SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 04 February 2026

Generated on 04 February 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-2026-23830	SandboxJS is a JavaScript sandboxing library. Versions prior to 0.8.26 have a sandbox escape vulnerability due to `AsyncFunction` not being isolated in `SandboxFunction`. The library attempts to sandbox code execution by replacing the global `Function` constructor with a safe, sandboxed version (`SandboxFunction`). This is handled in `utils.ts` by mapping `Function` to `sandboxFunction` within a map used for lookups. However, before version 0.8.26, the library did not include mappings for `AsyncFunction`, `GeneratorFunction`, and `AsyncGeneratorFunction`. These constructors are not global properties but can be accessed via the `.constructor` property of an instance (e.g., `(async () => {}).constructor`). In `executor.ts`, property access is handled. When code running inside the sandbox accesses `.constructor` on an async function (which the sandbox allows creating), the `executor` retrieves the property value. Since `AsyncFunction` was not in the safe-replacement map, the `executor` returns the actual native host `AsyncFunction` constructor. Constructors for functions in JavaScript (like `Function`, `AsyncFunction`) create functions that execute in the global scope. By obtaining the host `AsyncFunction` constructor, an attacker can create a new async function that executes entirely outside the sandbox context, bypassing all restrictions and gaining full access to the host environment (Remote Code Execution). Version 0.8.26 patches this vulnerability.	10.0	More Details
CVE-2025-57792	Explorance Blue versions prior to 8.14.9 contain a SQL injection vulnerability caused by insufficient validation of user input in a web application endpoint. An attacker can supply crafted input that is executed as part of backend database queries. The issue is exploitable without authentication, significantly raising the risk.	10.0	More Details
	In the Eclipse Theia Website repository, the GitHub Actions workflow		

CVE-2026-1699	.github/workflows/preview.yml used pull_request_target trigger while checking out and executing untrusted pull request code. This allowed any GitHub user to execute arbitrary code in the repository's CI environment with access to repository secrets and a GITHUB_TOKEN with extensive write permissions (contents:write, packages:write, pages:write, actions:write). An attacker could exfiltrate secrets, publish malicious packages to the eclipse-theia organization, modify the official Theia website, and push malicious code to the repository.	10.0	More Details
CVE-2026-25142	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.27, SanboxJS does not properly restrict __lookupGetter__ which can be used to obtain prototypes, which can be used for escaping the sandbox / remote code execution. This vulnerability is fixed in 0.8.27.	10.0	More Details
CVE-2025-70841	Dokans Multi-Tenancy Based eCommerce Platform SaaS 3.9.2 allows unauthenticated remote attackers to obtain sensitive application configuration data via direct request to /script/.env file. The exposed file contains Laravel application encryption key (APP_KEY), database credentials, SMTP/SendGrid API credentials, and internal configuration parameters, enabling complete system compromise including authentication bypass via session token forgery, direct database access to all tenant data, and email infrastructure takeover. Due to the multi-tenancy architecture, this vulnerability affects all tenants in the system.	10.0	More Details
CVE-2025-10878	A SQL injection vulnerability exists in the login functionality of Fikir Odalari AdminPando 1.0.1 before 2026-01-26. The username and password parameters are vulnerable to SQL injection, allowing unauthenticated attackers to bypass authentication completely. Successful exploitation grants full administrative access to the application, including the ability to manipulate the public-facing website content (HTML/DOM manipulation).	10.0	More Details
CVE-2026-24897	Erugo is a self-hosted file-sharing platform. In versions up to and including 0.2.14, an authenticated low-privileged user can upload arbitrary files to any specified location due to insufficient validation of user-supplied paths when creating shares. By specifying a writable path within the public web root, an attacker can upload and execute arbitrary code on the server, resulting in remote code execution (RCE). This vulnerability allows a low-privileged user to fully compromise the affected Erugo instance. Version 0.2.15 fixes the issue.	10.0	More Details
CVE-2026-24841	Dokploy is a free, self-hostable Platform as a Service (PaaS). In versions prior to 0.26.6, a critical command injection vulnerability exists in Dokploy's WebSocket endpoint `/docker-container-terminal`. The `containerId` and `activeWay` parameters are directly interpolated into shell commands without sanitization, allowing authenticated attackers to execute arbitrary commands on the host server. Version 0.26.6 fixes the issue.	9.9	More Details
CVE-2026-0963	An input neutralization vulnerability in the File Operations API Endpoint component of Crafty Controller allows a remote, authenticated attacker to perform file tampering and remote code execution via path traversal.	9.9	More Details
CVE-2025-57795	Explorance Blue versions prior to 8.14.13 contain an authenticated remote file download vulnerability in a web service component. In default configurations, this flaw can be leveraged to achieve remote code execution.	9.9	More Details
CVE-2026-23515	Signal K Server is a server application that runs on a central hub in a boat. Prior to 1.5.0, a command injection vulnerability allows authenticated users with write permissions to execute arbitrary shell commands on the Signal K server when the set-system-time plugin is enabled. Unauthenticated users can also exploit this vulnerability if security is disabled on the Signal K server. This occurs due to unsafe construction of shell commands when processing navigation.datetime values received via WebSocket delta messages. This vulnerability is fixed in 1.5.0.	9.9	More Details
CVE-2026-	CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to version 0.28.5.0, an authenticated user with file editor permissions can achieve Remote Code Execution	9.9	More

25510	(RCE) by leveraging the file creation and save endpoints, an attacker can upload and execute arbitrary PHP code on the server. This issue has been patched in version 0.28.5.0.		Details
CVE-2020-37080	webTareas 2.0.p8 contains a file deletion vulnerability in the print_layout.php administration component that allows authenticated attackers to delete arbitrary files. Attackers can exploit the vulnerability by manipulating the 'atttmp1' parameter to specify and delete files on the server through an unauthenticated file deletion mechanism.	9.8	More Details
CVE-2025-5319	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Emit Information and Communication Technologies Industry and Trade Ltd. Co. Efficiency Management System allows SQL Injection.This issue affects Efficiency Management System: through 03022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2026-25200	A vulnerability in MagicInfo9 Server allows authorized users to upload HTML files without authentication, leading to Stored XSS, which can result in account takeover This issue affects MagicINFO 9 Server: less than 21.1090.1.	9.8	More Details
CVE-2026-25202	The database account and password are hardcoded, allowing login with the account to manipulate the database in MagicInfo9 Server.This issue affects MagicINFO 9 Server: less than 21.1090.1.	9.8	More Details
CVE-2025-15030	The User Profile Builder WordPress plugin before 3.15.2 does not have a proper password reset process, allowing a few unauthenticated requests to reset the password of any user by knowing their username, such as administrator ones, and therefore gain access to their account	9.8	More Details
CVE-2026-20418	In Thread, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00465153; Issue ID: MSV-4927.	9.8	More Details
CVE-2022-50981	An unauthenticated remote attacker can gain full access on the affected devices as they are shipped without a password by default and setting one is not enforced.	9.8	More Details
CVE-2025-66480	Wildfire IM is an instant messaging and real-time audio/video solution. Prior to 1.4.3, a critical vulnerability exists in the im-server component related to the file upload functionality found in com.xiaoleilu.loServer.action.UploadFileAction. The application exposes an endpoint (/fs) that handles multipart file uploads but fails to properly sanitize the filename provided by the user. Specifically, the writeFileUploadData method directly concatenates the configured storage directory with the filename extracted from the upload request without stripping directory traversal sequences (e.g., ../../). This vulnerability allows an attacker to write arbitrary files to any location on the server's filesystem where the application process has write permissions. By uploading malicious files (such as scripts, executables, or overwriting configuration files like authorized_keys or cron jobs), an attacker can achieve Remote Code Execution (RCE) and completely compromise the server. This vulnerability is fixed in 1.4.3.	9.8	More Details
CVE-2026-22778	vLLM is an inference and serving engine for large language models (LLMs). From 0.8.3 to before 0.14.1, when an invalid image is sent to vLLM's multimodal endpoint, PIL throws an error. vLLM returns this error to the client, leaking a heap address. With this leak, we reduce ASLR from 4 billion guesses to ~8 guesses. This vulnerability can be chained a heap overflow with JPEG2000 decoder in OpenCV/FFmpeg to achieve remote code execution. This vulnerability is fixed in 0.14.1.	9.8	More Details
CVE-2020-37094	EspoCRM 5.8.5 contains an authentication vulnerability that allows attackers to access other user accounts by manipulating authorization headers. Attackers can decode and modify Basic Authorization and Espo-Authorization tokens to gain unauthorized access to administrative user information and privileges.	9.8	More Details

CVE-2020-37075	LanSend 3.2 contains a buffer overflow vulnerability in the Add Computers Wizard file import functionality that allows remote attackers to execute arbitrary code. Attackers can craft a malicious payload file to trigger a structured exception handler (SEH) overwrite and execute shellcode when importing computers from a file.	9.8	More Details
CVE-2020-37090	School ERP Pro 1.0 contains a file upload vulnerability that allows students to upload arbitrary PHP files to the messaging system. Attackers can upload malicious PHP scripts through the message attachment feature, enabling remote code execution on the server.	9.8	More Details
CVE-2020-37065	StreamRipper32 version 2.6 contains a buffer overflow vulnerability in the Station/Song Section that allows attackers to overwrite memory by manipulating the SongPattern input. Attackers can craft a malicious payload exceeding 256 bytes to potentially execute arbitrary code and compromise the application.	9.8	More Details
CVE-2020-37066	GoldWave 5.70 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by crafting malicious input in the File Open URL dialog. Attackers can generate a specially crafted text file with Unicode-encoded shellcode to trigger a stack-based overflow and execute commands when the file is opened.	9.8	More Details
CVE-2020-37052	AirControl 1.4.2 contains a pre-authentication remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary system commands through malicious Java expression injection. Attackers can exploit the /.seam endpoint by crafting a specially constructed URL with embedded Java expressions to run commands with the application's system privileges.	9.8	More Details
CVE-2020-37067	Filetto 1.0 FTP server contains a denial of service vulnerability in the FEAT command processing that allows attackers to crash the service. Attackers can send an oversized FEAT command with 11,008 bytes of repeated characters to trigger a buffer overflow and terminate the FTP service.	9.8	More Details
CVE-2020-37068	Konica Minolta FTP Utility 1.0 contains a buffer overflow vulnerability in the LIST command that allows attackers to overwrite system registers. Attackers can send an oversized buffer of 1500 'A' characters to crash the FTP server and potentially execute unauthorized code.	9.8	More Details
CVE-2020-37082	webERP 4.15.1 contains an unauthenticated file access vulnerability that allows remote attackers to download database backup files without authentication. Attackers can directly access generated backup files in the companies/weberp/ directory by requesting the Backup_[timestamp].sql.gz file.	9.8	More Details
CVE-2020-37069	Konica Minolta FTP Utility 1.0 contains a buffer overflow vulnerability in the NLST command that allows attackers to overwrite system registers. Attackers can send an oversized buffer of 1500 'A' characters to crash the FTP server and potentially execute unauthorized code.	9.8	More Details
CVE-2020-37070	CloudMe 1.11.2 contains a buffer overflow vulnerability that allows remote attackers to execute arbitrary code through crafted network packets. Attackers can exploit the vulnerability by sending a specially crafted payload to the CloudMe service running on port 8888, enabling remote code execution.	9.8	More Details
CVE-2020-37071	CraftCMS 3 vCard Plugin 1.0.0 contains a deserialization vulnerability that allows unauthenticated attackers to execute arbitrary PHP code through a crafted payload. Attackers can generate a malicious serialized payload that triggers remote code execution by exploiting the plugin's vCard download functionality with a specially crafted request.	9.8	More Details
CVE-2020-37074	Remote Desktop Audit 2.3.0.157 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code during the Add Computers Wizard file import process. Attackers can craft a malicious payload file to trigger a structured exception handler (SEH) bypass and execute shellcode when importing computer lists.	9.8	More Details

CVE-2020-37056	Crystal Shard http-protection 0.2.0 contains an IP spoofing vulnerability that allows attackers to bypass protection middleware by manipulating request headers. Attackers can hardcode consistent IP values across X-Forwarded-For, X-Client-IP, and X-Real-IP headers to circumvent security checks and gain unauthorized access.	9.8	More Details
CVE-2020-37043	10-Strike Bandwidth Monitor 3.9 contains a buffer overflow vulnerability that allows attackers to bypass SafeSEH, ASLR, and DEP protections through carefully crafted input. Attackers can exploit the vulnerability by sending a malicious payload to the application's registration key input, enabling remote code execution and launching arbitrary system commands.	9.8	More Details
CVE-2020-37050	Quick Player 1.3 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by crafting a malicious .m3l file with carefully constructed payload. Attackers can trigger the vulnerability by loading a specially crafted file through the application's file loading mechanism, potentially enabling remote code execution.	9.8	More Details
CVE-2020-37010	BearShare Lite 5.2.5 contains a buffer overflow vulnerability in the Advanced Search keywords input that allows attackers to execute arbitrary code. Attackers can craft a specially designed payload to overwrite the EIP register and execute shellcode by pasting malicious content into the search keywords field.	9.8	More Details
CVE-2025-40551	SolarWinds Web Help Desk was found to be susceptible to an untrusted data deserialization vulnerability that could lead to remote code execution, which would allow an attacker to run commands on the host machine. This could be exploited without authentication.	9.8	More Details
CVE-2025-40552	SolarWinds Web Help Desk was found to be susceptible to an authentication bypass vulnerability that if exploited, would allow a malicious actor to execute actions and methods that should be protected by authentication.	9.8	More Details
CVE-2025-40553	SolarWinds Web Help Desk was found to be susceptible to an untrusted data deserialization vulnerability that could lead to remote code execution, which would allow an attacker to run commands on the host machine. This could be exploited without authentication.	9.8	More Details
CVE-2025-40554	SolarWinds Web Help Desk was found to be susceptible to an authentication bypass vulnerability that, if exploited, could allow an attacker to invoke specific actions within Web Help Desk.	9.8	More Details
CVE-2026-1056	The Snow Monkey Forms plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'generate_user_dirpath' function in all versions up to, and including, 12.0.3. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	9.8	More Details
CVE-2025-61140	The value function in jsonpath 1.1.1 lib/index.js is vulnerable to Prototype Pollution.	9.8	More Details
CVE-2020-36961	10-Strike Network Inventory Explorer 8.65 contains a buffer overflow vulnerability in exception handling that allows remote attackers to execute arbitrary code. Attackers can craft a malicious file with 209 bytes of padding and a specially constructed Structured Exception Handler to trigger code execution.	9.8	More Details
CVE-2020-36962	Tendenci 12.3.1 contains a CSV formula injection vulnerability in the contact form message field that allows attackers to inject malicious formulas during export. Attackers can submit crafted payloads like '=10+20+cmd|' /C calc'!A0' in the message field to trigger arbitrary command execution when the CSV is opened in spreadsheet applications.	9.8	More Details
CVE-	YATinyWinFTP contains a denial of service vulnerability that allows attackers to crash		

