophic backtracking. This vulnerability is fixed in 6.0.1.
CVE-2026-35208	lichess.org is the forever free, adless and open source chess server. Any approved streamer can inject arbitrary HTML into /streamer and the homepage “Live strea blocks inline script execution, but the issue is still a server-side HTML injection sink. To trigger this, a Lichess account only needs to satisfy the normal streamer rec than 2 days with at least 15 games, or a verified/titled account. After moderator approval, once the streamer goes live, Lichess pulls the platform title and renders profile. This vulnerability is fixed with commit 0d5002696ae705e1888bf77de107c73de57bb1b3.
CVE-2026-5599	A user with API access and "manage users" permission in any venueless world is able to trigger deletion of user accounts in other worlds.
CVE-2026-35185	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Prior to 25.0.0, the /server-status endpoint is publicly accessible and exposes sensitive in addresses, and server configuration details. This allows any unauthenticated user to monitor real-time user interactions and gather internal infrastructure informat
CVE-2026-29143	SEPPmail Secure Email Gateway before version 15.0.3 does not properly authenticate the inner message of S/MIME-encrypted MIME entities, allowing an attacker t
CVE-2026-23412	In the Linux kernel, the following vulnerability has been resolved: netfilter: bpf: defer hook memory release until rcu readers are done Yiming Qian reports UaF whe after-free in nfnl_hook_dump_one.isra.0+0xe71/0x10f0 Read of size 8 at addr ffff888003edbf88 by task poc/79 Call Trace: <TASK> nfnl_hook_dump_one.isra.0+0x release until after concurrent readers have completed.
CVE-2026-35178	Workbench is a suite of tools for administrators and developers to interact with Salesforce.com organizations via the Force.com APIs. Prior to 65.0.0, Workbench co processes attacker-controlled cookie values in an unsafe manner. This vulnerability is fixed in 65.0.0.
CVE-2026-23413	In the Linux kernel, the following vulnerability has been resolved: clsact: Fix use-after-free in init/destroy rollback asymmetry Fix a use-after-free in the clsact qdisc clsact instance, and then in a second step having a replacement failure for the new clsact qdisc instance. clsact_init() initializes ingress first and then takes care of failure, the kernel will trigger the clsact_destroy() callback. Commit 1cb6f0bae504 ("bpf: Fix too early release of tcx_entry") details the way how the transition is ha tcx_miniq_inc reference count on the ingress side, but not yet on the egress side. clsact_destroy() tests whether the {ingress,egress}_entry was non-NULL. Howeve egress_entry from the previous clsact instance. What we really need to test for is whether the qdisc instance-specific ingress or egress side previously got initialize mini_qdisc_pair_inited, and utilizes that upon clsact_destroy() in order to fix the use-after-free scenario. Convert the ingress_destroy() side as well so both are cons
CVE-2026-23414	In the Linux kernel, the following vulnerability has been resolved: tls: Purge async_hold in tls_decrypt_async_wait() The async_hold queue pins encrypted input skbs tls_decrypt_async_wait() returns, every AEAD operation has completed and the engine no longer references those skbs, so they can be freed unconditionally. A sub call site that must drain pending AEAD operations and release held skbs. Move __skb_queue_purge(&ctx->async_hold) into tls_decrypt_async_wait() so the purge is tls_do_decryption(), and the new read_sock batch path -- releases held skbs on synchronization without each site managing the purge independently. This fixes a le skbs to the async_hold queue. tls_decrypt_sg() will then call tls_decrypt_async_wait() to process all pending decrypts, and drop back to synchronous mode, but tls_ in "fully-async" mode, which may not be the case here. [pabeni@redhat.com: added leak comment]
CVE-2026-23415	In the Linux kernel, the following vulnerability has been resolved: futex: Fix UaF between futex_key_to_node_opt() and vma_replace_policy() During futex_key_to_n Concurrently, mbind() may call vma_replace_policy() which frees the old mempolicy immediately via kmem_cache_free(). This creates a race where __futex_key_to mpol->mode. [151.412631] BUG: KASAN: slab-use-after-free in __futex_key_to_node (kernel/futex/core.c:349) [151.414046] Read of size 2 at addr ffff888001c496 (mm/kasan/generic.c:271) [151.416777] __futex_key_to_node (kernel/futex/core.c:349) [151.416822] get_futex_key (kernel/futex/core.c:374 kernel/futex/core.c:3
CVE-2026-23416	In the Linux kernel, the following vulnerability has been resolved: mm/mseal: update VMA end correctly on merge Previously we stored the end of the current VMA advance to the next VMA. However, this doesn't take into account the fact that a VMA might be updated due to a merge by vma_modify_flags(), which can result in incorrect curr_start on the next iteration. Resolve the issue by setting curr_end to vma->vm_end unconditionally to ensure this value remains updated should this curr_[start/end] to be clamped to the input range and VMAs, which also happens to simplify the logic.

CVE-2026-23417	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix constant blinding for PROBE_MEM32 stores BPF_ST | BPF_PROBE_MEM32 immediate store survive unblinded into JIT-compiled native code when bpf_jit_harden >= 1. The root cause is that convert_ctx_accesses() rewrites BPF_ST|BPF_MEM to BPF_ST|BPF_ bpf_jit_blind_constants() runs during JIT compilation. The blinding switch only matches BPF_ST|BPF_MEM (mode 0x60), not BPF_ST|BPF_PROBE_MEM32 (mode 0xa0) bpf_jit_blind_insn() alongside the existing BPF_ST|BPF_MEM cases. The blinding transformation is identical: load the blinded immediate into BPF_REG_AX via mov+x instruction must preserve the BPF_PROBE_MEM32 mode so the architecture JIT emits the correct arena addressing (R12-based on x86-64). Cannot use the BPF_STX directly instead.
CVE-2026-29144	SEPPmail Secure Email Gateway before version 15.0.3 allows an attacker to bypass subject sanitization and forge security tags using Unicode lookalike characters.
CVE-2026-35396	WeGIA is a Web manager for charitable institutions. Prior to 3.6.9, an Open Redirect vulnerability was identified in the /WeGIA/controle/control.php endpoint of the metodo=listarId and nomeClasse=IsaidaControle. The application fails to validate or restrict the nextPage parameter, allowing attackers to redirect users to arbitra malware distribution, and social engineering using the trusted WeGIA domain. This vulnerability is fixed in 3.6.9.
CVE-2026-35473	WeGIA is a Web manager for charitable institutions. Prior to 3.6.9, an Open Redirect vulnerability was identified in the /WeGIA/controle/control.php endpoint of the metodo=listarId and nomeClasse=IentradaControle. The application fails to validate or restrict the nextPage parameter, allowing attackers to redirect users to arbi malware distribution, and social engineering using the trusted WeGIA domain. This vulnerability is fixed in 3.6.9.
CVE-2026-29140	SEPPmail Secure Email Gateway before version 15.0.3 allows an attacker to cause attacker-controlled certificates to be used for future encryption to a victim by ad
CVE-2026-35454	The Code Extension Marketplace is an open-source alternative to the VS Code Marketplace. Prior to 2.4.2, Zip Slip vulnerability in coder/code-marketplace allowed passed raw zip entry names to a callback that wrote files via filepath.Join with no boundary check; filepath.Join resolved .. components but did not prevent the resu
CVE-2026-23424	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Validate command buffer payload count The count field in the command header exceed the remaining buffer space.
CVE-2026-23423	In the Linux kernel, the following vulnerability has been resolved: btrfs: free pages on error in btrfs_uring_read_extent() In this function the 'pages' object is never f executes in the future. But that's just the happy path. Along the way previous allocations might have gone wrong, or we might not get -EIOCBQUEUED from btrfs_e frees all memory allocated by this function without assuming any deferred execution, and this also needs to happen for the 'pages' allocation.
CVE-2026-29137	SEPPmail Secure Email Gateway before version 15.0.3 allows an attacker to hide security tags from users by crafting a long subject.
CVE-2026-29138	SEPPmail Secure Email Gateway before version 15.0.3 allows attackers with a specially crafted email address to claim another user's PGP signature as their own.
CVE-2026-29139	SEPPmail Secure Email Gateway before version 15.0.3 allows account takeover by abusing GINA account initialization to reset a victim account password.
CVE-2026-23422	In the Linux kernel, the following vulnerability has been resolved: dpaa2-switch: Fix interrupt storm after receiving bad if_id in IRQ handler Commit 31a7a0bbeb00 for if_id to avoid an out-of-bounds access. If an out-of-bounds if_id is detected, the interrupt status is not cleared. This may result in an interrupt storm. Clear the in experimental AI code review agent at Google.
CVE-2026-23421	In the Linux kernel, the following vulnerability has been resolved: drm/xe/configfs: Free ctx_restore_mid_bb in release ctx_restore_mid_bb memory is allocated in w ctx_restore_mid_bb[0].cs as well to avoid leaking the allocation when the configfs device is removed. (cherry picked from commit a235e7d0098337c3f2d1e8f3610
CVE-2026-35398	WeGIA is a Web manager for charitable institutions. Prior to 3.6.9, an Open Redirect vulnerability was identified in the /WeGIA/controle/control.php endpoint of the metodo=listarTodos & listarId_Nome and nomeClasse=OrigemControle. The application fails to validate or restrict the nextPage parameter, allowing attackers to r credential theft, malware distribution, and social engineering using the trusted WeGIA domain. This vulnerability is fixed in 3.6.9.
CVE-2026-29141	SEPPmail Secure Email Gateway before version 15.0.3 allows an attacker to bypass subject sanitization and forge tags such as [signed OK].
CVE-2026-29142	SEPPmail Secure Email Gateway before version 15.0.3 allows an attacker to forge a GINA-encrypted email.
CVE-2026-23420	In the Linux kernel, the following vulnerability has been resolved: wifi: wlcore: Fix a locking bug Make sure that wl->mutex is locked before it is unlocked. This has
CVE-2026-23419	In the Linux kernel, the following vulnerability has been resolved: net/rds: Fix circular locking dependency in rds_tcp_tune syzbot reported a circular locking depend socket lock: == WARNING: possible circular locking dependency detected == kworker/u10:8/15040 is trying to acquire lock: ffffffff8e9aaf80 (fs_reclain lock: ffff88805a3c1ce0 (k-sk_lock-AF_INET6){+.+.}-{0:0}, at: rds_tcp_tune+0xd7/0x930 The issue occurs because sk_net_refcnt_upgrade() performs memory alloc a circular dependency with fs_reclaim. Fix this by moving sk_net_refcnt_upgrade() outside the socket lock critical section. This is safe because the fields modified b concurrent code path at this point. v2: - Corrected fixes tag - check patch line wrap nits - ai commentary nits
CVE-2026-23418	In the Linux kernel, the following vulnerability has been resolved: drm/xe/reg_sr: Fix leak on xa_store failure Free the newly allocated entry when xa_store() fails to from commit 6bc6fec71ac45f52db609af4e62bdb96b9f5fadb)
CVE-2026-35472	WeGIA is a Web manager for charitable institutions. Prior to 3.6.9, an Open Redirect vulnerability was identified in the /WeGIA/controle/control.php endpoint of the metodo=listarTodos and nomeClasse=EstoqueControle. The application fails to validate or restrict the nextPage parameter, allowing attackers to redirect users to malware distribution, and social engineering using the trusted WeGIA domain. This vulnerability is fixed in 3.6.9.
CVE-2026-	WeGIA is a Web manager for charitable institutions. Prior to 3.6.9, a stored XSS vulnerability allows an attacker to inject malicious scripts through a backup filenam compromising session data or executing actions on behalf of the user. This vulnerability is fixed in 3.6.9.

35399	
CVE-2026-26927	Szafir SDK Web is a browser plug-in that can run SzafirHost application which download the necessary files when launched. In Szafir SDK Web it is possible to chan can craft a website that is able to launch SzafirHost application with arbitrary arguments via Szafir SDK Web browser addon. No validation will be performed to che related to the actual address of the calling web application. The URL address specified in `document_base_url` parameter is then shown in the application confirma in the context of attacker's website URL and might download additional files and libraries from that website. When victim accepts the application execution for the prompt won't be shown and the application will be called in the context of URL provided by the attacker without any interaction. This issue was fixed in version 0.0
CVE-2026-35053	OneUptime is an open-source monitoring and observability platform. Prior to version 10.0.42, the Worker service's ManualAPI exposes workflow execution endpoint without any authentication middleware. An attacker who can obtain or guess a workflow ID can trigger arbitrary workflow execution with attacker-controlled input This issue has been patched in version 10.0.42.
CVE-2026-34932	hoppscotch is an open source API development ecosystem. Prior to version 2026.3.0, there is a stored XSS vulnerability that can lead to CSRF. This issue has been
CVE-2026-34940	KubeAI is an AI inference operator for kubernetes. Prior to 0.23.2, the ollamaStartupProbeScript() function in internal/modelcontroller/engine_ollama.go constructs modelParam). This shell command is executed via bash -c as a Kubernetes startup probe. An attacker who can create or update Model custom resources can inject fixed in 0.23.2.
CVE-2026-31407	In the Linux kernel, the following vulnerability has been resolved: netfilter: conntrack: add missing netlink policy validations Hyunwoo Kim reports out-of-bounds ac validation. Extend the netlink policies accordingly. Quoting the reporter: nlattr_to_sctp() assigns the user-supplied CTA_PROTOINFO_SCTP_STATE value directly to c exp->dir = 100, the access at ct->master->tuplehash[100] reads 5600 bytes past the start of a 320-byte nf_conn object, causing a slab-out-of-bounds read confirm
CVE-2026-31408	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: SCO: Fix use-after-free in sco_recv_frame() due to missing sock_hold sco_recv_frame() holding a reference to the socket. A concurrent close() can free the socket between the lock release and the subsequent sk->sk_state access, resulting in a use-aft use sco_sock_hold() to safely hold a reference under the lock. Fix by using sco_sock_hold() to take a reference before releasing the lock, and adding sock_put() on
CVE-2026-31409	In the Linux kernel, the following vulnerability has been resolved: ksmbd: unset conn->binding on failed binding request When a multichannel SMB2_SESSION_SETU true but never clears it on the error path. This leaves the connection in a binding state where all subsequent ksmbd_session_lookup_all() calls fall back to the globa
CVE-2026-31410	In the Linux kernel, the following vulnerability has been resolved: ksmbd: use volume UUID in FS_OBJECT_ID_INFORMATION Use sb->s_uuid for a proper volume ide stfs.f_fsid obtained from vfs_statfs().
CVE-2026-34598	YesWiki is a wiki system written in PHP. Prior to version 4.6.0, a stored and blind XSS vulnerability exists in the form title field. A malicious attacker can inject JavaS When any user visits that injected page, the JavaScript payload gets executed. This issue has been patched in version 4.6.0.
CVE-2026-34593	Ash Framework is a declarative, extensible framework for building Elixir applications. Prior to version 3.22.0, Ash.Type.Module.cast_input/2 unconditionally creates starts with "Elixir.", before verifying whether the referenced module exists. Because Erlang atoms are never garbage-collected and the BEAM atom table has a hard to any resource attribute or argument of type :module can exhaust this table and crash the entire BEAM VM, taking down the application. This issue has been patch
CVE-2026-34969	Nhost is an open source Firebase alternative with GraphQL. Prior to 0.48.0, the auth service's OAuth provider callback flow places the refresh token directly into the history, server access logs, HTTP Referer headers, and proxy/CDN logs. Note that the refresh token is one-time use and all of these leak vectors are on owned infra in 0.48.0.
CVE-2026-34591	Poetry is a dependency manager for Python. From version 1.4.0 to before version 2.3.3, a crafted wheel can contain ../ paths that Poetry writes to disk without cont It is reachable from untrusted package artifacts during normal install flows. (Normally, installing a malicious wheel is not sufficient for execution of malicious code. imported or invoked by the user.). This issue has been patched in version 2.3.3.
CVE-2026-26928	SzafirHost downloads necessary files in the context of the initiating web page. When called, SzafirHost updates its dynamic library. JAR files are correctly verified b see if it had been digitally signed by the vendor. The application doesn't verify hash or vendor's digital signature of uploaded DLL, SO, JNILIB or DYLIB file. The atta by the application. This issue was fixed in version 1.1.0.