2020-36964	the FTP service by sending a 272-byte buffer with a trailing space. Attackers can exploit the service by connecting and sending a malformed command that triggers a buffer overflow and service crash.	9.8	More Details
CVE-2020-36967	Zortam Mp3 Media Studio 27.60 contains a buffer overflow vulnerability in the library creation file selection process that allows remote code execution. Attackers can craft a malicious text file with shellcode to trigger a structured exception handler (SEH) overwrite and execute arbitrary commands on the target system.	9.8	More Details
CVE-2020-36997	BacklinkSpeed 2.4 contains a buffer overflow vulnerability that allows attackers to corrupt the Structured Exception Handler (SEH) chain through malicious file import. Attackers can craft a specially designed payload file to overwrite SEH addresses, potentially executing arbitrary code and gaining control of the application.	9.8	More Details
CVE-2020-37000	Free MP3 CD Ripper 2.8 contains a stack buffer overflow vulnerability that allows remote attackers to execute arbitrary code by crafting a malicious WAV file with oversized payload. Attackers can leverage a specially crafted exploit file with shellcode, SEH bypass, and egghunter technique to achieve remote code execution on vulnerable Windows systems.	9.8	More Details
CVE-2020-37002	Ajenti 2.1.36 contains an authentication bypass vulnerability that allows remote attackers to execute arbitrary commands after successful login. Attackers can leverage the /api/terminal/create endpoint to send a netcat reverse shell payload targeting a specified IP and port.	9.8	More Details
CVE-2026-1281	A code injection in Ivanti Endpoint Manager Mobile allowing attackers to achieve unauthenticated remote code execution.	9.8	More Details
CVE-2026-1340	A code injection in Ivanti Endpoint Manager Mobile allowing attackers to achieve unauthenticated remote code execution.	9.8	More Details
CVE-2020-37012	Tea LaTex 1.0 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary shell commands through the /api.php endpoint. Attackers can craft a malicious LaTeX payload with shell commands that are executed when processed by the application's tex2png API action.	9.8	More Details
CVE-2026-1453	A missing authentication for critical function vulnerability in KiloView Encoder Series could allow an unauthenticated attacker to create or delete administrator accounts. This vulnerability can grant the attacker full administrative control over the product.	9.8	More Details
CVE-2020-37027	Sickbeard alpha contains a remote command injection vulnerability that allows unauthenticated attackers to execute arbitrary commands through the extra scripts configuration. Attackers can set malicious commands in the extra scripts field and trigger processing to execute remote code on the vulnerable Sickbeard installation.	9.8	More Details
CVE-2019-25232	NetPCLinker 1.0.0.0 contains a buffer overflow vulnerability in the Clients Control Panel DNS/IP field that allows attackers to execute arbitrary shellcode. Attackers can craft a malicious payload in the DNS/IP input to overwrite SEH handlers and execute shellcode when adding a new client.	9.8	More Details
CVE-2025-69929	An issue in N3uron Web User Interface v.1.21.7-240207.1047 allows a remote attacker to escalate privileges via the password hashing on the client side using the MD5 algorithm over a predictable string format	9.8	More Details
CVE-2025-51958	aelsantex runcommand 2014-04-01, a plugin for DokuWiki, allows unauthenticated attackers to execute arbitrary system commands via lib/plugins/runcommand/postaction.php.	9.8	More Details
	Cybersecurity AI (CAI) is a framework for AI Security. In versions up to and including 0.5.10, the CAI (Cybersecurity AI) framework contains multiple argument injection		

CVE-2026-25130	vulnerabilities in its function tools. User-controlled input is passed directly to shell commands via `subprocess.Popen()` with `shell=True`, allowing attackers to execute arbitrary commands on the host system. The `find_file()` tool executes without requiring user approval because find is considered a "safe" pre-approved command. This means an attacker can achieve Remote Code Execution (RCE) by injecting malicious arguments (like -exec) into the args parameter, completely bypassing any human-in-the-loop safety mechanisms. Commit e22a1220f764e2d7cf9da6d6144926f53ca01cde contains a fix.	9.6	More Details
CVE-2026-1568	Rapid7 InsightVM versions before 8.34.0 contain a signature verification issue on the Assertion Consumer Service (ACS) cloud endpoint that could allow an attacker to gain unauthorized access to InsightVM accounts setup via "Security Console" installations, resulting in full account takeover. The issue occurs due to the application processing these unsigned assertions and issuing session cookies that granted access to the targeted user accounts. This has been fixed in version 8.34.0 of InsightVM.	9.6	More Details
CVE-2026-20407	In wlan STA driver, there is a possible escalation of privilege due to a missing bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00464377; Issue ID: MSV-4905.	9.3	More Details
CVE-2026-25150	Qwik is a performance focused javascript framework. Prior to version 1.19.0, a prototype pollution vulnerability exists in the formToObj() function within @builder.io/qwik-city middleware. The function processes form field names with dot notation (e.g., user.name) to create nested objects, but fails to sanitize dangerous property names like __proto__, constructor, and prototype. This allows unauthenticated attackers to pollute Object.prototype by sending crafted HTTP POST requests, potentially leading to privilege escalation, authentication bypass, or denial of service. This issue has been patched in version 1.19.0.	9.3	More Details
CVE-2026-24838	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to versions 9.13.10 and 10.2.0, module title supports richtext which could include scripts that would execute in certain scenarios. Versions 9.13.10 and 10.2.0 contain a fix for the issue.	9.1	More Details
CVE-2026-22806	vCluster Platform provides a Kubernetes platform for managing virtual clusters, multi-tenancy, and cluster sharing. Prior to versions 4.6.0, 4.5.4, 4.4.2, and 4.3.10, when an access key is created with a limited scope, the scope can be bypassed to access resources outside of it. However, the user still cannot access resources beyond what is accessible to the owner of the access key. Versions 4.6.0, 4.5.4, 4.4.2, and 4.3.10 fix the vulnerability. Some other mitigations are available. Users can limit exposure by reviewing access keys which are scoped and ensuring any users with access to them have appropriate permissions set. Creating automation users with very limited permissions and using access keys for these automation users can be used as a temporary workaround where upgrading is not immediately possible but scoped access keys are needed.	9.1	More Details
CVE-2026-25137	The NixOs Odoo package is an open source ERP and CRM system. From 21.11 to before 25.11 and 26.05, every NixOS based Odoo setup publicly exposes the database manager without any authentication. This allows unauthorized actors to delete and download the entire database, including Odoos file store. Unauthorized access is evident from http requests. If kept, searching access logs and/or Odoos log for requests to /web/database can give indicators, if this has been actively exploited. The database manager is a featured intended for development and not meant to be publicly reachable. On other setups, a master password acts as 2nd line of defence. However, due to the nature of NixOS, Odoo is not able to modify its own configuration file and thus unable to persist the auto-generated password. This also applies when manually setting a master password in the web-UI. This means, the password is lost when restarting Odoo. When no password is set, the user is prompted to set one directly via the database manager. This requires no authentication or action by any authorized user or the system administrator. Thus, the database is effectively world readable by anyone able to reach Odoo. This vulnerability is fixed in 25.11 and 26.05.	9.1	More Details

CVE-2025-57794	Explorance Blue versions prior to 8.14.9 contain an authenticated unrestricted file upload vulnerability in the administrative interface. The application does not adequately restrict uploaded file types, allowing malicious files to be uploaded and executed by the server. This condition enables remote code execution under default configurations.	9.1	More Details
CVE-2025-69602	A session fixation vulnerability exists in 66biolinks v62.0.0 by AltumCode, where the application does not regenerate the session identifier after successful authentication. As a result, the same session cookie value is reused for users logging in from the same browser, allowing an attacker who can set or predict a session ID to potentially hijack an authenticated session.	9.1	More Details
CVE-2026-1632	MOMA Seismic Station Version v2.4.2520 and prior exposes its web management interface without requiring authentication, which could allow an unauthenticated attacker to modify configuration settings, acquire device data or remotely reset the device.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-24772	OpenProject is an open-source, web-based project management software. To enable the real time collaboration on documents, OpenProject 17.0 introduced a synchronization server. The OpenPrioject backend generates an authentication token that is currently valid for 24 hours, encrypts it with a shared secret only known to the synchronization server. The frontend hands this encrypted token and the backend URL over to the synchronization server to check user's ability to work on the document and perform intermittent saves while editing. The synchronization server does not properly validate the backend URL and sends a request with the decrypted authentication token to the endpoint that was given to the server. An attacker could use this vulnerability to decrypt a token that he intercepted by other means to gain an access token to interact with OpenProject on the victim's behalf. This vulnerability was introduced with OpenProject 17.0.0 and was fixed in 17.0.2. As a workaround, disable the collaboration feature via Settings -> Documents -> Real time collaboration -> Disable. Additionally the `hocuspocus` container should also be disabled.	8.9	More Details
CVE-2026-25059	OpenList Frontend is a UI component for OpenList. Prior to 4.1.10, the application contains path traversal vulnerability in multiple file operation handlers in server/handles/fsmanage.go. Filename components in req.Names are directly concatenated with validated directories using stdpath.Join. This allows ".." sequences to bypass path restrictions, enabling users to access other users' files within the same storage mount and perform unauthorized actions such as deletion, renaming, or copying of files. An authenticated attacker can bypass directory-level authorisation by injecting traversal sequences into filename components, enabling unauthorised file removal and copying across user boundaries within the same storage mount. This vulnerability is fixed in 4.1.10.	8.8	More Details
CVE-2025-69516	A Server-Side Template Injection (SSTI) vulnerability in the /reporting/templates/preview/ endpoint of Amidaware Tactical RMM, affecting versions equal to or earlier than v1.3.1, allows low-privileged users with Report Viewer or Report Manager permissions to achieve remote command execution on the server. This occurs due to improper sanitization of the template_md parameter, enabling direct injection of Jinja2 templates. This occurs due to misuse of the generate_html() function, the user-controlled value is inserted into `env.from_string`, a function that processes Jinja2 templates arbitrarily, making an SSTI possible.	8.8	More Details
CVE-	OpenClaw (formerly Clawdbot) is a personal AI assistant you run on your own devices. Prior to 2026.1.29, a command injection vulnerability existed in OpenClaw’s Docker		

2026-24763	sandbox execution mechanism due to unsafe handling of the PATH environment variable when constructing shell commands. An authenticated user able to control environment variables could influence command execution within the container context. This vulnerability is fixed in 2026.1.29.	8.8	More Details
CVE-2020-37023	Koken CMS 0.22.24 contains a file upload vulnerability that allows authenticated attackers to bypass file extension restrictions by renaming malicious PHP files. Attackers can upload PHP files with system command execution capabilities by manipulating the file upload request through a web proxy and changing the file extension.	8.8	More Details
CVE-2026-1861	Heap buffer overflow in libvpx in Google Chrome prior to 144.0.7559.132 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2020-37113	GUnet OpenEclass 1.7.3 allows authenticated users to bypass file extension restrictions when uploading files. By renaming a PHP file to .php3 or .PhP, an attacker can upload a web shell and execute arbitrary code on the server. This vulnerability enables remote code execution by bypassing the intended file type checks in the exercise submission feature.	8.8	More Details
CVE-2020-37116	GUnet OpenEclass 1.7.3 includes phpMyAdmin 2.10.0.2 by default, which allows remote logins. Attackers with access to the platform can remotely access phpMyAdmin and, after uploading a shell, view the config.php file to obtain the MySQL password, leading to full database compromise.	8.8	More Details
CVE-2025-14386	The Search Atlas SEO – Premier SEO Plugin for One-Click WP Publishing & Integrated AI Optimization plugin for WordPress is vulnerable to authentication bypass due to a missing capability check on the 'generate_sso_url' and 'validate_sso_token' functions in versions 2.4.4 to 2.5.12. This makes it possible for authenticated attackers, with Subscriber-level access and above, to extract the 'nonce_token' authentication value to log in to the first Administrator's account.	8.8	More Details
CVE-2020-37078	i-doit Open Source CMDB 1.14.1 contains a file deletion vulnerability in the import module that allows authenticated attackers to delete arbitrary files by manipulating the delete_import parameter. Attackers can send a POST request to the import module with a crafted filename to remove files from the server's filesystem.	8.8	More Details
CVE-2026-1862	Type Confusion in V8 in Google Chrome prior to 144.0.7559.132 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2020-37009	MedDream PACS Server 6.8.3.751 contains an authenticated remote code execution vulnerability that allows authorized users to upload malicious PHP files. Attackers can exploit the uploadImage.php endpoint by authenticating and uploading a PHP shell to execute arbitrary system commands with elevated privileges.	8.8	More Details
CVE-2026-25253	OpenClaw (aka clawdbot or Moltbot) before 2026.1.29 obtains a gatewayUrl value from a query string and automatically makes a WebSocket connection without prompting, sending a token value.	8.8	More Details
CVE-2022-50975	An unauthenticated remote attacker is able to use an existing session id of a logged in user and gain full access to the device if configuration via ethernet is enabled.	8.8	More Details
CVE-2026-25201	An unauthenticated user can upload arbitrary files to execute remote code, leading to privilege escalation in MagicInfo9 Server. This issue affects MagicINFO 9 Server: less than 21.1090.1.	8.8	More Details
	During the installation of the Native Access application, a privileged helper `com.native-instruments.NativeAccess.Helper2`, which is used by Native Access to trigger functions via XPC communication like copy-file, remove or set-permissions, is deployed as well. The communication with the XPC service of the privileged helper is only allowed if the client process is signed with the corresponding certificate and fulfills the following code signing		

CVE-2026-24070	requirement: "anchor trusted and certificate leaf[subject.CN] = \"Developer ID Application: Native Instruments GmbH (83K5EG6Z9V)\"" The Native Access application was found to be signed with the `com.apple.security.cs.allow-dyld-environment-variables` and `com.apple.security.cs.disable-library-validation` entitlements leading to DYLIB injection and therefore command execution in the context of this application. A low privileged user can exploit the DYLIB injection to trigger functions of the privileged helper XPC service resulting in privilege escalation by first deleting the /etc/sudoers file and then copying a malicious version of that file to /etc/sudoers.	8.8	More Details
CVE-2025-65875	An arbitrary file upload vulnerability in the AddFont() function of FPDF v1.86 and earlier allows attackers to execute arbitrary code via uploading a crafted PHP file.	8.8	More Details
CVE-2020-36969	M/Monit 3.7.4 contains a privilege escalation vulnerability that allows authenticated users to modify user permissions by manipulating the admin parameter. Attackers can send a POST request to the /api/1/admin/users/update endpoint with a crafted payload to grant administrative access to a standard user account.	8.8	More Details
CVE-2026-20408	In wlan, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00461651; Issue ID: MSV-4758.	8.8	More Details
CVE-2026-1580	A security issue was discovered in ingress-nginx where the `nginx.ingress.kubernetes.io/auth-method` Ingress annotation can be used to inject configuration into nginx. This can lead to arbitrary code execution in the context of the ingress-nginx controller, and disclosure of Secrets accessible to the controller. (Note that in the default installation, the controller can access all Secrets cluster-wide.)	8.8	More Details
CVE-2026-37032	Wing FTP Server 6.3.8 contains a remote code execution vulnerability in its Lua-based web console that allows authenticated users to execute system commands. Attackers can leverage the console to send POST requests with malicious commands that trigger operating system execution through the os.execute() function.	8.8	More Details
CVE-2026-1730	The OS DataHub Maps plugin for WordPress is vulnerable to arbitrary file uploads due to incorrect file type validation in the 'OS_DataHub_Maps_Admin::add_file_and_ext' function in all versions up to, and including, 1.8.3. This makes it possible for authenticated attackers, with Author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2020-37073	Victor CMS 1.0 contains an authenticated file upload vulnerability that allows administrators to upload PHP files with arbitrary content through the user_image parameter. Attackers can upload a malicious PHP shell to the /img/ directory and execute system commands by accessing the uploaded file with a 'cmd' parameter.	8.8	More Details
CVE-2026-24954	Deserialization of Untrusted Data vulnerability in magepeopleteam WpEvently mage-eventpress allows Object Injection.This issue affects WpEvently: from n/a through <= 5.0.8.	8.8	More Details
CVE-2025-67645	OpenEMR is a free and open source electronic health records and medical practice management application. Versions prior to 7.0.4 have a broken access control in the Profile Edit endpoint. An authenticated normal user can modify the request parameters (pubpid / pid) to reference another user’s record; the server accepts the modified IDs and applies the changes to that other user’s profile. This allows one user to alter another user’s profile data (name, contact info, etc.), and could enable account takeover. Version 7.0.4 fixes the issue.	8.8	More Details
CVE-2025-58150	Shadow mode tracing code uses a set of per-CPU variables to avoid cumbersome parameter passing. Some of these variables are written to with guest controlled data, of guest controllable size. That size can be larger than the variable, and bounding of the writes was missing.	8.8	More Details
	An HTML injection vulnerability in Amidaware Inc Tactical RMM v1.3.1 and earlier allows		