CVE-2026-33271	Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis True Image (Windows) before build 42902.
CVE-2026-34444	Lupa integrates the runtimes of Lua or LuaJIT2 into CPython. In 2.6 and earlier, attribute_filter is not consistently applied when attributes are accessed through buil restrictions and eventually achieve arbitrary code execution.
CVE-2026-28728	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis True Image (Windows) before build 42902.
CVE-2026-27774	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis True Image (Windows) before build 42902.
CVE-2026-34217	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.36, a scope modification vulnerability exists in @nyariv/sandboxjs. The vulnerability allows untrusted sand sandbox scope objects in the scope hierarchy to untrusted code; an unexpected and undesired exploit. While this could allow modifying scopes inside the sandbox execution. This vulnerability is fixed in 0.8.36.
CVE-2026-5664	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-30078. Reason: This candidate is a reservation duplicate of CVE-2026 candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2026-35002	Agno versions prior to 2.3.24 contain an arbitrary code execution vulnerability in the model execution component that allows attackers to execute arbitrary Python influence the field_type value in a FunctionCall to achieve remote code execution.
CVE-2026-31406	In the Linux kernel, the following vulnerability has been resolved: xfrm: Fix work re-schedule after cancel in xfrm_nat_keepalive_net_fini() After cancel_delayed_wor remaining states via __xfrm_state_delete(), which calls xfrm_nat_keepalive_state_updated() to re-schedule nat_keepalive_work. The following is a simple race scena xfrm_nat_keepalive_net_fini() cancel_delayed_work_sync(nat_keepalive_work); xfrm_state_fini() xfrm_state_flush() xfrm_state_delete(x) __xfrm_state_delete(x) xfrm rcu_barrier(); net_complete_free(); net_passive_dec(net); llist_add(&net->defer_free_list, &defer_free_list); cleanup_net() [Round 2] rcu_barrier(); net_complete_free

	this, cancel_delayed_work_sync() is replaced with disable_delayed_work_sync().
CVE-2026-34977	Aperi'Solve is an open-source steganalysis web platform. Prior to 3.2.1, when uploading a JPEG, a user can specify an optional password to accompany the JPEG. Th subsequently passed into a bash -c command, without any form of sanitization or validation. An unauthenticated attacker can achieve root-level RCE inside the wo uploaded images, analysis results, and plaintext steganography passwords stored on disk. Because the container shares a Docker network with PostgreSQL and Re or manipulate the job queue to poison results for other users. If Docker socket mounting or host volume mounts are present, this could escalate to full host compro fixed in 3.2.1.
CVE-2026-31405	In the Linux kernel, the following vulnerability has been resolved: media: dvb-net: fix OOB access in ULE extension header tables The ule_mandatory_ext_handlers[with 255 elements (valid indices 0-254), but the index htype is derived from network-controlled data as (ule_sndu_type & 0x00FF), giving a range of 0-255. When h OOB value may be called as a function pointer. Add a bounds check on htype against the array size before either table is accessed. Out-of-range values now cause
CVE-2026-34989	CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to 31.0.0.0, profile name (e.g., full name / username). An attacker can inject a malicious JavaScript payload into their profile name, which is then stored server-side. This stored encoding, leading to stored cross-site scripting (XSS). This vulnerability is fixed in 31.0.0.0.
CVE-2025-48651	StrongBox in Android before security patch level 2026-04-05 has a vulnerability of High Severity, aka A-434039170, A-467765081, A-467765894, and A-467762899
CVE-2026-34931	hoppscotch is an open source API development ecosystem. Prior to version 2026.3.0, there is an open redirect vulnerability that leads to token exfiltration. With th has been patched in version 2026.3.0.
CVE-2026-2737	A vulnerability exists in Progress Flowmon versions prior to 12.5.8 and 13.0.6, whereby an administrator who clicks a malicious link provided by an attacker may in
CVE-2026-35175	Ajenti is a Linux and BSD modular server admin panel. Prior to 2.2.15, an authenticated user (using the auth_users plugin authentication method) could install a cu
CVE-2026-34834	Bulwark Webmail is a self-hosted webmail client for Stalwart Mail Server. Prior to version 1.4.10, the verifyIdentity() function contained logic that returned true if no security checks and access/modify user settings via the /api/settings endpoint by providing arbitrary headers. This issue has been patched in version 1.4.10.
CVE-2026-34833	Bulwark Webmail is a self-hosted webmail client for Stalwart Mail Server. Prior to version 1.4.10, the GET /api/auth/session endpoint previously included the user's local caches, and network proxie. This issue has been patched in version 1.4.10.
CVE-2026-35166	Hugo is a static site generator. From 0.60.0 to before 0.159.2, links and image links in the default markdown to HTML renderer are not properly escaped. Hugo use are not affected. This vulnerability is fixed in 0.159.2.
CVE-2026-32871	FastMCP is a Pythonic way to build MCP servers and clients. Prior to version 3.2.0, the OpenAPIProvider in FastMCP exposes internal APIs to MCP clients by parsing requests to the backend service. A vulnerability exists in the _build_url() method. When an OpenAPI operation defines path parameters (e.g., /api/v1/users/{user_id without URL-encoding. Subsequently, urllib.parse.urljoin() resolves the final URL. Since urljoin() interprets ../ sequences as directory traversal, an attacker controllir prefix and access arbitrary backend endpoints. This results in authenticated SSRF, as requests are sent with the authorization headers configured in the MCP provi
CVE-2026-35052	D-Tale is the combination of a Flask back-end and a React front-end to view & analyze Pandas data structures. Prior to 3.22.0, users hosting D-Tale publicly while u allowing attackers to run malicious code on the server. This vulnerability is fixed in 3.22.0.
CVE-2026-35047	Brave CMS is an open-source CMS. Prior to 2.0.6, an Unrestricted File Upload vulnerability in the CKEditor endpoint allows attackers to upload arbitrary files, includi potentially resulting in full system compromise, data exfiltration, or service disruption. All users running affected versions of BraveCMS are impacted. This vulnerab
CVE-2026-34825	NocoBase is an AI-powered no-code/low-code platform for building business applications and enterprise solutions. Prior to version 2.0.30, NocoBase plugin-workflow without parameterization or escaping. Any user who triggers a workflow containing a SQL node with template variables from user-controlled data can inject arbitra
CVE-2026-34759	OneUptime is an open-source monitoring and observability platform. Prior to version 10.0.42, multiple notification API endpoints are registered without authenticat ClusterKeyAuthorization.isAuthorizedServiceMiddleware. These endpoints are externally reachable via the Nginx proxy at /notification/. Combined with a projectId l numbers on the victim's Twilio account and delete all existing alerting numbers. This issue has been patched in version 10.0.42.
CVE-2026-34743	XZ Utils provide a general-purpose data-compression library plus command-line tools. Prior to version 5.8.3, if lzma_index_decoder() was used to decode an Index t subsequent lzma_index_append() would allocate too little memory, and a buffer overflow would occur. This issue has been patched in version 5.8.3.
CVE-2026-34735	The Hytale Modding Wiki is a free service for Hytale mods to host their documentation & wikis. In version 1.2.0 and prior, the quickUpload() endpoint validates uplo but constructs the stored filename using the client-supplied file extension from getClientOriginalExtension(). These two checks are independent: an attacker can up file is stored on the public disk and is directly accessible via URL, allowing server-side code execution. At time of publication no known patches exist.
CVE-2026-34992	Antrea is a Kubernetes networking solution intended to be Kubernetes native. Prior to 2.4.5 and 2.5.2, a missing encryption vulnerability affects inter-Node Pod traf enabled (trafficEncryptionMode: ipsec), Antrea fails to apply encryption for IPv6 Pod traffic. While the IPv4 traffic is correctly encrypted via ESP (Encapsulating Secu packets are encapsulated (using Geneve or VXLAN) but bypass the IPsec encryption layer. Impacted Users: users with dual-stack clusters and IPsec encryption ena 2.4.5 and 2.5.2.
CVE-2026-35471	goshs is a SimpleHTTPServer written in Go. Prior to 2.0.0-beta.3, tdeleteFile() missing return after path traversal check. This vulnerability is fixed in 2.0.0-beta.3.