CVE-2025-69517	authenticated users to inject arbitrary HTML content during the creation of a new agent via the POST /api/v3/newagent/ endpoint. The agent_id parameter accepts up to 255 characters and is improperly sanitized using DOMPurify.sanitize() with the html: true option enabled, which fails to adequately filter HTML input. The injected HTML is rendered in the Tactical RMM management panel when an administrator attempts to remove or shut down the affected agent, potentially leading to client-side attacks such as UI manipulation or phishing. NOTE: the Supplier's position is that this has incorrect information.	8.8	More Details
CVE-2026-1686	A security flaw has been discovered in Totolink A3600R 5.9c.4959. This issue affects the function setAppEasyWizardConfig in the library /lib/cste_modules/app.so. Performing a manipulation of the argument apcliSsid results in buffer overflow. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-1637	A vulnerability was identified in Tenda AC21 16.03.08.16. The affected element is the function fromAdvSetMacMtuWan of the file /goform/AdvSetMacMtuWan. The manipulation leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-24854	ChurchCRM is an open-source church management system. A SQL Injection vulnerability exists in endpoint `/PaddleNumEditor.php` in ChurchCRM prior to version 6.7.2. Any authenticated user, including one with zero assigned permissions, can exploit SQL injection through the `PerID` parameter. Version 6.7.2 contains a patch for the issue.	8.8	More Details
CVE-2026-24512	A security issue was discovered in ingress-nginx cthe `rules.http.paths.path` Ingress field can be used to inject configuration into nginx. This can lead to arbitrary code execution in the context of the ingress-nginx controller, and disclosure of Secrets accessible to the controller. (Note that in the default installation, the controller can access all Secrets cluster-wide.)	8.8	More Details
CVE-2026-0844	The Simple User Registration plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 6.7 due to insufficient restriction on the 'profile_save_field' function. This makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to modify their user role by supplying the 'wp_capabilities' parameter during a profile update.	8.8	More Details
CVE-2026-24665	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, a stored Cross-Site Scripting (XSS) vulnerability allows authenticated students to inject malicious JavaScript into uploaded assignment files, which is executed when instructors view the submission. This issue has been patched in version 4.2.	8.7	More Details
CVE-2025-4686	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Kodmatic Computer Software Tourism Construction Industry and Trade Ltd. Co. Online Exam and Assessment allows SQL Injection.This issue affects Online Exam and Assessment: through 30012026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.6	More Details
CVE-2025-8587	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AKCE Software Technology R&D Industry and Trade Inc. SKSPro allows SQL Injection.This issue affects SKSPro: through 07012026.	8.6	More Details
CVE-2026-1761	A flaw was found in libsoup. This stack-based buffer overflow vulnerability occurs during the parsing of multipart HTTP responses due to an incorrect length calculation. A remote attacker can exploit this by sending a specially crafted multipart HTTP response, which can lead to memory corruption. This issue may result in application crashes or arbitrary code execution in applications that process untrusted server responses, and it does not require authentication or user interaction.	8.6	More Details
CVE-	Explorance Blue versions prior to 8.14.9 contain a SQL injection vulnerability caused by insufficient validation of user-supplied input in a web application component. Crafted		More

2025-57793	input can be executed as part of backend database queries. The issue is exploitable without authentication, significantly elevating the risk.	8.6	Details
CVE-2025-6397	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ankara Hosting Website Design Website Software allows Reflected XSS.This issue affects Website Software: through 03022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.6	More Details
CVE-2025-69662	SQL injection vulnerability in geopandas before v.1.1.2 allows an attacker to obtain sensitive information via the to_postgis()` function being used to write GeoDataFrames to a PostgreSQL database.	8.6	More Details
CVE-2026-25022	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Iqonic Design KiviCare kivicare-clinic-management-system allows Blind SQL Injection.This issue affects KiviCare: from n/a through <= 3.6.16.	8.5	More Details
CVE-2020-37049	Frigate 3.36.0.9 contains a local buffer overflow vulnerability in the Command Line input field that allows attackers to execute arbitrary code. Attackers can craft a malicious payload to overflow the buffer, bypass DEP, and execute commands like launching calc.exe through a specially crafted input sequence.	8.4	More Details
CVE-2020-36971	Nidesoft 3GP Video Converter 2.6.18 contains a local stack buffer overflow vulnerability in the license registration parameter. Attackers can craft a malicious payload and paste it into the 'License Code' field to execute arbitrary code on the system.	8.4	More Details
CVE-2020-37036	RM Downloader 2.50.60 contains a local buffer overflow vulnerability in the 'Load' parameter that allows attackers to execute arbitrary code by overwriting memory. Attackers can craft a malicious payload with an egg hunter technique to bypass memory protections and execute commands like launching calc.exe.	8.4	More Details
CVE-2020-37040	Code Blocks 17.12 contains a local buffer overflow vulnerability that allows attackers to execute arbitrary code by crafting a malicious file name with Unicode characters. Attackers can trigger the vulnerability by pasting a specially crafted payload into the file name field during project creation, potentially executing system commands like calc.exe.	8.4	More Details
CVE-2020-37042	Frigate Professional 3.36.0.9 contains a local buffer overflow vulnerability in the 'Find Computer' feature that allows attackers to execute arbitrary code by overflowing the computer name input field. Attackers can craft a malicious payload that triggers a buffer overflow, enabling code execution and launching calculator as a proof of concept.	8.4	More Details
CVE-2020-37029	FTPDummy 4.80 contains a local buffer overflow vulnerability in its preference file handling that allows attackers to execute arbitrary code. Attackers can craft a malicious preference file with carefully constructed shellcode to trigger a structured exception handler overwrite and execute system commands.	8.4	More Details
CVE-2020-36970	PMB 5.6 contains a local file disclosure vulnerability in getgif.php that allows attackers to read arbitrary system files by manipulating the 'chemin' parameter. Attackers can exploit the unsanitized file path input to access sensitive files like /etc/passwd by sending crafted requests to the getgif.php endpoint.	8.4	More Details
CVE-2020-37031	Simple Startup Manager 1.17 contains a local buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting memory through the 'File' input parameter. Attackers can craft a malicious payload with 268 bytes to trigger code execution, bypassing DEP and overwriting memory addresses to launch calc.exe.	8.4	More Details
CVE-2025-36384	IBM Db2 for Windows 12.1.0 - 12.1.3 could allow a local user with filesystem access to escalate their privileges due to the use of an unquoted search path element.	8.4	More Details
CVE-2020-37024	Nidesoft DVD Ripper 5.2.18 contains a local buffer overflow vulnerability in the License Code registration parameter that allows attackers to execute arbitrary code. Attackers can craft a malicious payload and paste it into the License Code field to trigger a stack-based buffer overflow and execute shellcode.	8.4	More Details

CVE-2020-37025	Port Forwarding Wizard 4.8.0 contains a buffer overflow vulnerability that allows local attackers to execute arbitrary code through a long request in the Register feature. Attackers can craft a malicious payload with an egg tag and overwrite SEH handlers to potentially execute shellcode on vulnerable Windows systems.	8.4	More Details
CVE-2020-37001	Frigate Professional 3.36.0.9 contains a local buffer overflow vulnerability in the Pack File feature that allows attackers to execute arbitrary code by overflowing the 'Archive To' input field. Attackers can craft a malicious payload that overwrites the Structured Exception Handler (SEH) and uses an egghunter technique to execute a reverse shell payload.	8.4	More Details
CVE-2020-37028	Socusoft Photo to Video Converter Professional 8.07 contains a local buffer overflow vulnerability in the 'Output Folder' input field that allows attackers to execute arbitrary code. Attackers can craft a malicious payload and paste it into the output folder field to trigger a stack-based buffer overflow and potentially execute shellcode.	8.4	More Details
CVE-2020-37013	Audio Playback Recorder 3.2.2 contains a local buffer overflow vulnerability in the eject and registration parameters that allows attackers to execute arbitrary code. Attackers can craft malicious payloads and overwrite Structured Exception Handler (SEH) to execute shellcode when pasting specially crafted input into the application's input fields.	8.4	More Details
CVE-2020-36965	docPrint Pro 8.0 contains a local buffer overflow vulnerability in the 'Add URL' input field that allows attackers to execute arbitrary code by overwriting memory. Attackers can craft a malicious payload that triggers a structured exception handler (SEH) overwrite to execute shellcode and gain remote system access.	8.4	More Details
CVE-2025-62514	Parsec is a cloud-based application for cryptographically secure file sharing. In versions on the 3.x branch prior to 3.6.0, `libparsec_crypto`, a component of the Parsec application, does not check for weak order point of Curve25519 when compiled with its RustCrypto backend. In practice this means an attacker in a man-in-the-middle position would be able to provide weak order points to both parties in the Diffie-Hellman exchange, resulting in a high probability to for both parties to obtain the same shared key (hence leading to a successful SAS code exchange, misleading both parties into thinking no MITM has occurred) which is also known by the attacker. Note only Parsec web is impacted (as Parsec desktop uses `libparsec_crypto` with the libsodium backend). Version 3.6.0 of Parsec patches the issue.	8.3	More Details
CVE-2020-36972	SmartBlog 2.0.1 contains a blind SQL injection vulnerability in the 'id_post' parameter of the details controller that allows attackers to extract database information. Attackers can systematically test and retrieve database contents by injecting crafted SQL queries that compare character-by-character of database information.	8.2	More Details
CVE-2020-37035	e-Learning PHP Script 0.1.0 contains a SQL injection vulnerability in the search functionality that allows attackers to manipulate database queries through unvalidated user input. Attackers can inject malicious SQL code in the 'search' parameter to potentially extract, modify, or access sensitive database information.	8.2	More Details
CVE-2020-37033	Infor Storefront B2B 1.0 contains a SQL injection vulnerability that allows attackers to manipulate database queries through the 'usr_name' parameter in login requests. Attackers can exploit the vulnerability by injecting malicious SQL code into the 'usr_name' parameter to potentially extract or modify database information.	8.2	More Details
CVE-2020-36945	WebDamn User Registration Login System contains a SQL injection vulnerability that allows unauthenticated attackers to bypass login authentication by manipulating email credentials. Attackers can inject the payload '<email>' OR '1'='1' in both username and password fields to gain unauthorized access to the user panel.	8.2	More Details
CVE-2020-37083	PHP AddressBook 9.0.0.1 contains a time-based blind SQL injection vulnerability that allows remote attackers to manipulate database queries through the 'id' parameter. Attackers can inject crafted SQL statements with time delays to extract information by observing response times in the photo.php endpoint.	8.2	More Details

CVE-2026-0805	An input neutralization vulnerability in the Backup Configuration component of Crafty Controller allows a remote, authenticated attacker to perform file tampering and remote code execution via path traversal.	8.2	More Details
CVE-2020-37051	Online-Exam-System 2015 contains a time-based blind SQL injection vulnerability in the feedback form that allows attackers to extract database password hashes. Attackers can exploit the 'feed.php' endpoint by crafting malicious payload requests that use time delays to systematically enumerate user password characters.	8.2	More Details
CVE-2020-37089	School ERP Pro 1.0 contains a SQL injection vulnerability in the 'es_messagesid' parameter that allows attackers to manipulate database queries through GET requests. Attackers can exploit the vulnerable parameter by injecting crafted SQL statements to potentially extract, modify, or delete database information.	8.2	More Details
CVE-2020-37057	Online-Exam-System 2015 contains a SQL injection vulnerability in the feedback module that allows attackers to manipulate database queries through the 'fid' parameter. Attackers can inject malicious SQL code into the 'fid' parameter to potentially extract, modify, or delete database information.	8.2	More Details
CVE-2025-1395	Generation of Error Message Containing Sensitive Information vulnerability in Codriapp Innovation and Software Technologies Inc. HeyGarson allows Fuzzing for application mapping.This issue affects HeyGarson: through 30012026. NOTE: The vendor was contacted several times to verifying fixing process but did not respond in any way.	8.2	More Details
CVE-2020-37006	berliCRM 1.0.24 contains a SQL injection vulnerability in the 'src_record' parameter that allows remote attackers to manipulate database queries. Attackers can inject malicious SQL code through a crafted POST request to the index.php endpoint to potentially extract or modify database information.	8.2	More Details
CVE-2025-55292	Meshtastic is an open source mesh networking solution. In the current Meshtastic architecture, a Node is identified by their NodeID, generated from the MAC address, rather than their public key. This aspect downgrades the security, specifically by abusing the HAM mode which doesn't use encryption. An attacker can, as such, forge a NodeInfo on behalf of a victim node advertising that the HAM mode is enabled. This, in turn, will allow the other nodes on the mesh to accept the new information and overwriting the NodeDB. The other nodes will then only be able to send direct messages to the victim by using the shared channel key instead of the PKC. Additionally, because HAM mode by design doesn't provide any confidentiality or authentication of information, the attacker could potentially also be able to change the Node details, like the full name, short code, etc. To keep the attack persistent, it is enough to regularly resend the forged NodeInfo, in particular right after the victim sends their own. A patch is available in version 2.7.6.834c3c5.	8.2	More Details
CVE-2020-37076	Victor CMS version 1.0 contains a SQL injection vulnerability in the 'post' parameter on post.php that allows remote attackers to manipulate database queries. Attackers can exploit this vulnerability by sending crafted UNION SELECT payloads to extract database information through boolean-based, error-based, and time-based injection techniques.	8.2	More Details
CVE-2026-24842	node-tar,a Tar for Node.js, contains a vulnerability in versions prior to 7.5.7 where the security check for hardlink entries uses different path resolution semantics than the actual hardlink creation logic. This mismatch allows an attacker to craft a malicious TAR archive that bypasses path traversal protections and creates hardlinks to arbitrary files outside the extraction directory. Version 7.5.7 contains a fix for the issue.	8.2	More Details
CVE-2019-25260	OXID eShop versions 6.x prior to 6.3.4 contains a SQL injection vulnerability in the 'sorting' parameter that allows attackers to insert malicious database content. Attackers can exploit the vulnerability by manipulating the sorting parameter to inject PHP code into the database and execute arbitrary code through crafted URLs.	8.2	More Details
CVE-2020-37110	60CycleCMS 2.5.2 contains an SQL injection vulnerability in news.php and common/lib.php that allows attackers to manipulate database queries through unvalidated user input. Attackers can exploit vulnerable query parameters like 'title' to inject malicious SQL code and potentially extract or modify database contents. This issue	8.2	More Details

	does not involve cross-site scripting.		
CVE-2020-36999	Elaniin CMS 1.0 contains an authentication bypass vulnerability that allows attackers to access the dashboard by manipulating the login page with SQL injection. Attackers can bypass authentication by sending crafted email and password parameters with '=''or' payload to login.php, granting unauthorized access to the system.	8.2	More Details
CVE-2020-37004	Ultimate Project Manager CRM PRO 2.0.5 contains a blind SQL injection vulnerability that allows attackers to extract usernames and password hashes from the tbl_users database table. Attackers can exploit the /frontend/get_article_suggestion/ endpoint by crafting malicious search parameters to progressively guess and retrieve user credentials through boolean-based inference techniques.	8.2	More Details
CVE-2025-40536	SolarWinds Web Help Desk was found to be susceptible to a security control bypass vulnerability that if exploited, could allow an unauthenticated attacker to gain access to certain restricted functionality.	8.1	More Details
CVE-2025-67848	A flaw was found in Moodle. This authentication bypass vulnerability allows suspended users to authenticate through the Learning Tools Interoperability (LTI) Provider. The issue arises from the LTI authentication handlers failing to enforce the user's suspension status, enabling unauthorized access to the system. This can lead to information disclosure or other unauthorized actions by users who should be restricted.	8.1	More Details
CVE-2025-13982	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Login Time Restriction allows Cross Site Request Forgery.This issue affects Login Time Restriction: from 0.0.0 before 1.0.3.	8.1	More Details
CVE-2026-1375	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to Insecure Direct Object References (IDOR) in all versions up to, and including, 3.9.5. This is due to missing object-level authorization checks in the `course_list_bulk_action()`, `bulk_delete_course()`, and `update_course_status()` functions. This makes it possible for authenticated attackers, with Tutor Instructor-level access and above, to modify or delete arbitrary courses they do not own by manipulating course IDs in bulk action requests.	8.1	More Details
CVE-2025-14975	The Custom Login Page Customizer WordPress plugin before 2.5.4 does not have a proper password reset process, allowing a few unauthenticated requests to reset the password of any user by knowing their username, such as administrator ones, and therefore gain access to their account	8.1	More Details
CVE-2026-25060	OpenList Frontend is a UI component for OpenList. Prior to 4.1.10, certificate verification is disabled by default for all storage driver communications. The TlsInsecureSkipVerify setting is default to true in the DefaultConfig() function in internal/conf/config.go. This vulnerability enables Man-in-the-Middle (MitM) attacks by disabling TLS certificate verification, allowing attackers to intercept and manipulate all storage communications. Attackers can exploit this through network-level attacks like ARP spoofing, rogue Wi-Fi access points, or compromised internal network equipment to redirect traffic to malicious endpoints. Since certificate validation is skipped, the system will unknowingly establish encrypted connections with attacker-controlled servers, enabling full decryption, data theft, and manipulation of all storage operations without triggering any security warnings. This vulnerability is fixed in 4.1.10.	8.1	More Details
CVE-2026-1803	A weakness has been identified in Ziroom ZHOME A0101 1.0.1.0. Impacted is an unknown function of the component Dropbear SSH Service. This manipulation causes use of default credentials. Remote exploitation of the attack is possible. The complexity of an attack is rather high. The exploitability is considered difficult. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	8.1	More Details
	jsPDF is a library to generate PDFs in JavaScript. Prior to 4.1.0, user control of properties and methods of the Acroform module allows users to inject arbitrary PDF objects, such as JavaScript actions. If given the possibility to pass unsanitized input to one of the following		