CVE-2026-35474	WeGIA is a Web manager for charitable institutions. Prior to 3.6.9, open redirect has been found in WeGIA webapp. The redirect parameter is taken directly from $_ header("Location: ...") call. This vulnerability is fixed in 3.6.9.
	In the Linux kernel, the following vulnerability has been resolved: PM: runtime: Fix a race condition related to device removal The following code in pm_runtime_wo /* Maybe the parent is now able to suspend. */ if (parent && !parent->power.ignore_children) { spin_unlock(&dev->power.lock); spin_lock(&parent->power.lock); rp >power.lock); } Fix this by inserting a flush_work() call in pm_runtime_remove(). Without this patch blktest block/001 triggers the following complaint sporadically:

CVE-2026-23452	ffff88812bef7198 by task kworker/u553:1/3081 Workqueue: pm pm_runtime_work Call Trace: <TASK> dump_stack_lvl+0x61/0x80 print_address_description.const __kasan_check_byte+0x42/0x60 lock_acquire.part.0+0x38/0x230 lock_acquire+0x70/0x160 _raw_spin_lock+0x36/0x50 rpm_suspend+0xc6a/0xfe0 rpm_idle+0x5 worker_thread+0x5eb/0xfe0 kthread+0x37b/0x480 ret_from_fork+0x6cb/0x920 ret_from_fork_asm+0x11/0x20 </TASK> Allocated by task 4314: kasan_save_stac __kasan_kmalloc+0xa0/0xb0 __kmalloc_noprof+0x311/0x990 scsi_alloc_target+0x122/0xb60 [scsi_mod] __scsi_scan_target+0x101/0x460 [scsi_mod] scsi_scan_ch store_scan+0x2d2/0x390 [scsi_mod] dev_attr_store+0x43/0x80 sysfs_kf_write+0xde/0x140 kernfs_fop_write_iter+0x3ef/0x670 vfs_write+0x506/0x1470 ksys_writ do_syscall_64+0xee/0xfc0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 Freed by task 4314: kasan_save_stack+0x2a/0x50 kasan_save_track+0x18/0x40 kasan_s scsi_target_dev_release+0x3d/0x60 [scsi_mod] device_release+0xa3/0x220 kobject_cleanup+0x105/0x3a0 kobject_put+0x72/0xd0 put_device+0x17/0x20 scsi_d kobject_cleanup+0x105/0x3a0 kobject_put+0x72/0xd0 put_device+0x17/0x20 scsi_device_put+0x7f/0xc0 [scsi_mod] sdev_store_delete+0xa5/0x120 [scsi_mod] c kernfs_fop_write_iter+0x3ef/0x670 vfs_write+0x506/0x1470 ksys_write+0xfd/0x230 __x64_sys_write+0x76/0xc0 x64_sys_call+0x213/0x1810
CVE-2026-34513	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, an unbounded DNS cache could result in excessive mem 3.13.4.
CVE-2024-36057	Koha Library before 23.05.10 fails to sanitize user-controllable filenames prior to unzipping, leading to remote code execution. The line "qx/unzip $filename -d $dir metacharacters because input data can be controlled by an attacker and is directly included in a system command, i.e., an attack can occur via malicious filename
CVE-2026-23441	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Prevent concurrent access to IPSec ASO context The query or updating IPSec offload c each PF, which contains a shared DMA-mapped context for all ASO operations. A race condition exists because the ASO spinlock is released before the hardware ha overwrites the shared context in the DMA area. When the first operation's completion is processed later, it reads this corrupted context, leading to unexpected beh within each IPSec offload object. The shared ASO context is now copied to this private context while the ASO spinlock is held. Subsequent processing uses this save
CVE-2026-23440	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix race condition during IPSec ESN update In IPSec full offload mode, the device repo this event by querying the IPSec ASO and checking that the esn_event_arm field is 0x0, which indicates an event has occurred. After handling the event, the driver exists in this handling path. After validating the event, the driver calls mlx5_accel_esp_modify_xfrm() to update the kernel's xfrm state. This function temporarily re setting esn_event_arm to 0x1. This prevents the driver from reprocessing the same ESN update if the hardware sends events for other reason. Since the next ESN an update, as it will happen long after this handling has finished. Processing the event twice causes the ESN high-order bits (esn_msb) to be incremented incorrect anti-replay failures and a complete halt of IPSec traffic. Fix this by re-arming the ESN event immediately after it is validated, before calling mlx5_accel_esp_modify_ the race window.
CVE-2026-23439	In the Linux kernel, the following vulnerability has been resolved: udp_tunnel: fix NULL deref caused by udp_sock_create6 when CONFIG_IPV6=n When CONFIG_IPV creating a socket. Callers such as fou_create() then proceed to dereference the uninitialized socket pointer, resulting in a NULL pointer dereference. The captured N RIP: 0010:fou_nl_add_doit (net/ipv4/fou_core.c:590 net/ipv4/fou_core.c:764) [...] Call Trace: <TASK> genl_family_rcv_msg_doit.constprop.0 (net/netlink/genetlink.c: netlink_rcv_skb (net/netlink/af_netlink.c:2550) genl_rcv (net/netlink/genetlink.c:1219) netlink_unicast (net/netlink/af_netlink.c:1319 net/netlink/af_netlink.c:1344) ne (discriminator 1) net/socket.c:742 (discriminator 1)) __sys_sendto (./include/linux/file.h:62 (discriminator 1) ./include/linux/file.h:83 (discriminator 1) net/socket.c:21 net/socket.c:2209 (discriminator 1) net/socket.c:2209 (discriminator 1)) do_syscall_64 (arch/x86/entry/syscall_64.c:63 (discriminator 1) arch/x86/entry/syscall_64.c: (net/arch/x86/entry/entry_64.S:130) This patch makes udp_sock_create6 return -EPFNOSUPPORT instead, so callers correctly take their error paths. There is only o
CVE-2026-23438	In the Linux kernel, the following vulnerability has been resolved: net: mvpp2: guard flow control update with global_tx_fc in buffer switching mvpp2_bm_switch_bu per-cpu and shared buffer pool modes. This function programs CM3 flow control registers via mvpp2_cm3_read()/mvpp2_cm3_write(), which dereference priv->cm3 device tree (the third reg entry added by commit 60523583b07c ("dts: marvell: add CM3 SRAM memory to cp11x ethernet device tree")), priv->cm3_base remains mvpp2_bm_switch_buffers(), for example an MTU change that crosses the jumbo frame threshold, will crash: Unable to handle kernel NULL pointer dereference at = 0x25: DABT (current EL), IL = 32 bits pc : readl+0x0/0x18 lr : mvpp2_cm3_read.isra.0+0x14/0x20 Call trace: readl+0x0/0x18 mvpp2_bm_pool_update_fc+0x40/ mvpp2_bm_switch_buffers.isra.0+0x80/0x1c0 mvpp2_change_mtu+0x140/0x380 __dev_set_mtu+0x1c/0x38 dev_set_mtu_ext+0x78/0x118 dev_set_mtu+0x48/0x other flow control call site in the driver already guards hardware access with either priv->global_tx_fc or port->tx_fc. mvpp2_bm_switch_buffers() is the only place re-enable calls in mvpp2_bm_switch_buffers(), consistent with the rest of the driver.
CVE-2026-23437	In the Linux kernel, the following vulnerability has been resolved: net: shaper: protect late read accesses to the hierarchy We look up a netdev during prep of Netli take its lock or RCU which are the actual protections. This is not proper, a conversion from a ref to a locked netdev must include a liveness check (a check if the ne needs a separate change to protect from creating the hierarchy after flush has already run.
CVE-2026-23436	In the Linux kernel, the following vulnerability has been resolved: net: shaper: protect from late creation of hierarchy We look up a netdev during prep of Netlink op lock or RCU which are the actual protections. The netdev may get unregistered in between the time we take the ref and the time we lock it. We may allocate the hi in pre- already, this saves us from the race and removes the need for dedicated lock/unlock callbacks completely. After all, if there's any chance of write happening lock for devices which don't support shapers but we're only dealing with SET operations here, not taking the lock would be optimizing for an error case.
CVE-2026-4277	An issue was discovered in 6.0 before 6.0.4, 5.2 before 5.2.13, and 4.2 before 4.2.30. Add permissions on inline model instances were not validated on submission series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank N05ec@LZU-DSLab for reporting this issue.
CVE-2026-23442	In the Linux kernel, the following vulnerability has been resolved: ipv6: add NULL checks for idev in SRv6 paths __in6_dev_get() can return NULL when the device h Add NULL checks for idev returned by __in6_dev_get() in both seg6_hmac_validate_skb() and ipv6_srh_rcv() to prevent potential NULL pointer dereferences.
CVE-2026-34514	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, an attacker who controls the content_type parameter in patched in version 3.13.4.
CVE-2026-34515	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, on Windows the static resource handler may expose info
CVE-2026-23435	In the Linux kernel, the following vulnerability has been resolved: perf/x86: Move event pointer setup earlier in x86_pmu_enable() A production AMD EPYC system c pointer dereference, address: 0000000000000198 RIP: x86_perf_event_update+0xc/0xa0 Call Trace: <NMI> amd_pmu_v2_handle_irq+0x1a6/0x390 perf_event_nr RDI=0, corresponding to the `if (unlikely(!hwc->event_base))` check in x86_perf_event_update() where hwc = &event->hw and event is NULL. drgn inspection of t >events[]: active_mask: 0x1e (bits 1, 2, 3, 4) events[1]: 0xff1100136cbd4f38 (valid) events[2]: 0x0 (NULL, but active_mask bit 2 set) events[3]: 0xff1100076fd2cf3 events[2] was found in event_list[2] with hw.idx=2 and hw.state=0x0, confirming x86_pmu_start() had run (which clears hw.state and sets active_mask) but event (STOPPED|UPTODATE|ARCH), showing it was stopped when the PMU rescheduled events, confirming the throttle-then-reschedule sequence occurred. The root caus record loss") which moved the cpuc->events[idx] assignment out of x86_pmu_start() and into step 2 of x86_pmu_enable(), after the PERF_HES_ARCH check. This b specifically the unthrottle path: perf_adjust_freq_unthr_events() -> perf_event_unthrottle_group() -> perf_event_unthrottle() -> event->pmu->start(event, 0) -> x8 perf events overflows, triggering group throttle via perf_event_throttle_group(). All events are stopped: active_mask bits cleared, events[] preserved (x86_pmu_sto (PERF_HES_STOPPED), x86_pmu_enable() runs due to other scheduling activity. Stopped events that need to move counters get PERF_HES_ARCH set and events[ol be skipped -- events[new_idx] is never set. 3. The timer tick unthrottles the group via pmu->start(). Since commit 7e772a93eb61 removed the events[] assignmen NULL. 4. A PMC overflow NMI fires. The handler iterates active counters, finds active_mask[2] set, reads events[2] which is NULL, and crashes dereferencing it. Mov PERF_HES_ARCH check, so that events[] is populated even for events that are not immediately started. This ensures the unthrottle path via pmu->start() always fir

CVE-2026-23434	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: serialize lock/unlock against other NAND operations nand_lock() and nand_unlock(controllers that implement SET_FEATURES via multiple low-level PIO commands, these can race with concurrent UBI/UBIFS background erase/write operations that nand_get_device()/nand_release_device() around the lock/unlock operations to serialize them against all other NAND controller access.
CVE-2026-23433	In the Linux kernel, the following vulnerability has been resolved: arm_mpam: Fix null pointer dereference when restoring bandwidth counters When an MSC suppo mpam_restore_mbwu_state() calls __ris_msmon_read() via ipi to restore the configuration of the bandwidth counters. It doesn't care about the value read, mbwu_a __ris_msmon_read() adds to it. This results in a kernel oops with a call trace such as: Call trace: __ris_msmon_read+0x19c/0x64c (P) mpam_restore_mbwu_state+0 worker_thread+0x188/0x310 kthread+0x11c/0x130 ret_from_fork+0x10/0x20 Provide a local variable for val to avoid __ris_msmon_read() dereferencing a null poi
CVE-2026-34517	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, for some multipart form fields, aiohttp read the entire fie version 3.13.4.
CVE-2026-34518	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, when following redirects to a different origin, aiohttp dro This issue has been patched in version 3.13.4.
CVE-2025-24817	Nokia MantaRay NM is vulnerable to an OS command injection vulnerability due to improper neutralization of special elements used in an OS command in Sympton
CVE-2026-23443	In the Linux kernel, the following vulnerability has been resolved: ACPI: processor: Fix previous acpi_processor_errata_piix4() fix After commi f132e089fe89 ("ACPI: pointers may be dereferenced after dropping references to the device objects pointed to by them, which may cause a use-after-free to occur. Moreover, debug me them are unset. Address all of these issues by moving message printing to the points in the code where the errata flags are set.
CVE-2026-35475	WeGIA is a Web manager for charitable institutions. Prior to 3.6.9, the redirect parameter is taken directly from $_GET with no URL validation or whitelist check, the
CVE-2026-23447	In the Linux kernel, the following vulnerability has been resolved: net: usb: cdc_ncm: add ndpoffset to NDP32 nframes bounds check The same bounds-check bug f DPE array size is validated against the total skb length without accounting for ndpoffset, allowing out-of-bounds reads when the NDP32 is placed near the end of th the NDP-plus-DPE-array size more clearly. Compile-tested only.
CVE-2026-23451	In the Linux kernel, the following vulnerability has been resolved: bonding: prevent potential infinite loop in bond_header_parse() bond_header_parse() can loop if a hierarchy top. Add new "const struct net_device *dev" parameter to (struct header_ops)->parse() method to make sure the recursion is bounded, and that the fina
CVE-2026-23450	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix NULL dereference and UAF in smc_tcp_syn_recv_sock() Syzkaller reported a panic in (softirq) via icsk_af_ops->syn_recv_sock on the clcsock (TCP listening socket). It reads sk_user_data to get the smc_sock pointer. However, when the SMC listen soc NULL under sk_callback_lock, and then the smc_sock itself can be freed via sock_put() in smc_release(). This leads to two issues: 1) NULL pointer dereference: sk_u but the smc_sock is freed before its fields (e.g., queued_smc_hs, ori_af_ops) are accessed. The race window looks like this (the syzkaller crash [1] triggers via the S tcp_check_req() path has the same race): CPU A (softirq) CPU B (process ctx) tcp_v4_rcv() TCP_NEW_SYN_RECV: sk = req->rsk_listener sock_hold(sk) /* No lock on write_unlock_bh(cb_lock) ... smc_clcsock_release() sock_put(smc->sk) x2 -> smc_sock freed! tcp_check_req() smc_tcp_syn_recv_sock(): smc = user_data(sk) -> NU are two independent objects with separate refcounts. TCP stack holds a reference on the clcsock, which keeps it alive, but this does NOT prevent the smc_sock fro smc_sock. Since smc_tcp_syn_recv_sock() is called in the TCP three-way handshake path, taking read_lock_bh on sk_callback_lock is too heavy and would not survi SOCK_RCU_FREE on the SMC listen socket so that smc_sock freeing is deferred until after the RCU grace period. This guarantees the memory is still valid when acc Use refcount_inc_not_zero(&smc->sk.sk_refcnt) to pin the smc_sock. If the refcount has already reached zero (close path completed), it returns false and we bail ou rcu_read_lock(), but it only checks for NULL and accesses the global smc_hs_wq, never dereferencing any smc_sock field, so it is not affected. Reproducer was verif applied. [1] https://syzkaller.appspot.com/bug?extid=827ae2bfb3a3529333e9
CVE-2026-5199	A writer role user in an attacker-controlled namespace could signal, delete, and reset workflows or activities in a victim namespace on the same cluster. Exploitatic operations, signal names. This was due to a bug introduced in Temporal Server v1.29.0 which inadvertently allowed an attacker to control the namespace name va code. The batch activity validated the namespace ID but did not cross-check the namespace name against the worker's bound namespace, allowing the per-names Exploitation requires a server configuration where internal components have cross-namespace authorization, such as deployment of the internal-frontend service c impacted Temporal Cloud when the attacker and victim namespaces were on the same cell, with the same preconditions as self-hosted clusters.