CVE-2026-24737	methods or properties, a user can inject arbitrary PDF objects, such as JavaScript actions, which are executed when the victim opens the document. The vulnerable API members are AcroformChoiceField.addOption, AcroformChoiceField.setOptions, AcroFormCheckBox.appearanceState, and AcroFormRadioButton.appearanceState. The vulnerability has been fixed in jsPDF@4.1.0.	8.1	More Details
CVE-2021-47909	Mult-E-Cart Ultimate 2.4 contains multiple SQL injection vulnerabilities in inventory, customer, vendor, and order modules. Remote attackers with privileged vendor or admin roles can exploit the 'id' parameter to execute malicious SQL commands and compromise the database management system.	8.1	More Details
CVE-2021-47915	PHP Melody version 3.0 contains a remote SQL injection vulnerability in the video edit module that allows authenticated attackers to inject malicious SQL commands. Attackers can exploit the unvalidated 'vid' parameter to execute arbitrary database queries and potentially compromise the web application and database management system.	8.1	More Details
CVE-2021-47918	Simple CMS 2.1 contains a remote SQL injection vulnerability that allows privileged attackers to inject unfiltered SQL commands in the users module. Attackers can exploit unvalidated input parameters in the admin.php file to compromise the database management system and web application.	8.1	More Details
CVE-2025-14472	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Acquia Content Hub allows Cross Site Request Forgery.This issue affects Acquia Content Hub: from 0.0.0 before 3.6.4, from 3.7.0 before 3.7.3.	8.1	More Details
CVE-2026-1531	A flaw was found in foreman_kubevirt. When configuring the connection to OpenShift, the system disables SSL verification if a Certificate Authority (CA) certificate is not explicitly set. This insecure default allows a remote attacker, capable of intercepting network traffic between Satellite and OpenShift, to perform a Man-in-the-Middle (MITM) attack. Such an attack could lead to the disclosure or alteration of sensitive information.	8.1	More Details
CVE-2026-1530	A flaw was found in fog-kubevirt. This vulnerability allows a remote attacker to perform a Man-in-the-Middle (MITM) attack due to disabled certificate validation. This enables the attacker to intercept and potentially alter sensitive communications between Satellite and OpenShift, resulting in information disclosure and data integrity compromise.	8.1	More Details
CVE-2026-1610	A vulnerability was found in Tenda AX12 Pro V2 16.03.49.24_cn. Affected by this issue is some unknown functionality of the component Telnet Service. Performing a manipulation results in hard-coded credentials. The attack is possible to be carried out remotely. A high degree of complexity is needed for the attack. The exploitation is known to be difficult. The exploit has been made public and could be used.	8.1	More Details
CVE-2025-7016	Improper Access Control vulnerability in Akın Software Computer Import Export Industry and Trade Ltd. QR Menu allows Authentication Abuse.This issue affects QR Menu: before s1.05.12.	8.0	More Details
CVE-2025-9974	The unified WEBUI application of the ONT/Beacon device contains an input handling flaw that allows authenticated users to trigger unintended system-level command execution. Due to insufficient validation of user-supplied data, a low-privileged authenticated attacker may be able to execute arbitrary commands on the underlying ONT/Beacon operating system, potentially impacting the confidentiality, integrity, and availability of the device.	8.0	More Details
CVE-2026-23997	FacturaScripts is open-source enterprise resource planning and accounting software. In 2025.71 and earlier, a Stored Cross-Site Scripting (XSS) vulnerability was discovered in the Observations field. The flaw occurs in the History view, where historical data is rendered without proper HTML entity encoding. This allows an attacker to execute arbitrary JavaScript in the browser of viewing the history by administrators.	8.0	More Details
CVE-2026-	Dokploy is a free, self-hostable Platform as a Service (PaaS). In versions prior to 0.26.6, a hardcoded credential in the provided installation script (located at https://dokploy.com/install.sh, line 154) uses a hardcoded password when creating the	8.0	More

24840	database container. This means that nearly all Dokploy installations use the same database credentials and could be compromised. Version 0.26.6 contains a patch for the issue.		Details
CVE-2025-33219	NVIDIA Display Driver for Linux contains a vulnerability in the NVIDIA kernel module where an attacker could cause an integer overflow or wraparound. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, or information disclosure.	7.8	More Details
CVE-2025-61731	Building a malicious file with cmd/go can cause can cause a write to an attacker-controlled file with partial control of the file content. The "#cgo pkg-config:" directive in a Go source file provides command-line arguments to provide to the Go pkg-config command. An attacker can provide a "--log-file" argument to this directive, causing pkg-config to write to an attacker-controlled location.	7.8	More Details
CVE-2025-33218	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where an attacker could cause an integer overflow. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, or information disclosure.	7.8	More Details
CVE-2026-24856	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Versions prior to 2.3.1.2 have an undefined behavior issue when floating-point NaN values are converted to unsigned short integer types during ICC profile XML parsing potentially corrupting memory structures and enabling arbitrary code execution. This vulnerability affects users of the iccDEV library who process ICC color profiles. ICC Profile Injection vulnerabilities arise when user-controllable input is incorporated into ICC profile data or other structured binary blobs in an unsafe manner. Version 2.3.1.2 contains a fix for the issue. No known workarounds are available.	7.8	More Details
CVE-2026-25502	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, stack-based buffer overflow in icFixXml() function when processing malformed ICC profiles, allows potential arbitrary code execution through crafted NamedColor2 tags. This issue has been patched in version 2.3.1.2.	7.8	More Details
CVE-2020-37017	CodeMeter 6.60 contains an unquoted service path vulnerability that allows local users to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted binary path in the CodeMeter Runtime Server service to inject malicious code that would execute with LocalSystem permissions.	7.8	More Details
CVE-2025-33220	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager, where a malicious guest could cause heap memory access after the memory is freed. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, or information disclosure.	7.8	More Details
CVE-2026-21418	Dell Unity, version(s) 5.5.2 and prior, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	7.8	More Details
CVE-2020-37020	SonarQube 8.3.1 contains an unquoted service path vulnerability that allows local attackers to gain SYSTEM privileges by exploiting the service executable path. Attackers can replace the wrapper.exe in the service path with a malicious executable to execute code with highest system privileges during service restart.	7.8	More Details
CVE-2025-69604	An issue in Shirt Pocket's SuperDuper! 3.11 and earlier allow a local attacker to modify the default task template to install an arbitrary package that can run shell scripts with root privileges and Full Disk Access, thus bypassing macOS privacy controls.	7.8	More Details
CVE-2020-37021	10-Strike Bandwidth Monitor 3.9 contains an unquoted service path vulnerability in multiple services that allows local attackers to escalate privileges. Attackers can place a malicious executable in specific file path locations to achieve privilege escalation to	7.8	More Details

	SYSTEM during service startup.		
CVE-2025-33217	NVIDIA Display Driver for Windows contains a vulnerability where an attacker could trigger a use after free. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	7.8	More Details
CVE-2020-37016	BarcodeOCR 19.3.6 contains an unquoted service path vulnerability that allows local attackers to execute code with elevated privileges during system startup. Attackers can exploit the unquoted path in the service configuration to inject malicious executables that will run with LocalSystem privileges.	7.8	More Details
CVE-2026-24149	NVIDIA Megatron-LM for all platforms contains a vulnerability in a script, where malicious data created by an attacker may cause a code injection issue. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, information disclosure, data tampering.	7.8	More Details
CVE-2020-37059	Popcorn Time 6.2.1.14 contains an unquoted service path vulnerability that allows local non-privileged users to potentially execute code with elevated system privileges. Attackers can insert malicious executables in Program Files (x86) or system root directories to be executed with SYSTEM-level permissions during service startup.	7.8	More Details
CVE-2020-36985	IP Watcher 3.0.0.30 contains an unquoted service path vulnerability in its Windows service configuration that allows local attackers to execute arbitrary code. Attackers can exploit the unquoted binary path to inject malicious executables that will be launched with elevated LocalSystem privileges during service startup.	7.8	More Details
CVE-2026-22277	Dell UnityVSA, version(s) 5.4 and prior, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	7.8	More Details
CVE-2020-37061	BOOTP Turbo 2.0.1214 contains an unquoted service path vulnerability that allows local attackers to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted executable path to inject malicious code that will be executed when the service starts with LocalSystem permissions.	7.8	More Details
CVE-2020-37063	TFTP Turbo 4.6.1273 contains an unquoted service path vulnerability that allows local attackers to potentially execute arbitrary code with elevated privileges. Attackers can exploit the unquoted path in the service configuration to inject malicious executables that will be launched with LocalSystem permissions.	7.8	More Details
CVE-2020-37030	Outline Service 1.3.3 contains an unquoted service path vulnerability that allows local users to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted binary path in C:\Program Files (x86)\Outline to inject malicious code that would execute with LocalSystem permissions during service startup.	7.8	More Details
CVE-2026-20409	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10363246; Issue ID: MSV-5779.	7.8	More Details
CVE-2026-20411	In cameraisp, there is a possible escalation of privilege due to use after free. This could lead to local denial of service if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10351676; Issue ID: MSV-5737.	7.8	More Details
CVE-2026-20412	In cameraisp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10351676; Issue ID: MSV-5733.	7.8	More Details

CVE-2026-24071	It was found that the XPC service offered by the privileged helper of Native Access uses the PID of the connecting client to verify its code signature. This is considered insecure and can be exploited by PID reuse attacks. The connection handler function uses _xpc_connection_get_pid(arg2) as argument for the hasValidSignature function. This value can not be trusted since it is vulnerable to PID reuse attacks.	7.8	More Details
CVE-2025-47358	Memory Corruption when user space address is modified and passed to mem_free API, causing kernel memory to be freed inadvertently.	7.8	More Details
CVE-2025-47359	Memory Corruption when multiple threads simultaneously access a memory free API.	7.8	More Details
CVE-2025-47397	Memory Corruption when initiating GPU memory mapping using scatter-gather lists due to unchecked IOMMU mapping errors.	7.8	More Details
CVE-2025-47398	Memory Corruption while deallocating graphics processing unit memory buffers due to improper handling of memory pointers.	7.8	More Details
CVE-2025-47399	Memory Corruption while processing IOCTL call to update sensor property settings with invalid input parameters.	7.8	More Details
CVE-2020-37102	Adaware Web Companion 4.9.2159 contains an unquoted service path vulnerability in the WCAssistantService that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted binary path to inject malicious executables that will be run with LocalSystem privileges during service startup.	7.8	More Details
CVE-2020-37101	VPN Unlimited 6.1 contains an unquoted service path vulnerability that allows local attackers to inject malicious executables into the service binary path. Attackers can exploit the unquoted path in 'C:\Program Files (x86)\VPN Unlimited\' to replace the service executable and gain elevated system privileges.	7.8	More Details
CVE-2020-37100	Sync Breeze Enterprise 12.4.18 contains an unquoted service path vulnerability that allows local attackers to execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted binary path by placing malicious executables in specific file system locations to hijack the service startup process.	7.8	More Details
CVE-2020-37099	Disk Savvy Enterprise 12.3.18 contains an unquoted service path vulnerability in its service configuration that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in 'C:\Program Files\Disk Savvy Enterprise\bin\disksvs.exe' to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2020-37098	Disk Sorter Enterprise 12.4.16 contains an unquoted service path vulnerability that allows local attackers to execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted path in the service configuration to inject malicious executables that will be launched with LocalSystem permissions.	7.8	More Details
CVE-2019-25261	AnyDesk 5.4.0 contains an unquoted service path vulnerability in its Windows service configuration that allows local attackers to potentially inject malicious executables. Attackers can exploit the unquoted binary path to place malicious files in service executable locations, potentially gaining elevated system privileges.	7.8	More Details
CVE-2020-37062	DHCP Turbo 4.61298 contains an unquoted service path vulnerability that allows local attackers to potentially execute arbitrary code by exploiting the service binary path. Attackers can place malicious executables in the service path to gain elevated privileges when the service starts.	7.8	More Details
CVE-	EPSON EasyMP Network Projection 2.81 contains an unquoted service path vulnerability in the EMP_NSWLSV service that allows local users to potentially execute arbitrary code.		

2020-37064	Attackers can exploit the unquoted path in C:\Program Files (x86)\EPSON Projector\EasyMP Network Projection V2\ to inject malicious code that would execute with LocalSystem privileges.	7.8	More Details
CVE-2020-37055	SpyHunter 4 contains an unquoted service path vulnerability that allows local users to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted service path by placing malicious executables in specific file system locations to gain elevated access during service startup.	7.8	More Details
CVE-2020-36987	Program Access Controller 1.2.0.0 contains an unquoted service path vulnerability in PACService.exe that allows local attackers to execute code with elevated privileges. Attackers can exploit the unquoted path during system startup or reboot to inject and run malicious executables with LocalSystem permissions.	7.8	More Details
CVE-2020-37058	Andrea ST Filters Service 1.0.64.7 contains an unquoted service path vulnerability in its Windows service configuration. Local attackers can exploit the unquoted path to inject malicious code that will execute with elevated LocalSystem privileges during service startup.	7.8	More Details
CVE-2020-37060	Atomic Alarm Clock 6.3 contains a local privilege escalation vulnerability in its service configuration that allows attackers to execute arbitrary code with SYSTEM privileges. Attackers can exploit the unquoted service path by placing a malicious executable named 'Program.exe' to gain persistent system-level access.	7.8	More Details
CVE-2025-62348	Salt's junos execution module contained an unsafe YAML decode/load usage. A specially crafted YAML payload processed by the junos module could lead to unintended code execution under the context of the Salt process.	7.8	More Details
CVE-2025-57283	The Node.js package browserstack-local 1.5.8 contains a command injection vulnerability. This occurs because the logfile variable is not properly sanitized in lib/Local.js.	7.8	More Details
CVE-2020-36992	Nord VPN 6.31.13.0 contains an unquoted service path vulnerability in its nordvpn-service that allows local attackers to execute code with elevated privileges. Attackers can exploit the unquoted binary path during system startup or reboot to potentially run malicious code with LocalSystem permissions.	7.8	More Details
CVE-2020-36991	ShareMouse 5.0.43 contains an unquoted service path vulnerability that allows local users to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the insecure service path configuration by placing malicious executables in specific system directories to gain elevated access during service startup.	7.8	More Details
CVE-2020-37048	Iskysoft Application Framework Service 2.4.3.241 contains an unquoted service path vulnerability that allows local users to potentially execute arbitrary code with elevated privileges. Attackers can exploit the unquoted path in the service configuration to inject malicious executables that would be run with the service's high-level system permissions.	7.8	More Details
CVE-2020-36989	ForensiT AppX Management Service 2.2.0.4 contains an unquoted service path vulnerability that allows local users to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted path in the service configuration to inject malicious code that would execute with LocalSystem account permissions during service startup.	7.8	More Details
CVE-2020-36990	Input Director 1.4.3 contains an unquoted service path vulnerability in its Windows service configuration that allows local attackers to execute code with elevated privileges. Attackers can exploit the unquoted path during system startup or reboot to inject and run malicious executables with LocalSystem permissions.	7.8	More Details
CVE-2025-46691	Dell PremierColor Panel Driver, versions prior to 1.0.0.1 A01, contains an Improper Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	7.8	More Details

CVE-2020-37037	Avast SecureLine 5.5.522.0 contains an unquoted service path vulnerability that allows local users to potentially execute code with elevated system privileges. Attackers can exploit the unquoted path in the service configuration to inject malicious code that would execute with LocalSystem account permissions during service startup.	7.8	More Details
CVE-2020-36986	Prey 1.9.6 contains an unquoted service path vulnerability that allows local users to potentially execute code with elevated privileges. Attackers can exploit the unquoted path in the CronService to insert malicious code that would execute during application startup or system reboot.	7.8	More Details
CVE-2020-36984	EPSON 1.124 contains an unquoted service path vulnerability in the SENADB service that allows local attackers to execute code with elevated system privileges. Attackers can exploit the unquoted path in C:\Program Files (x86)\EPSON_P2B\Printer Software\Status Monitor\ to inject malicious executables that will run with LocalSystem permissions.	7.8	More Details
CVE-2026-24669	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, an insecure password reset mechanism allows local attackers to reuse a valid password reset token after it has already been used, enabling unauthorized password changes and potential account takeover. This issue has been patched in version 4.2.	7.8	More Details
CVE-2020-37047	Deep Instinct Windows Agent 1.2.29.0 contains an unquoted service path vulnerability in the DeepMgmtService that allows local users to potentially execute code with elevated privileges. Attackers can exploit the unquoted path in C:\Program Files\HP Sure Sense\DeepMgmtService.exe to inject malicious code that would execute with LocalSystem permissions during service startup.	7.8	More Details
CVE-2020-37045	Veritas NetBackup 7.0 contains an unquoted service path vulnerability in the NetBackup INET Daemon service that allows local users to potentially execute arbitrary code. Attackers can exploit the unquoted path in C:\Program Files\Veritas\NetBackup\bin\bpinetd.exe to inject malicious code that would execute with elevated LocalSystem privileges.	7.8	More Details
CVE-2022-40620	FunJSQ, a third-party module integrated on some NETGEAR routers and Orbi WiFi Systems, does not properly validate TLS certificates when downloading update packages through its auto-update mechanism. An attacker (suitably positioned on the network) could intercept the update request and deliver a malicious update package in order to gain arbitrary code execution on affected devices. This affects R6230 before 1.1.0.112, R6260 before 1.1.0.88, R7000 before 1.0.11.134, R8900 before 1.0.5.42, R9000 before 1.0.5.42, and XR300 before 1.0.3.72 and Orbi RBR20 before 2.7.2.26, RBR50 before 2.7.4.26, RBS20 before 2.7.2.26, and RBS50 before 2.7.4.26.	7.7	More Details
CVE-2022-40619	FunJSQ, a third-party module integrated on some NETGEAR routers and Orbi WiFi Systems, exposes an HTTP server over the LAN interface of affected devices. This interface is vulnerable to unauthenticated arbitrary command injection through the funjsq_access_token parameter. This affects R6230 before 1.1.0.112, R6260 before 1.1.0.88, R7000 before 1.0.11.134, R8900 before 1.0.5.42, R9000 before 1.0.5.42, and XR300 before 1.0.3.72 and Orbi RBR20 before 2.7.2.26, RBR50 before 2.7.4.26, RBS20 before 2.7.2.26, and RBS50 before 2.7.4.26.	7.7	More Details
CVE-2026-25153	Backstage is an open framework for building developer portals, and @backstage/plugin-techdocs-node provides common node.js functionalities for TechDocs. In versions of @backstage/plugin-techdocs-node prior to 1.13.11 and 1.14.1, when TechDocs is configured with `runIn: local`, a malicious actor who can submit or modify a repository's `mkdocs.yml` file can execute arbitrary Python code on the TechDocs build server via MkDocs hooks configuration. @backstage/plugin-techdocs-node versions 1.13.11 and 1.14.1 contain a fix. The fix introduces an allowlist of supported MkDocs configuration keys. Unsupported configuration keys (including `hooks`) are now removed from `mkdocs.yml` before running the generator, with a warning logged to indicate which keys were removed. Users of `@techdocs/cli` should also upgrade to the latest version, which includes the fixed `@backstage/plugin-techdocs-node` dependency. Some workarounds are available. Configure TechDocs with `runIn: docker` instead of `runIn: local` to provide	7.7	More Details

	container isolation, though it does not fully mitigate the risk. Limit who can modify `mkdocs.yml` files in repositories that TechDocs processes; only allow trusted contributors. Implement PR review requirements for changes to `mkdocs.yml` files to detect malicious `hooks` configurations before they are merged. Use MkDocs < 1.4.0 (e.g., 1.3.1) which does not support hooks. Note: This may limit access to newer MkDocs features. Building documentation in CI/CD pipelines using `@techdocs/cli` does not mitigate this vulnerability, as the CLI uses the same vulnerable `@backstage/plugin-techdocs-node` package.		
CVE-2022-50976	A local attacker could cause a full device reset by resetting the device passwords using an invalid reset file via USB.	7.7	More Details
CVE-2025-68662	Discourse is an open source discussion platform. In versions prior to 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0, a hostname validation issue in FinalDestination could allow bypassing SSRF protections under certain conditions. This issue is patched in versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0. No known workarounds are available.	7.6	More Details
CVE-2025-14914	IBM WebSphere Application Server Liberty 17.0.0.3 through 26.0.0.1 could allow a privileged user to upload a zip archive containing path traversal sequences resulting in an overwrite of files leading to arbitrary code execution.	7.6	More Details
CVE-2025-8461	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Seres Software syWEB allows Reflected XSS.This issue affects syWEB: through 03022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.6	More Details
CVE-2025-8456	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kod8 Software Technologies Trade Ltd. Co. Kod8 Individual and SME Website allows Reflected XSS.This issue affects Kod8 Individual and SME Website: through 03022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.6	More Details
CVE-2025-8589	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AKCE Software Technology R&D Industry and Trade Inc. SKSPro allows Reflected XSS.This issue affects SKSPro: through 07012026.	7.6	More Details
CVE-2026-25116	Runtipi is a personal homeserver orchestrator. Starting in version 4.5.0 and prior to version 4.7.2, an unauthenticated Path Traversal vulnerability in the `UserConfigController` allows any remote user to overwrite the system's `docker-compose.yml` configuration file. By exploiting insecure URN parsing, an attacker can replace the primary stack configuration with a malicious one, resulting in full Remote Code Execution (RCE) and host filesystem compromise the next time the instance is restarted by the operator. Version 4.7.2 fixes the vulnerability.	7.6	More Details
CVE-2025-7760	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ofisimo Web-Based Software Technologies Association Web Package Flora allows XSS Through HTTP Headers.This issue affects Association Web Package Flora: from v3.0 through 03022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.6	More Details
CVE-2026-24833	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to versions 9.13.10 and 10.2.0, a module could install with richtext in its description field which could contain scripts that will run for user in the Persona Bar. Versions 9.13.10 and 10.2.0 contain a fix for the issue.	7.6	More Details
CVE-2026-24836	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Starting in version 9.0.0 and prior to versions 9.13.10 and 10.2.0, extensions could write richtext in log notes which can include scripts that would run in the PersonaBar when displayed. Versions 9.13.10 and 10.2.0 contain a fix for the issue.	7.6	More Details
	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS)		

CVE-2026-24837	in the Microsoft ecosystem. Starting in version 9.0.0 and prior to versions 9.13.10 and 10.2.0, a module friendly name could include scripts that will run during some module operations in the Persona Bar. Versions 9.13.10 and 10.2.0 contain a fix for the issue.	7.6	More Details
CVE-2025-14840	Improper Check for Unusual or Exceptional Conditions vulnerability in Drupal HTTP Client Manager allows Forceful Browsing.This issue affects HTTP Client Manager: from 0.0.0 before 9.3.13, from 10.0.0 before 10.0.2, from 11.0.0 before 11.0.1.	7.5	More Details
CVE-2020-37097	Edimax EW-7438RPn 1.13 contains an information disclosure vulnerability that exposes WiFi network configuration details through the wlencrypt_wiz.asp file. Attackers can access the script to retrieve sensitive information including WiFi network name and plaintext password stored in device configuration variables.	7.5	More Details
CVE-2026-24773	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, an Insecure Direct Object Reference (IDOR) vulnerability allows unauthenticated remote attackers to access personal files of other users by directly requesting predictable user identifiers. This issue has been patched in version 4.2.	7.5	More Details
CVE-2025-65891	A GPU device-ID validation flaw in OneFlow v0.9.0 allows attackers to trigger a Denial of Dervice (DoS) by invoking flow.cuda.get_device_properties() with an invalid or negative device index.	7.5	More Details
CVE-2025-7714	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Global Interactive Design Media Software Inc. Content Management System (CMS) allows Command Line Execution through SQL Injection.This issue affects Content Management System (CMS): through 21072025.	7.5	More Details
CVE-2025-7713	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Global Interactive Design Media Software Inc. Content Management System (CMS) allows XSS Through HTTP Headers.This issue affects Content Management System (CMS): through 21072025.	7.5	More Details
CVE-2025-70999	A GPU device-ID validation flaw in the flow.cuda.get_device_capability() component of OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via a crafted device ID.	7.5	More Details
CVE-2025-71000	An issue in the flow.cuda.BoolTensor component of OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2020-37092	Netis E1+ version 1.2.32533 contains a hardcoded root account vulnerability that allows unauthenticated attackers to access the device with predefined credentials. Attackers can leverage the embedded root account with a crackable password to gain full administrative access to the network device.	7.5	More Details
CVE-2020-37015	Ruijie Networks Switch eWeb S29_RGOS 11.4 contains a directory traversal vulnerability that allows unauthenticated attackers to access sensitive configuration files by manipulating file path parameters. Attackers can exploit the /download.do endpoint with '../' sequences to retrieve system configuration files containing credentials and network settings.	7.5	More Details
CVE-2020-37093	Netis E1+ 1.2.32533 contains an information disclosure vulnerability that allows unauthenticated attackers to retrieve WiFi passwords through the netcore_get.cgi endpoint. Attackers can send a GET request to the endpoint to extract sensitive network credentials including SSID and WiFi passwords in plain text.	7.5	More Details
CVE-2020-37008	EasyPMS 1.0.0 contains an authentication bypass vulnerability that allows unprivileged users to manipulate SQL queries in JSON requests to access admin user information. Attackers can exploit weak input validation by injecting single quotes in ID parameters and modify admin user passwords without proper token authentication.	7.5	More Details

CVE-2020-36995	Mocha Telnet Lite for iOS 4.2 contains a denial of service vulnerability that allows attackers to crash the application by manipulating the user configuration input. Attackers can overwrite the 'User' field with 350 bytes of repeated characters to trigger an application crash and prevent normal functionality.	7.5	More Details
CVE-2026-25223	Fastify is a fast and low overhead web framework, for Node.js. Prior to version 5.7.2, a validation bypass vulnerability exists in Fastify where request body validation schemas specified by Content-Type can be completely circumvented. By appending a tab character (\t) followed by arbitrary content to the Content-Type header, attackers can bypass body validation while the server still processes the body as the original content type. This issue has been patched in version 5.7.2.	7.5	More Details
CVE-2026-1280	The Frontend File Manager Plugin for WordPress is vulnerable to unauthorized file sharing due to a missing capability check on the 'wpfm_send_file_in_email' AJAX action in all versions up to, and including, 23.5. This makes it possible for unauthenticated attackers to share arbitrary uploaded files via email by supplying a file ID. Since file IDs are sequential integers, attackers can enumerate all uploaded files on the site and exfiltrate sensitive data that was intended to be restricted to administrators only.	7.5	More Details
CVE-2026-1616	The uriargs concatenation in nginx configuration file present in Open Security Issue Management (OSIM) prior v2025.9.0 allows path traversal attacks via query parameters.	7.5	More Details
CVE-2026-0702	The VidShop – Shoppable Videos for WooCommerce plugin for WordPress is vulnerable to time-based SQL Injection via the 'fields' parameter in all versions up to, and including, 1.1.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-20402	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00693083; Issue ID: MSV-5928.	7.5	More Details
CVE-2026-20403	In Modem, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01689254 (Note: For N15 and NR16) / MOLY01689259 (Note: For NR17 and NR17R); Issue ID: MSV-4843.	7.5	More Details
CVE-2026-20404	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01689248; Issue ID: MSV-4837.	7.5	More Details
CVE-2026-20405	In Modem, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01688495; Issue ID: MSV-4818.	7.5	More Details
CVE-2026-20406	In Modem, there is a possible system crash due to an uncaught exception. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01726634; Issue ID: MSV-5728.	7.5	More Details
CVE-2025-40537	SolarWinds Web Help Desk was found to be susceptible to a hardcoded credentials vulnerability that, under certain situations, could allow access to administrative functions.	7.5	More Details
CVE-2020-	School ERP Pro 1.0 contains a file disclosure vulnerability that allows unauthenticated attackers to read arbitrary files by manipulating the 'document' parameter in download.php. Attackers can access sensitive configuration files by supplying directory	7.5	More

37088	traversal paths to retrieve system credentials and configuration information.		Details
CVE-2020-37039	Frigate 2.02 contains a denial of service vulnerability that allows attackers to crash the application by sending oversized input to the command line interface. Attackers can generate a payload of 8000 repeated characters and paste it into the application's command line field to trigger an application crash.	7.5	More Details
CVE-2020-37041	OpenCTI 3.3.1 is vulnerable to a directory traversal attack via the static/css endpoint. An unauthenticated attacker can read arbitrary files from the filesystem by sending crafted GET requests with path traversal sequences (e.g., '../') in the URL. For example, requesting /static/css//../../../../../../../etc/passwd returns the contents of /etc/passwd. This vulnerability was discovered by Raif Berkay Dincel and confirmed on Linux Mint and Windows 10.	7.5	More Details
CVE-2026-20420	In Modem, there is a possible system crash due to incorrect error handling. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01738313; Issue ID: MSV-5935.	7.5	More Details
CVE-2025-65890	A device-ID validation flaw in OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) by calling flow.cuda.synchronize() with an invalid or out-of-range GPU device index.	7.5	More Details
CVE-2025-65889	A type validation flaw in the flow.dstack() component of OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2020-36943	aSc TimeTables 2021.6.2 contains a denial of service vulnerability that allows attackers to crash the application by overwriting subject title fields with excessive data. Attackers can generate a 10,000-character buffer and paste it into the subject title to trigger application instability and potential crash.	7.5	More Details
CVE-2025-65888	A dimension validation flaw in the flow.empty() component of OneFlow 0.9.0 allows attackers to cause a Denial of Service (DoS) via a negative or excessively large dimension value.	7.5	More Details
CVE-2024-4027	A flaw was found in Undertow. Servlets using a method that calls HttpServletRequestImpl.getParameterNames() can cause an OutOfMemoryError when the client sends a request with large parameter names. This issue can be exploited by an unauthorized user to cause a remote denial-of-service (DoS) attack.	7.5	More Details
CVE-2025-65886	A shape mismatch vulnerability in OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via supplying crafted tensor shapes.	7.5	More Details
CVE-2020-36963	Intelbras Router RF 301K firmware version 1.1.2 contains an authentication bypass vulnerability that allows unauthenticated attackers to download router configuration files. Attackers can send a specific HTTP GET request to /cgi-bin/DownloadCfg/RouterCfm.cfg to retrieve sensitive router configuration without authentication.	7.5	More Details
CVE-2026-25128	fast-xml-parser allows users to validate XML, parse XML to JS object, or build XML from JS object without C/C++ based libraries and no callback. In versions 4.3.6 through 5.3.3, a RangeError vulnerability exists in the numeric entity processing of fast-xml-parser when parsing XML with out-of-range entity code points (e.g., `&#9999999;` or `&#xFFFFFF;`). This causes the parser to throw an uncaught exception, crashing any application that processes untrusted XML input. Version 5.3.4 fixes the issue.	7.5	More Details
CVE-2025-63658	A stack overflow in the mk_http_index_lookup function (mk_server/mk_http.c) of monkey commit f37e984 allows attackers to cause a Denial of Service (DoS) via sending a crafted HTTP request to the server.	7.5	More Details
CVE-	An out-of-bounds read in the mk_mimetype_find function (mk_server/mk_mimetype.c) of		