CVE-2026-23449	In the Linux kernel, the following vulnerability has been resolved: net/sched: teql: Fix double-free in teql_master_xmit Whenever a TEQL devices has a lockless Qdis datapath. Failure to do so may cause crashes like the following: [238.028993][T318] BUG: KASAN: double-free in skb_release_data (net/core/skbuff.c:1139) [238. 238.029749][T318] [238.029900][T318] CPU: 3 UID: 0 PID: 318 Comm: poc_teql_ke Not tainted 7.0.0-rc3-00149-ge5b31d988a41 #704 PREEMPT(full) [238.0299 T318] Call Trace: [238.029913][T318] <TASK> [238.029916][T318] dump_stack_lvl (lib/dump_stack.c:122) [238.029928][T318] print_report (mm/kasan/report. (net/core/skbuff.c:1139) [238.029944][T318] ? srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) ... [238.029957][T318] ? skb_release_data (net/core/skbuff. mm/kasan/report.c:563) [238.029979][T318] ? skb_release_data (net/core/skbuff.c:1139) [238.029989][T318] check_slab_allocation (mm/kasan/common.c:231) mm/slub.c:6168 (discriminator 1) mm/slub.c:6298 (discriminator 1)) [238.030004][T318] skb_release_data (net/core/skbuff.c:1139) ... [238.030025][T318] sk_sk (./include/linux/ptr_ring.h:171 ./include/linux/ptr_ring.h:309 ./include/linux/skb_array.h:98 net/sched/sch_generic.c:827) [238.030039][T318] ? srso_alias_return_th (net/sched/sch_generic.c:1034) [238.030062][T318] teql_destroy (./include/linux/spinlock.h:395 net/sched/sch_teql.c:157) [238.030071][T318] __qdisc_destroy (qdisc_graft (net/sched/sch_api.c:1062 net/sched/sch_api.c:1053 net/sched/sch_api.c:1159) [238.030089][T318] ? __pfx_qdisc_graft (net/sched/sch_api.c:1091) [2 238.030102][T318] ? srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) [238.030106][T318] ? srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) [238.03(238.072958][T318] Allocated by task 303 on cpu 5 at 238.026275s: [238.073392][T318] kasan_save_stack (mm/kasan/common.c:58) [238.073884][T318] kasa (discriminator 5)) [238.074230][T318] __kasan_slab_alloc (mm/kasan/common.c:369) [238.074578][T318] kmem_cache_alloc_node_noprof (./include/linux/kasan kmalloc_reserve (net/core/skbuff.c:616 (discriminator 107)) [238.076450][T318] __alloc_skb (net/core/skbuff.c:713) [238.076834][T318] alloc_skb_with_frags (./i sock_alloc_send_pskb (net/core/sock.c:2997) [238.077520][T318] packet_sendmsg (net/packet/af_packet.c:2926 net/packet/af_packet.c:3019 net/packet/af_packe 238.028496s: [238.082761][T318] kasan_save_stack (mm/kasan/common.c:58) [238.083481][T318] kasan_save_track (mm/kasan/common.c:64 (discriminator 5 kasan_save_free_info (mm/kasan/generic.c:587 (discriminator 1)) [238.085900][T318] __kasan_slab_free (mm/ ---truncated---
CVE-2026-34455	Hi.Events is an open-source event management and ticket selling platform. From version 0.8.0-beta.1 to before version 1.7.1-beta, multiple repository classes pass validation, enabling SQL injection. The application uses PostgreSQL which supports stacked queries. This issue has been patched in version 1.7.1-beta.
CVE-2026-23448	In the Linux kernel, the following vulnerability has been resolved: net: usb: cdc_ncm: add ndpoffset to NDP16 nframes bounds check cdc_ncm_rx_verify_ndp16() va correctly accounts for ndpoffset: if ((ndpoffset + sizeof(struct usb_cdc_ncm_ndp16)) > skb_in->len) but the second check omits it: if ((sizeof(struct usb_cdc_ncm_n DPE array size against the total skb length as if the NDP were at offset 0, rather than at ndpoffset. When the NDP is placed near the end of the NTB (large wNdpInd passes. cdc_ncm_rx_fixup() then reads out-of-bounds memory when iterating the DPE array. Add ndpoffset to the nframes bounds check and use struct_size_t() to
CVE-2026-35515	Nest is a framework for building scalable Node.js server-side applications. Prior to 11.1.18, SseStream._transform() interpolates message.type and message.id dire (\r, \n). Since the SSE protocol treats both \r and \n as field delimiters and \n\n as event boundaries, an attacker who can influence these fields through upstream d reconnection state. This vulnerability is fixed in 11.1.18.

CVE-2026-23446	In the Linux kernel, the following vulnerability has been resolved: net: usb: aqc111: Do not perform PM inside suspend callback syzbot reports "task hung in rpm_re routine. The simplified call trace looks like this: rpm_suspend() usb_suspend_both() - here udev->dev.power.runtime_status == RPM_SUSPENDING aqc111_suspend usb_autopm_get_interface() pm_runtime_resume_and_get() rpm_resume() - here we call rpm_resume() on our parent rpm_resume() - Here we wait for a status cha and locks up the whole networking stack. Fix this by replacing the write_cmd calls with their _nopm variants
CVE-2025-52908	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1280, 1330, 1380, 1480, 1580, W920, W930, a overflow via a certain ioctl message, issue 1 of 2.
CVE-2026-23445	In the Linux kernel, the following vulnerability has been resolved: igc: fix page fault in XDP TX timestamps handling If an XDP application that requested TX timesta kernel splat is reported: [883.803618] [T1554] BUG: unable to handle page fault for address: ffffcfb6200fd008 ... [883.803650] [T1554] Call Trace: [883.803652 [883.803660] [T1554] igc_tsync_interrupt+0x2d5/0x300 [igc] ... During shutdown of the TX ring the xsk_meta pointers are left behind, so that the IRQ handler is t data on TX shutdown. TX timestamps on other queues remain unaffected.
CVE-2026-23444	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: always free skb on ieee80211_tx_prepare_skb() failure ieee80211_tx_prepare_sk (ieee80211_tx_prepare() returning TX_DROP) does not free it, while invoke_tx_handlers() failure and the fragmentation check both do. Add kfree_skb() to the first e (ath9k, mt76, mac80211_hwsim) to avoid double-free. Document the skb ownership guarantee in the function's kdoc.
CVE-2026-33816	Memory-safety vulnerability in github.com/jackc/pgx/v5.
CVE-2026-33815	Memory-safety vulnerability in github.com/jackc/pgx/v5.
CVE-2026-30460	Daylight Studio FuelCMS v1.5.2 was discovered to contain an authenticated remote code execution (RCE) vulnerability in the Blocks module.
CVE-2026-1079	A native messaging host vulnerability in Pega Browser Extension (PBE) affects users of all versions of Pega Robotic Automation who have installed Pega Browser Ex PBE. The vulnerability could occur if a user navigates to this website. The malicious website could then present an unexpected message box.
CVE-2026-1078	An arbitrary file-write vulnerability in Pega Browser Extension (PBE) affects Pega Robotic Automation version 22.1 or R25 users who are running automations that v includes malicious code. The vulnerability could occur if a Robot Runtime user navigates to the malicious website.
CVE-2026-23432	In the Linux kernel, the following vulnerability has been resolved: mshv: Fix use-after-free in mshv_map_user_memory error path In the error path of mshv_map_us When userspace later unmaps the memory, the notifier fires and accesses the freed region, causing a use-after-free and potential kernel panic. Replace vfree() wit region.
CVE-2026-35458	Gotenberg is an API for converting document formats. In 8.29.1 and earlier, Gotenberg uses dlclark/regexp2 to compile user-supplied scope patterns without settin indefinitely.
CVE-2026-34519	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, an attacker who controls the reason parameter when cre has been patched in version 3.13.4.
CVE-2026-1839	A vulnerability in the HuggingFace Transformers library, specifically in the `Trainer` class, allows for arbitrary code execution. The `_load_rng_state()` method in `s `weights_only=True` parameter. This issue affects all versions of the library supporting `torch>=2.2` when used with PyTorch versions below 2.6, as the `safe_glo exploit this vulnerability by supplying a malicious checkpoint file, such as `rng_state.pth`, which can execute arbitrary code when loaded. The issue is resolved in v
CVE-2026-4420	Bludit is vulnerable to Stored Cross-Site Scripting (XSS) in its page creating functionality. An authenticated attacker with page creation privileges (such as Author, E newly created article. This payload will be executed when a victim visits the URL of the uploaded resource. The uploaded resource itself is accessible without authe administrator if the victim has enough privileges. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulne vulnerable, other versions were not tested and might also be vulnerable.
CVE-2025-59710	An issue was discovered in Biztalk360 before 11.5. Because of incorrect access control, any user is able to request the loading a DLL file. During the loading, a met to achieve remote code execution on the server.
CVE-2025-59709	An issue was discovered in Biztalk360 through 11.5. because of mishandling of user-provided input in a path to be read by the server, a Super User attacker is able Directory Traversal.
CVE-2026-3882	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-28810	Generation of Predictable Numbers or Identifiers vulnerability in Erlang/OTP kernel (inet_res, inet_db modules) allows DNS Cache Poisoning. The built-in DNS resolv and does not implement source port randomization. Response validation relies almost entirely on this ID, making DNS cache poisoning practical for an attacker wh recommendations for mitigating forged DNS answers. inet_res is intended for use in trusted network environments and with trusted recursive resolvers. Earlier doc to deploy the resolver in environments where spoofed DNS responses are possible. This vulnerability is associated with program files lib/kernel/src/inet_db.erl and l 27.3.4.10 and 26.2.5.19 corresponding to kernel from 3.0 until 10.6.2, 10.2.7.4 and 9.2.4.11.
CVE-2026-4759	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-1114	In parisneo/lollms version 2.1.0, the application's session management is vulnerable to improper access control due to the use of a weak secret key for signing JSO force attack to recover the secret key. Once the secret key is obtained, the attacker can forge administrative tokens by modifying the JWT payload and resigning it impersonate the administrator, and gain access to restricted endpoints. The issue is resolved in version 2.2.0.
CVE-2026-23426	In the Linux kernel, the following vulnerability has been resolved: drm/logicvc: Fix device node reference leak in logicvc_drm_config_parse() The logicvc_drm_config release the reference, leading to a device node reference leak. Fix this by using the __free(device_node) cleanup attribute to automatic release the reference when

CVE-2026-34525	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, multiple Host headers were allowed in aiohttp. This issue
CVE-2026-23425	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Fix ID register initialization for non-protected pKVM guests In protected mode, the h protected VMs, this structure is initialized from the host's `kvm` state. Currently, `pkvm_init_features_from_host()` copies the `KVM_ARCH_FLAG_ID_REGS_INITIALIZ results in the hypervisor seeing the flag as set while the ID registers remain zeroed. Consequently, `kvm_has_feat()` checks at EL2 fail (return 0) for non-protected TCR2_EL1 support. As a result, certain system registers (e.g., TCR2_EL1, PIR_EL1, POR_EL1) are not saved/restored during the world switch, which could lead to sta hypervisor `kvm` for non-protected VMs during initialization, since we trust the host with its non-protected guests' features. Also ensure `KVM_ARCH_FLAG_ID_REG `vm_copy_id_regs` can properly initialize them and set the flag once done.
CVE-2026-29131	SEPPmail Secure Email Gateway before version 15.0.3 allows attackers with a specially crafted email address to read the contents of emails encrypted for other us
CVE-2026-29132	SEPPmail Secure Email Gateway before version 15.0.3 allows an attacker with access to a victim's GINA account to bypass a second-password check and read prot
CVE-2026-29133	SEPPmail Secure Email Gateway before version 15.0.3 allows an attacker to upload PGP keys with UIDs that do not match their email address.
CVE-2026-29134	SEPPmail Secure Email Gateway before version 15.0.3 allows an external user to modify GINA webdomain metadata and bypass per-domain restrictions.
CVE-2026-29135	SEPPmail Secure Email Gateway before version 15.0.3 allows an attacker to craft a password-tag that bypasses subject sanitization.
CVE-2026-29136	SEPPmail Secure Email Gateway before version 15.0.3 allows an attacker to inject HTML into notification emails about new CA certificates.
CVE-2025-68152	Juju is an open source application orchestration engine that enables any application operation on any infrastructure at any scale through special operators called ‘c a compromised workload machine under a Juju controller can read any log file for any entity in any model at any level. This issue has been patched in versions 2.9.
CVE-2025-39666	Local privilege escalation in Checkmk 2.2.0 (EOL), Checkmk 2.3.0 before 2.3.0p46, Checkmk 2.4.0 before 2.4.0p25, and Checkmk 2.5.0 (beta) before 2.5.0b3 allow context that are processed when the `omd` administrative command is run by root.
CVE-2025-68153	Juju is an open source application orchestration engine that enables any application operation on any infrastructure at any scale through special operators called ‘c user, machine or controller under a Juju controller can modify the resources of an application within the entire controller. This issue has been patched in versions 2
CVE-2026-23427	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in durable v2 replay of active file handles parse_durable_handle_context a DURABLE_REQ_V2 context with SMB2_FLAGS_REPLAY_OPERATION. ksmbd_lookup_fd_cguid() does not filter by fp->conn, so it returns file handles that are already overwriting connection is subsequently freed, __ksmbd_close_fd() dereferences the stale fp->conn via spin_lock(&fp->conn->llist_lock), causing a use-after-free. KA == [7.349607] BUG: KASAN: slab-use-after-free in _raw_ kworker/1:2/108 [7.350010] [7.350064] CPU: 1 UID: 0 PID: 108 Comm: kworker/1:2 Not tainted 7.0.0-rc3+ #58 PREEMPTLAZY [7.350068] Hardware name: QEMU 04/01/2014 [7.350070] Workqueue: ksmbd-io handle_ksmbd_work [7.350083] Call Trace: [7.350087] <TASK> [7.350087] dump_stack_lvl+0x64/0x80 [7.350094 7.350101] ? __pfx___mod_timer+0x10/0x10 [7.350106] ? _raw_spin_lock+0x75/0xe0 [7.350108] kasan_report+0xce/0x100 [7.350109] ? _raw_spin_lock+0x75/0x _raw_spin_lock+0x75/0xe0 [7.350118] ? __pfx__raw_spin_lock+0x10/0x10 [7.350119] ? __call_rcu_common.constprop.0+0x25e/0x780 [7.350125] ? close_id_del ksmbd_close_fd+0x135/0x1b0 [7.350133] smb2_close+0xb19/0x15b0 [7.350142] ? __pfx_smb2_close+0x10/0x10 [7.350143] ? xas_load+0x18/0x270 [7.35014 7.350150] ? _raw_spin_unlock+0xe/0x30 [7.350151] ? ksmbd_smb2_check_message+0xeb2/0x24c0 [7.350153] ? ksmbd_tree_conn_lookup+0xcd/0xf0 [7.35015 7.350162] ? assign_work+0x122/0x3e0 [7.350163] worker_thread+0x54b/0xf70 [7.350165] ? __pfx_worker_thread+0x10/0x10 [7.350166] kthread+0x346/0x47 __pfx_kthread+0x10/0x10 [7.350178] ret_from_fork+0x4fb/0x6c0 [7.350183] ? __pfx_ret_from_fork+0x10/0x10 [7.350185] ? __switch_to+0x36c/0xbe0 [7.35018 </TASK> [7.350197] [7.355160] Allocated by task 123: [7.355261] kasan_save_stack+0x33/0x60 [7.355373] kasan_save_track+0x14/0x30 [7.355484] __kasan ksmbd_kthread_fn+0x243/0xd70 [7.355839] kthread+0x346/0x470 [7.355942] ret_from_fork+0x4fb/0x6c0 [7.356051] ret_from_fork_asm+0x1a/0x30 [7.35616 7.356416] kasan_save_track+0x14/0x30 [7.356527] kasan_save_free_info+0x3b/0x60 [7.356646] __kasan_slab_free+0x43/0x70 [7.356761] kfree+0x1ca/0x430 ksmbd_conn_handler_loop+0x77e/0xd40 [7.357138] kthread+0x346/0x470 [7.357240] ret_from_fork+0x4fb/0x6c0 [7.357350] ret_from_fork_asm+0x1a/0x30 [7 7.357513] which belongs to the cache kmalloc-1k of size 1024 [7.357857] The buggy address is located 396 bytes inside of [7.357857] freed 1024-byte region ---
CVE-2026-23431	In the Linux kernel, the following vulnerability has been resolved: spi: amlogic-spisg: Fix memory leak in aml_spisg_probe() In aml_spisg_probe(), ctlr is allocated by paths. This leads to a memory leak whenever the driver fails to probe after the initial allocation. Convert to use devm_spi_alloc_host()/devm_spi_alloc_target() to fix
CVE-2026-30079	In OpenAirInterface V2.2.0 AMF, Out of sequence messages causes incorrect state transition during UE registration procedure. This allows authentication to be byp InitialUERegistration, a registration reject is received followed by a registration accept! This leads the UE to be registered without proper authentication.