2025-63657	monkey commit f37e984 allows attackers to cause a Denial of Service (DoS) via sending a crafted HTTP request to the server.	7.5	More Details
CVE-2025-63656	An out-of-bounds read in the header_cmp function (mk_server/mk_http_parser.c) of monkey commit f37e984 allows attackers to cause a Denial of Service (DoS) via sending a crafted HTTP request to the server.	7.5	More Details
CVE-2025-63655	A NULL pointer dereference in the mk_http_range_parse function (mk_server/mk_http.c) of monkey commit f37e984 allows attackers to cause a Denial of Service (DoS) via sending a crafted HTTP request to the server.	7.5	More Details
CVE-2025-63653	An out-of-bounds read in the mk_vhost_fdt_close function (mk_server/mk_vhost.c) of monkey commit f37e984 allows attackers to cause a Denial of Service (DoS) via sending a crafted HTTP request to the server.	7.5	More Details
CVE-2025-63652	A use-after-free in the mk_http_request_end function (mk_server/mk_http.c) of monkey commit f37e984 allows attackers to cause a Denial of Service (DoS) via sending a crafted HTTP request to the server.	7.5	More Details
CVE-2025-63651	A use-after-free in the mk_string_char_search function (mk_core/mk_string.c) of monkey commit f37e984 allows attackers to cause a Denial of Service (DoS) via sending a crafted HTTP request to the server.	7.5	More Details
CVE-2025-63650	An out-of-bounds read in the mk_ptr_to_buf in mk_core function (mk_memory.c) of monkey commit f37e984 allows attackers to cause a Denial of Service (DoS) via sending a crafted HTTP request to the server.	7.5	More Details
CVE-2025-63649	An out-of-bounds read in the http_parser_transfer_encoding_chunked function (mk_server/mk_http_parser.c) of monkey commit f37e984 allows attackers to cause a Denial of Service (DoS) via sending a crafted POST request to the server.	7.5	More Details
CVE-2026-25614	Blesta 3.x through 5.x before 5.13.3 allows object injection, aka CORE-5680.	7.5	More Details
CVE-2020-37085	VirtualTablet Server 3.0.2 contains a denial of service vulnerability that allows attackers to crash the service by sending oversized string payloads through the Thrift protocol. Attackers can exploit the vulnerability by sending a long string to the send_say() method, causing the server to become unresponsive.	7.5	More Details
CVE-2020-37034	HelloWeb 2.0 contains an arbitrary file download vulnerability that allows remote attackers to download system files by manipulating filepath and filename parameters. Attackers can send crafted GET requests to download.asp with directory traversal to access sensitive configuration and system files.	7.5	More Details
CVE-2020-37038	Code Blocks 20.03 contains a denial of service vulnerability that allows attackers to crash the application by manipulating input in the FSymbols search field. Attackers can paste a large payload of 5000 repeated characters into the search field to trigger an application crash.	7.5	More Details
CVE-2026-20419	In wlan AP/STA firmware, there is a possible system becoming irresponsive due to an uncaught exception. This could lead to remote (proximal/adjacent) denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00461663 / WCNCR00463309; Issue ID: MSV-4852.	7.5	More Details
CVE-2020-37011	Gnome Fonts Viewer 3.34.0 contains a heap corruption vulnerability that allows attackers to trigger an out-of-bounds write by crafting a malicious TTF font file. Attackers can generate a specially crafted TTF file with an oversized pattern to cause an infinite malloc() loop and potentially crash the gnome-font-viewer process.	7.5	More Details
CVE-2026-20421	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not	7.5	More Details

	needed for exploitation. Patch ID: MOLY01738293; Issue ID: MSV-5922.		
CVE-2022-50977	An unauthenticated remote attacker could potentially disrupt operations by switching between multiple configuration presets via HTTP.	7.5	More Details
CVE-2025-71003	An input validation vulnerability in the flow.arange() component of OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-71007	An input validation vulnerability in the oneflow.index_add component of OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-14550	An issue was discovered in 6.0 before 6.0.2, 5.2 before 5.2.11, and 4.2 before 4.2.28. `ASGIRequest` allows a remote attacker to cause a potential denial-of-service via a crafted request with multiple duplicate headers. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Jiyong Yang for reporting this issue.	7.5	More Details
CVE-2025-8590	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in AKCE Software Technology R&D Industry and Trade Inc. SKSPro allows Directory Indexing.This issue affects SKSPro: through 07012026.	7.5	More Details
CVE-2022-50978	An unauthenticated remote attacker could potentially disrupt operations by switching between multiple configuration presets via Modbus (TCP).	7.5	More Details
CVE-2026-20422	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00827332; Issue ID: MSV-5919.	7.5	More Details
CVE-2026-23743	Discourse is an open source discussion platform. In versions prior to 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0, permalinks pointing to access-restricted resources (private topics, categories, posts, or hidden tags) were redirecting users to URLs containing the resource slug, even when the user didn't have access to view the resource. This leaked potentially sensitive information (e.g., private topic titles) via the redirect Location header and the 404 page's search box. This issue is patched in versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0. No known workarounds are available.	7.5	More Details
CVE-2026-1285	An issue was discovered in 6.0 before 6.0.2, 5.2 before 5.2.11, and 4.2 before 4.2.28. `django.utils.text.Truncator.chars()` and `Truncator.words()` methods (with `html=True`) and the `truncatechars_html` and `truncatewords_html` template filters allow a remote attacker to cause a potential denial-of-service via crafted inputs containing a large number of unmatched HTML end tags. 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 Yoon for reporting this issue.	7.5	More Details
CVE-2024-54263	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Talemy Spirit Framework allows PHP Local File Inclusion.This issue affects Spirit Framework: from n/a through 1.2.13.	7.5	More Details
CVE-2025-67853	A flaw was found in Moodle. A remote attacker could exploit a lack of proper rate limiting in the confirmation email service. This vulnerability allows attackers to more easily enumerate or guess user credentials, facilitating brute-force attacks against user accounts.	7.5	More Details
CVE-2025-61726	The net/url package does not set a limit on the number of query parameters in a query. While the maximum size of query parameters in URLs is generally limited by the maximum request header size, the net/http.Request.ParseForm method can parse large URL-encoded forms. Parsing a large form containing many unique query parameters can cause excessive memory consumption.	7.5	More Details

CVE-2026-1594	A security vulnerability has been detected in itsourcecode Society Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/add_expenses.php. The manipulation of the argument detail leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-1595	A vulnerability was detected in itsourcecode Society Management System 1.0. This affects an unknown part of the file /admin/edit_student_query.php. The manipulation of the argument student_id results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-1590	A vulnerability was identified in itsourcecode School Management System 1.0. This impacts an unknown function of the file /ramonsys/faculty/index.php. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-1589	A vulnerability was determined in itsourcecode School Management System 1.0. This affects an unknown function of the file /ramonsys/inquiry/index.php. This manipulation of the argument txtsearch causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-1535	A security vulnerability has been detected in code-projects Online Music Site 1.0. This impacts an unknown function of the file /Administrator/PHP/AdminReply.php. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-24672	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, a Stored Cross-Site Scripting (XSS) vulnerability allows authenticated students to inject malicious JavaScript into user profile fields, which is executed when users with viewing privileges access affected application pages. This issue has been patched in version 4.2.	7.3	More Details
CVE-2026-1534	A weakness has been identified in code-projects Online Music Site 1.0. This affects an unknown function of the file /Administrator/PHP/AdminEditUser.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-1545	A weakness has been identified in itsourcecode School Management System 1.0. The affected element is an unknown function of the file /course/index.php. Executing a manipulation of the argument ID 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.	7.3	More Details
CVE-2026-1593	A weakness has been identified in itsourcecode Society Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/edit_expenses_query.php. Executing a manipulation of the argument detail 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 attacks.	7.3	More Details
CVE-2026-25156	HotCRP is conference review software. HotCRP versions from October 2025 through January 2026 delivered documents of all types with inline Content-Disposition, causing them to be rendered in the user’s browser rather than downloaded. (The intended behavior was for only `text/plain`, `application/pdf`, `image/gif`, `image/jpeg`, and `image/png` to be delivered inline, though adding `save=0` to the document URL could request inline delivery for any document.) This made users who clicked a document link vulnerable to cross-site scripting attacks. An uploaded HTML or SVG document would run in the viewer’s browser with access to their HotCRP credentials, and Javascript in that document could eventually make arbitrary calls to HotCRP’s API. Malicious documents could be uploaded to submission fields with “file upload” or “attachment” type, or as attachments to comments. PDF upload fields were not vulnerable. A search of documents uploaded to hotcrp.com found no evidence of exploitation. The vulnerability was	7.3	More Details

	introduced in commit aa20ef288828b04550950cf67c831af8a525f508 (11 October 2025), present in development versions and v3.2, and fixed in commit 8933e86c9f384b356dc4c6e9e2814dee1074b323 and v3.2.1. Additionally, c3d88a7e18d52119c65df31c2cc994edd2beccc5 and v3.2.1 remove support for `save=0`.		
CVE-2026-1740	A vulnerability was found in EFM ipTIME A8004T 14.18.2. This impacts the function httpcon_check_session_url of the file /cgi/timepro.cgi of the component Hidden Hiddenloginsetup Interface. The manipulation results in improper authentication. The attack may be performed from remote. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-1701	A security vulnerability has been detected in itsourcecode Student Management System 1.0. This issue affects some unknown processing of the file /enrollment/index.php. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-67850	A flaw was found in moodle. This vulnerability, known as Cross-Site Scripting (XSS), occurs due to insufficient checks on user-provided data in the formula editor's arithmetic expression fields. A remote attacker could inject malicious code into these fields. When other users view these expressions, the malicious code would execute in their web browsers, potentially compromising their data or leading to unauthorized actions.	7.3	More Details
CVE-2026-0832	The New User Approve plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a missing capability check on multiple REST API endpoints in all versions up to, and including, 3.2.2. This makes it possible for unauthenticated attackers to approve or deny user accounts, retrieve sensitive user information including emails and roles, and force logout of privileged users.	7.3	More Details
CVE-2026-1689	A vulnerability was detected in Tenda HG10 US_HG7_HG9_HG10re_300001138_en_xpon. The impacted element is the function checkUserFromLanOrWan of the file /boaform/admin/formLogin of the component Login Interface. The manipulation of the argument Host results in command injection. The attack can be launched remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-67849	A flaw was found in Moodle. This cross-site scripting (XSS) vulnerability, caused by improper sanitization of AI prompt responses, allows attackers to inject malicious HTML or script into web pages. When other users view these compromised pages, their sessions could be stolen, or the user interface could be manipulated.	7.3	More Details
CVE-2026-1687	A weakness has been identified in Tenda HG10 US_HG7_HG9_HG10re_300001138_en_xpon. Impacted is an unknown function of the file /boaform/formSamba of the component Boa Webserver. Executing a manipulation of the argument serverString can lead to command injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-1688	A security vulnerability has been detected in itsourcecode Directory Management System 1.0. The affected element is an unknown function of the file /admin/index.php. The manipulation of the argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-1802	A security flaw has been discovered in Ziroom ZHOME A0101 1.0.1.0. This issue affects the function macAddrClone of the file luci\controller\api\zrMacClone.lua. The manipulation of the argument macType results in command injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-25615	Blesta 3.x through 5.x before 5.13.3 allows object injection, aka CORE-5668.	7.2	More Details

CVE-2026-23896	immich is a high performance self-hosted photo and video management solution. Prior to version 2.5.0, API keys can escalate their own permissions by calling the update endpoint, allowing a low-privilege API key to grant itself full administrative access to the system. Version 2.5.0 fixes the issue.	7.2	More Details
CVE-2020-37072	Victor CMS 1.0 contains a stored cross-site scripting vulnerability in the 'comment_author' POST parameter that allows attackers to inject malicious scripts. Attackers can submit crafted JavaScript payloads through the comment submission form to execute arbitrary code in victim browsers.	7.2	More Details
CVE-2026-0709	Some Hikvision Wireless Access Points are vulnerable to authenticated command execution due to insufficient input validation. Attackers with valid credentials can exploit this flaw by sending crafted packets containing malicious commands to affected devices, leading to arbitrary command execution.	7.2	More Details
CVE-2026-22623	Due to insufficient input parameter validation on the interface, authenticated users of certain HIKSEMI NAS products can execute arbitrary commands on the device by crafting specific messages.	7.2	More Details
CVE-2026-1505	A vulnerability was found in D-Link DIR-615 4.10. This issue affects some unknown processing of the file /set_temp_nodes.php of the component URL Filter. The manipulation results in os command injection. The attack can be executed remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	7.2	More Details
CVE-2026-1400	The AI Engine – The Chatbot and AI Framework for WordPress plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the `rest_helpers_update_media_metadata` function in all versions up to, and including, 3.3.2. This makes it possible for authenticated attackers, with Editor-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. The attacker can upload a benign image file, then use the `update_media_metadata` endpoint to rename it to a PHP file, creating an executable PHP file in the uploads directory.	7.2	More Details
CVE-2025-36184	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 - 11.5.9 could allow an instance owner to execute malicious code that escalate their privileges to root due to execution of unnecessary privileges operated at a higher than minimum level.	7.2	More Details
CVE-2026-1777	The Amazon SageMaker Python SDK before v3.2.0 and v2.256.0 includes the ModelBuilder HMAC signing key in the cleartext response elements of the DescribeTrainingJob function. A third party with permissions to both call this API and permissions to modify objects in the Training Jobs S3 output location may have the ability to upload arbitrary artifacts which are executed the next time the Training Job is invoked.	7.2	More Details
CVE-2026-0617	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the customer profile fields in all versions up to, and including, 5.2.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an administrator views the customer's activity history.	7.2	More Details
CVE-2025-14610	The TableMaster for Elementor plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.3.6. This is due to the plugin not restricting which URLs can be fetched when importing CSV data from a URL in the Data Table widget. This makes it possible for authenticated attackers, with Author-level access and above, to make web requests to arbitrary locations, including localhost and internal network services, and read sensitive files such as wp-config.php via the 'csv_url' parameter.	7.2	More Details
CVE-	The Form Maker by 10Web plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 1.15.35. This is due to the plugin's default file upload allowlist including SVG files combined with weak substring-based extension		More

2026-1065	validation. This makes it possible for unauthenticated attackers to upload malicious SVG files containing JavaScript code that will execute when viewed by administrators or site visitors via file upload fields in forms granted they can submit forms.	7.2	Details
CVE-2026-1506	A vulnerability was determined in D-Link DIR-615 4.10. Impacted is an unknown function of the file /adv_mac_filter.php of the component MAC Filter Configuration. This manipulation of the argument mac causes os command injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. This vulnerability only affects products that are no longer supported by the maintainer.	7.2	More Details
CVE-2025-14554	The Sell BTC - Cryptocurrency Selling Calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'orderform_data' AJAX action in all versions up to, and including, 1.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in order records that will execute whenever an administrator accesses the Orders page in the admin dashboard. The vulnerability was partially patched in version 1.5.	7.2	More Details
CVE-2026-24902	TrustTunnel is an open-source VPN protocol with a server-side request forgery and and private network restriction bypass in versions prior to 0.9.114. In `tcp_forwarder.rs`, SSRF protection for `allow_private_network_connections = false` was only applied in the `TcpDestination::HostName(peer)` path. The `TcpDestination::Address(peer) => peer` path proceeded to `TcpStream::connect()` without equivalent checks (for example `is_global_ip`, `is_loopback`), allowing loopback/private targets to be reached by supplying a numeric IP. The vulnerability is fixed in version 0.9.114.	7.1	More Details
CVE-2026-1058	The Form Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via hidden field values in all versions up to, and including, 1.15.35. This is due to insufficient output escaping when displaying hidden field values in the admin submissions list. The plugin uses html_entity_decode() on user-supplied hidden field values without subsequent escaping before output, which converts HTML entity-encoded payloads back into executable JavaScript. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in the admin submissions view that will execute whenever an administrator accesses the submissions list.	7.1	More Details
CVE-2026-25126	PolarLearn is a free and open-source learning program. Prior to version 0-PRERELEASE-15, the vote API route (`POST /api/v1/forum/vote`) trusts the JSON body's `direction` value without runtime validation. TypeScript types are not enforced at runtime, so an attacker can send arbitrary strings (e.g., `"x"`) as `direction`. Downstream (`VoteServer`) treats any non-`"up"` and non-`null` value as a downvote and persists the invalid value in `votes_data`. This can be exploited to bypass intended business logic. Version 0-PRERELEASE-15 fixes the vulnerability.	7.1	More Details
CVE-2020-37081	Fishing Reservation System 7.5 contains multiple remote SQL injection vulnerabilities in admin.php, cart.php, and calendar.php that allow attackers to inject malicious SQL commands. Attackers can exploit vulnerable parameters like uid, pid, type, m, y, and code to compromise the database management system and web application without user interaction.	7.1	More Details
CVE-2025-47366	Cryptographic issue when a Trusted Zone with outdated code is triggered by a HLOS providing incorrect input.	7.1	More Details
CVE-2025-13096	IBM Business Automation Workflow containers V25.0.0 through V25.0.0-IF007, V24.0.1 - V24.0.1-IF007, V24.0.0 - V24.0.0-IF007 and IBM Business Automation Workflow traditional V25.0.0, V24.0.1, V24.0.0 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	7.1	More Details
CVE-2020-	PMB 5.6 contains a SQL injection vulnerability in the administration download script that allows authenticated attackers to execute arbitrary SQL commands through the 'logid' parameter. Attackers can leverage this vulnerability by sending crafted requests to the	7.1	More Details

37105	/admin/sauvegarde/download.php endpoint with manipulated logid values to interact with the database.		
CVE-2020-37112	GUnet OpenEclass 1.7.3 contains multiple SQL injection vulnerabilities that allow authenticated attackers to manipulate database queries through unvalidated parameters. Attackers can exploit the 'month' parameter in the agenda module and other endpoints to extract sensitive database information using error-based or time-based injection techniques.	7.1	More Details
CVE-2025-68479	Discourse is an open source discussion platform. In versions prior to 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0, some subscription endpoints lack proper checking for ownership before making changes. This issue is patched in versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0. No known workarounds are available.	7.1	More Details
CVE-2020-37108	PhpIX 2012 Professional contains a SQL injection vulnerability in the 'id' parameter of product_detail.php that allows remote attackers to manipulate database queries. Attackers can inject malicious SQL code through the 'id' parameter to potentially extract or modify database information.	7.1	More Details
CVE-2026-25503	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, type confusion allowed malformed ICC profiles to trigger undefined behavior when loading invalid icImageEncodingType values causing denial of service. This issue has been patched in version 2.3.1.2.	7.1	More Details
CVE-2020-37005	TimeClock Software 1.01 contains an authenticated time-based SQL injection vulnerability that allows attackers to enumerate valid usernames by manipulating the 'notes' parameter. Attackers can inject conditional time delays in the add_entry.php endpoint to determine user existence by measuring response time differences.	7.1	More Details
CVE-2020-37053	Navigate CMS 2.8.7 contains an authenticated SQL injection vulnerability that allows attackers to leak database information by manipulating the 'sidx' parameter in comments. Attackers can exploit the vulnerability to extract user activation keys by using time-based blind SQL injection techniques, potentially enabling password reset for administrative accounts.	7.1	More Details
CVE-2025-15396	The Library Viewer WordPress plugin before 3.2.0 does not sanitise and escape some parameters before outputting them back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	7.1	More Details
CVE-2026-24051	OpenTelemetry-Go is the Go implementation of OpenTelemetry. The OpenTelemetry Go SDK in version v1.20.0-1.39.0 is vulnerable to Path Hijacking (Untrusted Search Paths) on macOS/Darwin systems. The resource detection code in sdk/resource/host_id.go executes the ioreg system command using a search path. An attacker with the ability to locally modify the PATH environment variable can achieve Arbitrary Code Execution (ACE) within the context of the application. A fix was released with v1.40.0.	7.0	More Details
CVE-2025-13917	WSS Agent, prior to 9.8.5, may be susceptible to a Elevation of Privilege vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	7.0	More Details
CVE-2025-68119	Downloading and building modules with malicious version strings can cause local code execution. On systems with Mercurial (hg) installed, downloading modules from non-standard sources (e.g., custom domains) can cause unexpected code execution due to how external VCS commands are constructed. This issue can also be triggered by providing a malicious version string to the toolchain. On systems with Git installed, downloading and building modules with malicious version strings can allow an attacker to write to arbitrary files on the filesystem. This can only be triggered by explicitly providing the malicious version strings to the toolchain and does not affect usage of @latest or bare module paths.	7.0	More Details
	Discourse is an open source discussion platform. In versions prior to 3.5.4, 2025.11.2,		

CVE-2025-68933	2025.12.1, and 2026.1.0, non-admin moderators with the `moderators_change_post_ownership` setting enabled can change ownership of posts in private messages and restricted categories they cannot access, then export their data to view the content. This is a broken access control vulnerability affecting sites that grant moderators post ownership transfer permissions. This issue is patched in versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0. The patch adds visibility checks for both the topic and posts before allowing ownership transfer. As a workaround, disable the `moderators_change_post_ownership` site setting to prevent non-admin moderators from using the post ownership transfer feature.	6.9	More Details
CVE-2026-25210	In libexpat before 2.7.4, the doContent function does not properly determine the buffer size bufSize because there is no integer overflow check for tag buffer reallocation.	6.9	More Details
CVE-2025-47364	Memory corruption while calculating offset from partition start point.	6.8	More Details
CVE-2025-47363	Memory corruption when calculating oversized partition sizes without proper checks.	6.8	More Details
CVE-2026-24784	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Starting in version 9.0.0 and prior to versions 9.13.10 and 10.2.0, a content editor could inject scripts in module headers/footers that would run for other users. Versions 9.13.10 and 10.2.0 contain a fix for the issue.	6.8	More Details
CVE-2025-36365	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 - 11.5.9 and 12.1.0 - 12.1.3 under specific configuration of cataloged remote storage aliases could allow an authenticated user to execute unauthorized commands due to an authorization bypass vulnerability using a user-controlled key.	6.8	More Details
CVE-2026-23571	A command injection vulnerability was discovered in TeamViewer DEX (former 1E DEX), specifically within the 1E-Nomad-RunPkgStatusRequest instruction. Improper input validation allows authenticated attackers with actioner privilege to run elevated arbitrary commands on connected hosts via malicious commands injected into the instruction’s input field. Users of 1E Client version 24.5 or higher are not affected.	6.8	More Details
CVE-2025-57796	Explorance Blue versions prior to 8.14.12 use reversible symmetric encryption with a hardcoded static key to protect sensitive data, including user passwords and system configurations. This approach allows stored values to be decrypted offline if the encrypted data are obtained.	6.8	More Details
CVE-2026-23794	Reflected XSS in Apache Syncope's Enduser Login page. An attacker that tricks a legitimate user into clicking a malicious link and logging in to Syncope Enduser could steal that user's credentials. This issue affects Apache Syncope: from 3.0 through 3.0.15, from 4.0 through 4.0.3. Users are recommended to upgrade to version 3.0.16 / 4.0.4, which fix this issue.	6.8	More Details
CVE-2026-20410	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10362552; Issue ID: MSV-5760.	6.7	More Details
CVE-2026-20413	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10362725; Issue ID: MSV-5694.	6.7	More Details
CVE-2026-20414	In imgsys, there is a possible escalation of privilege due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10362999; Issue	6.7	More Details

	ID: MSV-5625.		
CVE-2025-13918	Symantec Endpoint Protection, prior to 14.3 RU10 Patch 1, RU9 Patch 2, and RU8 Patch 3, may be susceptible to a Elevation of Privilege vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	6.7	More Details
CVE-2026-25129	PsySH is a runtime developer console, interactive debugger, and REPL for PHP. Prior to versions 0.11.23 and 0.12.19, PsySH automatically loads and executes a `.psysh.php` file from the Current Working Directory (CWD) on startup. If an attacker can write to a directory that a victim later uses as their CWD when launching PsySH, the attacker can trigger arbitrary code execution in the victim's context. When the victim runs PsySH with elevated privileges (e.g., root), this results in local privilege escalation. This is a CWD configuration poisoning issue leading to arbitrary code execution in the victim user's context. If a privileged user (e.g., root, a CI runner, or an ops/debug account) launches PsySH with CWD set to an attacker-writable directory containing a malicious `.psysh.php`, the attacker can execute commands with that privileged user's permissions, resulting in local privilege escalation. Downstream consumers that embed PsySH inherit this risk. For example, Laravel Tinker (`php artisan tinker`) uses PsySH. If a privileged user runs Tinker while their shell is in an attacker-writable directory, the `.psysh.php` auto-load behavior can be abused in the same way to execute attacker-controlled code under the victim's privileges. Versions 0.11.23 and 0.12.19 patch the issue.	6.7	More Details
CVE-2026-1741	A vulnerability was determined in EFM ipTIME A8004T 14.18.2. Affected is the function httpcon_check_session_url of the file /sess-bin/d.cgi of the component Debug Interface. This manipulation of the argument cmd causes backdoor. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.6	More Details
CVE-2025-65887	A division-by-zero vulnerability in the flow.floor_divide() component of OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via a crafted input tensor with zero.	6.5	More Details
CVE-2022-50950	Webile 1.0.1 contains a directory traversal vulnerability that allows remote attackers to manipulate file system paths without authentication. Attackers can exploit path manipulation to access sensitive system directories and potentially compromise the mobile device's local file system.	6.5	More Details
CVE-2022-50980	A unauthenticated adjacent attacker could potentially disrupt operations by switching between multiple configuration presets via CAN.	6.5	More Details
CVE-2022-50979	An unauthenticated adjacent attacker could potentially disrupt operations by switching between multiple configuration presets via Modbus (RS485).	6.5	More Details
CVE-2026-24134	StudioCMS is a server-side-rendered, Astro native, headless content management system. Versions prior to 0.2.0 contain a Broken Object Level Authorization (BOLA) vulnerability in the Content Management feature that allows users with the "Visitor" role to access draft content created by Editor/Admin/Owner users. Version 0.2.0 patches the issue.	6.5	More Details
CVE-2025-12899	A flaw in Zephyr's network stack allows an IPv4 packet containing ICMP type 128 to be misclassified as an ICMPv6 Echo Request. This results in an out-of-bounds memory read and creates a potential information-leak vulnerability in the networking subsystem.	6.5	More Details
CVE-2026-24958	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetElements For Elementor jet-elements allows DOM-Based XSS.This issue affects JetElements For Elementor: from n/a through <= 2.7.12.2.	6.5	More Details

CVE-2025-47402	Transient DOS when processing a received frame with an excessively large authentication information element.	6.5	More Details
CVE-2021-47921	Free Photo & Video Vault 0.0.2 contains a directory traversal web vulnerability that allows remote attackers to manipulate application path requests and access sensitive system files. Attackers can exploit the vulnerability without privileges to retrieve environment variables and access unauthorized system paths.	6.5	More Details
CVE-2025-36366	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could allow a user to cause a denial of service by executing a query that invokes the JSON_Object scalar function, which may trigger an unhandled exception leading to abnormal server termination.	6.5	More Details
CVE-2026-1514	Official Document Management System developed by 2100 Technology has a Incorrect Authorization vulnerability, allowing authenticated remote attackers to modify front-end code to read all official documents.	6.5	More Details
CVE-2026-0683	The SupportCandy – Helpdesk & Customer Support Ticket System plugin for WordPress is vulnerable to SQL Injection via the Number-type custom field filter in all versions up to, and including, 3.4.4. This is due to insufficient escaping on the user-supplied operand value when using the equals operator and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above (customers), to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-36442	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 - 11.5.9 and 12.1.0 - 12.1.3 is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query with XML columns.	6.5	More Details
CVE-2025-36427	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 - 11.5.9 and 12.1.0 - 12.1.3 could allow a local user to cause a denial of service due to improper neutralization of special elements in data query logic.	6.5	More Details
CVE-2025-36424	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 - 11.5.9 and 12.1.0 - 12.1.3 could allow a local user to cause a denial of service due to improper neutralization of special elements in data query logic.	6.5	More Details
CVE-2025-36423	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 12.1.0 - 12.1.3 could allow a local user to cause a denial of service due to improper neutralization of special elements in data query logic.	6.5	More Details
CVE-2025-36407	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 - 11.5.9 and 12.1.0 - 12.1.3 could allow a local user to cause a denial of service due to improper neutralization of special elements in data query logic.	6.5	More Details
CVE-2025-36387	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5.0 - 11.5.9 could allow an authenticated user to cause a denial of service when given specially crafted query.	6.5	More Details
CVE-2026-24670	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, a broken access control vulnerability allows authenticated students to create new course units, an action normally restricted to higher-privileged roles. This issue has been patched in version 4.2.	6.5	More Details
CVE-2025-2668	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 - 11.5.9 is vulnerable to a denial of service as the server may crash when an authenticated user creates a specially crafted query.	6.5	More Details
CVE-2025-36098	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 - 11.5.9 and 12.1.0 - 12.1.3 could allow an authenticated user to cause a denial of service due to improper allocation of resources.	6.5	More Details

CVE-2025-36070	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 - 11.5.9 and 12.1.0 - 12.1.3 is vulnerable to a denial of service as a trap may occur when selecting from certain types of tables.	6.5	More Details
CVE-2026-24668	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, a broken access control vulnerability allows authenticated students to add content to existing course units, an action normally restricted to higher-privileged roles. This issue has been patched in version 4.2.	6.5	More Details
CVE-2026-24666	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, a Cross-Site Request Forgery (CSRF) vulnerability in multiple teacher-restricted endpoints allows attackers to induce authenticated teachers to perform unintended actions, such as modifying assignment grades, via crafted requests. This issue has been patched in version 4.2.	6.5	More Details
CVE-2020-37115	GUnet OpenEclass 1.7.3 stores user credentials in plaintext, allowing administrators to view all registered users' usernames and passwords without encryption. This vulnerability exposes sensitive information and increases the risk of credential theft and unauthorized access.	6.5	More Details
CVE-2026-24957	Missing Authorization vulnerability in WP Chill Strong Testimonials strong-testimonials allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Strong Testimonials: from n/a through <= 3.2.20.	6.5	More Details
CVE-2025-36009	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5.0 - 11.5.9 and 12.1.0 - 12.1.3 could allow an unauthenticated user to cause a denial of service due to excessive use of a global variable.	6.5	More Details
CVE-2025-36001	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 - 11.5.9 and 12.1.0 - 12.1.3 could allow an authenticated user to cause a denial of service using a specially crafted SQL statement including XML that performs uncontrolled recursion.	6.5	More Details
CVE-2026-24952	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Craig Hewitt Seriously Simple Podcasting seriously-simple-podcasting allows Stored XSS.This issue affects Seriously Simple Podcasting: from n/a through <= 3.14.1.	6.5	More Details
CVE-2026-24514	A security issue was discovered in ingress-nginx where the validating admission controller feature is subject to a denial of service condition. By sending large requests to the validating admission controller, an attacker can cause memory consumption, which may result in the ingress-nginx controller pod being killed or the node running out of memory.	6.5	More Details
CVE-2026-24888	Maker.js is a 2D vector line drawing and shape modeling for CNC and laser cutters. In versions up to and including 0.19.1, the `makerjs.extendObject` function copies properties from source objects without proper validation, potentially exposing applications to security risks. The function lacks `hasOwnProperty()` checks and does not filter dangerous keys, allowing inherited properties and potentially malicious properties to be copied to target objects. A patch is available in commit 85e0f12bd868974b891601a141974f929dec36b8, which is expected to be part of version 0.19.2.	6.5	More Details
CVE-2020-36968	M/Monit 3.7.4 contains an authentication vulnerability that allows authenticated attackers to retrieve user password hashes through an administrative API endpoint. Attackers can send requests to the /api/1/admin/users/list and /api/1/admin/users/get endpoints to extract MD5 password hashes for all users.	6.5	More Details
CVE-2025-69601	A directory traversal (Zip Slip) vulnerability exists in the “Static Sites” feature of 66biolinks v44.0.0 by AltumCode. Uploaded ZIP archives are automatically extracted without validating or sanitizing file paths. An attacker can include traversal sequences (e.g., ../) in ZIP entries to write files outside the intended extraction directory. This allows static files (html, js, css, images) file write to unintended locations, or overwriting existing HTML files, potentially leading to content defacement and, in certain deployments,	6.5	More Details