CVE-2026-23430	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Don't overwrite KMS surface dirty tracker We were overwriting the surface's dirty tr
CVE-2026-23429	In the Linux kernel, the following vulnerability has been resolved: iommu/sva: Fix crash in iommu_sva_unbind_device() domain->mm->iommu_mm can be freed by After iommu_domain_free() returns, accessing domain->mm->iommu_mm may dereference a freed mm structure, leading to a crash. Fix this by moving the code
	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free of share_conf in compound request smb2_get_ksmbd_tcon() reuses work ksmbd_tree_conn_lookup() checks t_state == TREE_CONNECTED on the initial lookup path, but the compound reuse path bypasses this check entirely. If a prior co TREE_DISCONNECTED and frees share_conf via ksmbd_share_config_put(), subsequent commands dereference the freed share_conf through work->tcon->share_c == [4.145059] BUG: KASAN: slab-use-after-free in smb2 kworker/1:1/44 [4.145772] [4.145867] CPU: 1 UID: 0 PID: 44 Comm: kworker/1:1 Not tainted 7.0.0-rc3+ #60 PREEMPTLAZY [4.145871] Hardware name: QEMU U

CVE-2026-23428	04/01/2014 [4.145875] Workqueue: ksmbd-io handle_ksmbd_work [4.145888] Call Trace: [4.145892] <TASK> [4.145894] dump_stack_lvl+0x64/0x80 [4.14591(4.145928] ? smb2_write+0xc74/0xe70 [4.145931] kasan_report+0xce/0x100 [4.145934] ? smb2_write+0xc74/0xe70 [4.145937] smb2_write+0xc74/0xe70 [4.1 4.145945] ? ksmbd_smb2_check_message+0xeb2/0x24c0 [4.145948] ? smb2_tree_disconnect+0x31c/0x480 [4.145951] handle_ksmbd_work+0x40f/0x1080 [4.1 4.145964] worker_thread+0x54b/0xf70 [4.145967] ? __pfx_worker_thread+0x10/0x10 [4.145970] kthread+0x346/0x470 [4.145976] ? recalc_sigpending+0x19b/ ret_from_fork+0x4fb/0x6c0 [4.145992] ? __pfx_ret_from_fork+0x10/0x10 [4.145995] ? __switch_to+0x36c/0xbe0 [4.145999] ? __pfx_kthread+0x10/0x10 [4.146(Allocated by task 44: [4.149953] kasan_save_stack+0x33/0x60 [4.150061] kasan_save_track+0x14/0x30 [4.150169] __kasan_kmalloc+0x8f/0xa0 [4.150274] ks ksmbd_tree_conn_connect+0x7e/0x600 [4.150529] smb2_tree_connect+0x2e6/0x1000 [4.150645] handle_ksmbd_work+0x40f/0x1080 [4.150761] process_one_ kthread+0x346/0x470 [4.151071] ret_from_fork+0x4fb/0x6c0 [4.151176] ret_from_fork_asm+0x1a/0x30 [4.151286] [4.151332] Freed by task 44: [4.151418] k kasan_save_free_info+0x3b/0x60 [4.151751] __kasan_slab_free+0x43/0x70 [4.151861] kfree+0x1ca/0x430 [4.151952] __ksmbd_tree_conn_disconnect+0xc8/0x handle_ksmbd_work+0x40f/0x1080 [4.152326] process_one_work+0x5fa/0xef0 [4.152438] worker_thread+0x54b/0xf70 [4.152545] kthread+0x346/0x470 [4.15 4.152853] [4.152900] The buggy address belongs to the object at ffff88810430c180 [4.152900] which belongs to the cache kmalloc-96 of size 96 [4.153226] The [ffff88810430c180, ffff88810430c1e0) [4.153549] [4.153596] The buggy address belongs to the physical page: [4.153750] page: refcount:0 mapcount:0 mappin -truncated---
CVE-2025-62818	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1 An out-of-bounds write occurs due to a mismatch between the TP-UDHI and UDL values when processing an SMS TP-UD packet.
CVE-2025-52909	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1280, 1330, 1380, 1480, 1580, W920, W930, ar overflow via a certain ioctl message, issue 2 of 2.
CVE-2026-5627	A path traversal vulnerability exists in mintplex-labs/anything-llm versions up to and including 1.9.1, within the `AgentFlows` component. The vulnerability arises fr `server/utils/agentFlows/index.js`. Specifically, the combination of `path.join` and `normalizePath` allows attackers to bypass directory restrictions and access or d as leaking sensitive configuration files containing API keys, or denial of service by deleting critical files like `package.json`. The issue is resolved in version 1.12.1.
CVE-2026-3987	A path traversal vulnerability in the Fireware OS Web UI on WatchGuard Firebox systems may allow a privileged authenticated remote attacker to execute arbitrary 12.6.1 up to and including 12.11.8 and 2025.1 up to and including 2026.1.2.
CVE-2025-0711	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2026-3466	Insufficient sanitization of dashboard dashlet title links in Checkmk 2.2.0 (EOL), Checkmk 2.3.0 before 2.3.0p46, Checkmk 2.4.0 before 2.4.0p25, and Checkmk 2.5. perform stored cross-site scripting (XSS) attacks by tricking a victim into clicking a crafted dashlet title link on a shared dashboard.
CVE-2026-33866	MLflow is vulnerable to an authorization bypass affecting the AJAX endpoint used to download saved model artifacts. Due to missing access-control validation, a us retrieve model artifacts they are not authorized to access. This issue affects MLflow version through 3.10.1
CVE-2026-33865	MLflow is vulnerable to Stored Cross-Site Scripting (XSS) caused by unsafe parsing of YAML-based MLmodel artifacts in its web interface. An authenticated attacker user views the artifact in the UI. This allows actions such as session hijacking or performing operations on behalf of the victim. This issue affects MLflow version thr
CVE-2026-32144	Improper Certificate Validation vulnerability in Erlang OTP public_key (pubkey_ocsp module) allows OCSP designated-responder authorization bypass via missing si does not verify that a CA-designated responder certificate was cryptographically signed by the issuing CA. Instead, it only checks that the responder certificate's is OCSPSigning extended key usage. An attacker who can intercept or control OCSP responses can create a self-signed certificate with a matching issuer name and th as valid. This affects SSL/TLS clients using OCSP stapling, which may accept connections to servers with revoked certificates, potentially transmitting sensitive data directly are also affected, with impact depending on usage context. This vulnerability is associated with program files lib/public_key/src/pubkey_ocsp.erl and progra 27.0 until OTP 28.4.2 and 27.3.4.10 corresponding to public_key from 1.16 until 1.20.3 and 1.17.1.2, and ssl from 11.2 until 11.5.4 and 11.2.12.7.
CVE-2026-28808	Incorrect Authorization vulnerability in Erlang OTP (inets modules) allows unauthenticated access to CGI scripts protected by directory rules when served via script_ mod_auth evaluates directory-based access controls against the DocumentRoot-relative path while mod_cgi executes the script at the ScriptAlias-resolved path. Th were meant to protect. This vulnerability is associated with program files lib/inets/src/http_server/mod_alias.erl, lib/inets/src/http_server/mod_auth.erl, and lib/inets 27.3.4.10 and 26.2.5.19 corresponding to inets from 5.10 until 9.6.2, 9.3.2.4 and 9.1.0.6.
CVE-2026-4656	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.