	further impact if sensitive files are overwritten.		
CVE-2026-24845	malcontent discovers supply-chain compromises through. context, differential analysis, and YARA. Starting in version 0.10.0 and prior to version 1.20.3, malcontent could be made to expose Docker registry credentials if it scanned a specially crafted OCI image reference. malcontent uses google/go-containerregistry for OCI image pulls, which by default uses the Docker credential keychain. A malicious registry could return a `WWW-Authenticate` header redirecting token authentication to an attacker-controlled endpoint, causing credentials to be sent to that endpoint. Version 1.20.3 fixes the issue by defaulting to anonymous auth for OCI pulls.	6.5	More Details
CVE-2025-69218	Discourse is an open source discussion platform. In versions prior to 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0, moderators can access the `top_uploads` admin report which should be restricted to admins only. This report displays direct URLs to all uploaded files on the site, including sensitive content such as user data exports, admin backups, and other private attachments that moderators should not have access to. This issue is patched in versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0. There is no workaround. Limit moderator privileges to trusted users until the patch is applied.	6.5	More Details
CVE-2025-71006	A floating point exception (FPE) in the oneflow.reshape component of OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via a crafted input.	6.5	More Details
CVE-2026-23570	A missing validation of a user-controlled value in the TeamViewer DEX Client (former 1E Client) - Content Distribution Service (NomadBranch.exe) prior version 26.1 for Windows allows an adjacent network attacker to tamper with log timestamps via crafted UDP Sync command. This could result in forged or nonsensical datetime prefixes and compromising log integrity and forensic correlation.	6.5	More Details
CVE-2026-23569	An out-of-bounds read vulnerability in the TeamViewer DEX Client (former 1E Client) - Content Distribution Service (NomadBranch.exe) prior version 26.1 for Windows allows a remote attacker to leak stack memory and cause a denial of service via a crafted request. The leaked stack memory could be used to bypass ASLR remotely and facilitate exploitation of other vulnerabilities on the affected system.	6.5	More Details
CVE-2025-68934	Discourse is an open source discussion platform. In versions prior to 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0, authenticated users can submit crafted payloads to /drafts.json that cause O(n^2) processing in Base62.decode, tying up workers for 35-60 seconds per request. This affects all users as the shared worker pool becomes exhausted. This issue is patched in versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0. Lowering the max_draft_length site setting reduces attack surface but does not fully mitigate the issue, as payloads under the limit can still trigger the slow code path.	6.5	More Details
CVE-2025-71002	A floating-point exception (FPE) in the flow.column_stack component of OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via a crafted input.	6.5	More Details
CVE-2020-36973	PDW File Browser 1.3 contains a remote code execution vulnerability that allows authenticated users to upload and rename webshell files to arbitrary web server locations. Attackers can upload a .txt webshell, rename it to .php, and move it to accessible directories using double-encoded path traversal techniques.	6.5	More Details
CVE-2025-71005	A floating point exception (FPE) in the oneflow.view component of OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via a crafted input.	6.5	More Details
CVE-2025-68666	Discourse is an open source discussion platform. In versions prior to 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0, users archives are viewable by users with moderation privileges even though moderators should not have access to the archives. Private topic/post content made by the users are leaked through the archives leading to a breach of confidentiality. This issue is patched in versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0. To work around this problem, a site admin can temporarily revoke the	6.5	More Details

	moderation role from all moderators until the Discourse instance has been upgraded to a version that has been patched.		
CVE-2020-37077	Booked Scheduler 2.7.7 contains a directory traversal vulnerability in the manage_email_templates.php script that allows authenticated administrators to access unauthorized files. Attackers can exploit the vulnerable 'tn' parameter to read files outside the intended directory by manipulating directory path traversal techniques.	6.5	More Details
CVE-2026-24742	Discourse is an open source discussion platform. In versions prior to 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0, non-admin moderators can view sensitive information in staff action logs that should be restricted to administrators only. The exposed information includes webhook payload URLs and secrets, API key details, site setting changes, private message content, restricted category names and structures, and private chat channel titles. This allows moderators to bypass intended access controls and extract confidential data by monitoring the staff action logs. With leaked webhook secrets, an attacker could potentially spoof webhook events to integrated services. This issue is patched in versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0. As a workaround, site administrators should review and limit moderator appointments to fully trusted users. There is no configuration-based workaround to prevent this access.	6.5	More Details
CVE-2025-61728	archive/zip uses a super-linear file name indexing algorithm that is invoked the first time a file in an archive is opened. This can lead to a denial of service when consuming a maliciously constructed ZIP archive.	6.5	More Details
CVE-2026-21865	Discourse is an open source discussion platform. In versions prior to 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0, moderators can convert some personal messages to public topics when they shouldn't have access. This issue is patched in versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0. As a workaround, site admin can temporarily revoke the moderation role from untrusted moderators or remove the moderator group from the "personal message enabled groups" site setting until the Discourse instance has been upgraded to a version that has been patched.	6.5	More Details
CVE-2026-23567	An integer underflow in the UDP command handler of the TeamViewer DEX Client (former 1E Client) - Content Distribution Service (NomadBranch.exe) prior version 26.1 for Windows allows an adjacent network attacker to trigger a heap-based buffer overflow and cause a denial-of-service (service crash) via specially crafted UDP packets.	6.5	More Details
CVE-2026-23565	A vulnerability in TeamViewer DEX Client (former 1E Client) - Content Distribution Service (NomadBranch.exe) prior version 26.1 for Windows allows an attacker on the adjacent network to cause the NomadBranch.exe process to terminate via crafted requests. This can result in a denial-of-service condition of the Content Distribution Service.	6.5	More Details
CVE-2026-23564	A vulnerability in TeamViewer DEX Client (former 1E Client) - Content Distribution Service (NomadBranch.exe) prior version 26.1 for Windows allows an attacker on the adjacent network to cause normally encrypted UDP traffic to be sent in cleartext. This can result in disclosure of sensitive information.	6.5	More Details
CVE-2025-71004	A segmentation violation in the oneflow.logical_or component of OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via a crafted input.	6.5	More Details
CVE-2026-23566	A vulnerability in TeamViewer DEX Client (former 1E Client) - Content Distribution Service (NomadBranch.exe) prior version 26.1 for Windows allows an attacker on the adjacent network to inject, tamper with, or forge log entries in \Nomad Branch.log via crafted data sent to the UDP network handler. This can impact log integrity and nonrepudiation.	6.5	More Details
CVE-2025-71001	A segmentation violation in the flow.column_stack component of OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via a crafted input.	6.5	More Details
	The Simple Folio plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_simple_folio_item_client_name' and '_simple_folio_item_link' meta fields in all versions		

CVE-2025-14039	up to, and including, 1.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12709	The Interactions – Create Interactive Experiences in the Block Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via event selectors in all versions up to, and including, 1.3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14283	The BlockArt Blocks – Gutenberg Blocks, Page Builder Blocks ,WordPress Block Plugin, Sections & Template Library plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the BlockArt Counter in all versions up to, and including, 2.2.14 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-54343	QWE DL 2.0.1 mobile web application contains a persistent input validation vulnerability allowing remote attackers to inject malicious script code through path parameter manipulation. Attackers can exploit the vulnerability to execute persistent cross-site scripting attacks, potentially leading to session hijacking and application module manipulation.	6.4	More Details
CVE-2022-50952	Banco Guayaquil 8.0.0 mobile iOS application contains a persistent cross-site scripting vulnerability in the TextBox Name Profile input. Attackers can inject malicious script code through a POST request that executes on application review without user interaction.	6.4	More Details
CVE-2022-50941	BootCommerce 3.2.1 contains persistent input validation vulnerabilities that allow remote attackers to inject malicious script code through guest order checkout input fields. Attackers can exploit unvalidated input parameters to execute arbitrary scripts, potentially leading to session hijacking, phishing attacks, and application module manipulation.	6.4	More Details
CVE-2022-50951	WiFi File Transfer 1.0.8 contains a persistent cross-site scripting vulnerability that allows remote attackers to inject malicious script codes through file and folder names. Attackers can exploit the web server's input validation weakness to execute arbitrary JavaScript when users preview infected file paths, potentially compromising user browser sessions.	6.4	More Details
CVE-2021-47885	Multiple payment terminal versions contain non-persistent cross-site scripting vulnerabilities in billing and payment information input fields. Attackers can inject malicious script code through vulnerable parameters to manipulate client-side requests and potentially execute session hijacking or phishing attacks.	6.4	More Details
CVE-2022-50940	Knap Advanced PHP Login 3.1.3 contains a persistent cross-site scripting vulnerability that allows remote attackers to inject malicious script code in the name parameter. Attackers can exploit the vulnerability to execute arbitrary scripts in users and activity log backend modules, potentially leading to session hijacking and persistent phishing attacks.	6.4	More Details
CVE-2022-50797	Stripe Green Downloads Wordpress Plugin 2.03 contains a persistent cross-site scripting vulnerability allowing remote attackers to inject malicious scripts in button label fields. Attackers can exploit input parameters to execute arbitrary scripts, potentially leading to session hijacking and application module manipulation.	6.4	More Details
CVE-2025-14865	The Passster – Password Protect Pages and Content plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'content_protector' shortcode in all versions up to, and including, 4.2.24. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will	6.4	More Details

	execute whenever a user accesses an injected page. The vulnerability was partially patched in version 4.2.21.		
CVE-2021-47919	Simple CMS 2.1 contains a non-persistent cross-site scripting vulnerability in the preview.php file's id parameter. Attackers can inject malicious script code through a GET request to execute arbitrary scripts and potentially hijack user sessions or perform phishing attacks.	6.4	More Details
CVE-2021-47917	Simple CMS 2.1 contains a persistent cross-site scripting vulnerability in user input parameters that allows remote attackers to inject malicious script code. Attackers can exploit the newUser and editUser modules to inject persistent scripts that execute on user list preview, potentially leading to session hijacking and application manipulation.	6.4	More Details
CVE-2019-25264	Snipe-IT 4.7.5 contains a persistent cross-site scripting vulnerability that allows authorized users to upload malicious SVG files with embedded JavaScript. Attackers can craft SVG files with script tags to execute arbitrary JavaScript when the accessory is viewed by other users.	6.4	More Details
CVE-2021-47914	PHP Melody version 3.0 contains a persistent cross-site scripting vulnerability in the edit-video.php submitted parameter that allows remote attackers to inject malicious script code. Attackers can exploit this vulnerability to execute arbitrary JavaScript, potentially leading to session hijacking, persistent phishing, and manipulation of application modules.	6.4	More Details
CVE-2021-47913	PHP Melody 3.0 contains a persistent cross-site scripting vulnerability in the video editor that allows privileged users to inject malicious scripts. Attackers can exploit the WYSIWYG editor to execute persistent scripts, potentially leading to session hijacking and application manipulation.	6.4	More Details
CVE-2021-47912	PHP Melody version 3.0 contains multiple non-persistent cross-site scripting vulnerabilities in categories, import, and user import files. Attackers can inject malicious scripts through unvalidated parameters to execute client-side attacks and potentially hijack user sessions.	6.4	More Details
CVE-2021-47908	Ultimate POS 4.4 contains a persistent cross-site scripting vulnerability in the product name parameter that allows remote attackers to inject malicious scripts. Attackers can exploit the vulnerability through product add or edit functions to execute arbitrary JavaScript and potentially hijack user sessions.	6.4	More Details
CVE-2025-36436	IBM Cloud Pak for Business Automation 25.0.0 through 25.0.0 Interim Fix 002, 24.0.1 through 24.0.1 Interim Fix 005, and 24.0.0 through 24.0.0 Interim Fix 007 is vulnerable to stored cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.4	More Details
CVE-2021-47856	Easy Cart Shopping Cart 2021 contains a non-persistent cross-site scripting vulnerability in the search module's keyword parameter. Remote attackers can inject malicious script code through the search input to compromise user sessions and manipulate application content.	6.4	More Details
CVE-2025-8072	The Target Video Easy Publish plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘placeholder_img’ parameter in all versions up to, and including, 3.8.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2020-37018	GOautodial 4.0 contains a persistent cross-site scripting vulnerability that allows authenticated agents to inject malicious scripts through message subjects. Attackers can craft messages with embedded JavaScript that will execute when an administrator reads the message, potentially stealing session cookies or executing client-side attacks.	6.4	More Details
CVE-	Zendesk SweetHawk Survey 1.6 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts through support ticket submissions.		More

2019-25263	Attackers can insert XSS payloads like script tags into ticket text that automatically execute when survey pages are loaded by other users.	6.4	Details
CVE-2026-1755	The Menu Icons by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_wp_attachment_image_alt' post meta in all versions up to, and including, 0.13.20 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1210	The Happy Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_elementor_data' meta field in all versions up to, and including, 3.20.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2020-37103	DotNetNuke 9.5 contains a persistent cross-site scripting vulnerability that allows normal users to upload malicious XML files with executable scripts through journal tools. Attackers can upload XML files with XHTML namespace scripts to execute arbitrary JavaScript in users' browsers, potentially bypassing CSRF protections and performing more damaging attacks.	6.4	More Details
CVE-2026-1244	The Forms Bridge – Infinite integrations plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' shortcode attribute in the 'financoop_campaign' shortcode in all versions up to, and including, 4.2.5. This is due to insufficient input sanitization and output escaping on the user-supplied 'id' parameter in the forms_bridge_financoop_shortcode_error function. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9082	The WPBITS Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widget parameters in versions up to, and including, 1.8 due to insufficient input sanitization and output escaping when dynamic content is enabled. This makes it possible for authenticated attackers with contributor-level permissions and above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2020-37022	OpenZ ERP 3.6.60 contains a persistent cross-site scripting vulnerability in the Employee module's name and description parameters. Attackers can inject malicious scripts through POST requests to , enabling session hijacking and manipulation of application modules.	6.4	More Details
CVE-2020-37019	Orchard Core RC1 contains a persistent cross-site scripting vulnerability that allows remote attackers to inject malicious scripts through blog post creation. Attackers can create blog posts with embedded JavaScript in the MarkdownBodyPart.Source parameter to execute arbitrary scripts in victim browsers.	6.4	More Details
CVE-2026-1295	The Buy Now Plus – Buy Now buttons for Stripe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'buynowplus' shortcode in all versions up to, and including, 1.0.2 due to insufficient input sanitization and output escaping on shortcode attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2019-25265	Online Inventory Manager 3.2 contains a stored cross-site scripting vulnerability in the group description field of the admin edit groups section. Attackers can inject malicious JavaScript through the description field that will execute when the groups page is viewed, allowing potential cookie theft and client-side script execution.	6.4	More Details
CVE-2020-	Dolibarr 11.0.3 contains a persistent cross-site scripting vulnerability in LDAP synchronization settings that allows attackers to inject malicious scripts through multiple parameters. Attackers can exploit the host, slave, and port parameters in	6.4	More

36966	/dolibarr/admin/ldap.php to execute arbitrary JavaScript and potentially steal user cookie information.		Details
CVE-2020-36996	PHPFusion 9.03.50 contains a persistent cross-site scripting vulnerability in the print.php page that fails to properly sanitize user-submitted message content. Attackers can inject malicious JavaScript through forum messages that will execute when the print page is generated, allowing script execution in victim browsers.	6.4	More Details
CVE-2020-37014	Tryton 5.4 contains a persistent cross-site scripting vulnerability in the user profile name input that allows remote attackers to inject malicious scripts. Attackers can exploit the vulnerability by inserting script payloads in the name field, which execute in the frontend and backend user interfaces.	6.4	More Details
CVE-2020-37003	Sellacious eCommerce 4.6 contains a persistent cross-site scripting vulnerability in the Manage Your Addresses module that allows attackers to inject malicious scripts. Attackers can exploit multiple address input fields like full name, company, and address to execute persistent script code that can hijack user sessions and manipulate application modules.	6.4	More Details
CVE-2020-36998	Forma.lms The E-Learning Suite 2.3.0.2 contains a persistent cross-site scripting vulnerability in multiple course and profile parameters. Attackers can inject malicious scripts in course code, name, description fields, and email parameter to execute arbitrary JavaScript without proper input sanitization.	6.4	More Details
CVE-2026-24775	OpenProject is an open-source, web-based project management software. In the new editor for collaborative documents based on BlockNote, OpenProject maintainers added a custom extension in OpenProject version 17.0.0 that allows to mention OpenProject work packages in the document. To show work package details, the editor loads details about the work package via the OpenProject API. For this API call, the extension to the BlockNote editor did not properly validate the given work package ID to be only a number. This allowed an attacker to generate a document with relative links that upon opening could make arbitrary `GET` requests to any URL within the OpenProject instance. This issue was patched in version version 0.0.22 of op-blocknote-extensions, which was shipped with OpenProject 17.0.2. If users cannot update immediately to version 17.0.2 of OpenProject, administrators can disable collaborative document editing in Settings -> Documents -> Real time collaboration -> Disable.	6.3	More Details
CVE-2026-1546	A security vulnerability has been detected in jishenghua jshERP up to 3.6. The impacted element is the function getBillItemByParam of the file /jshERP-boot/depotItem/importItemExcel of the component com.jsh.erp.datasource.mappers.DepotItemMapperEx. The manipulation of the argument barCodes leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2025-15344	Tanium addressed a SQL injection vulnerability in Asset.	6.3	More Details
CVE-2026-1601	A weakness has been identified in Totolink A7000R 4.1cu.4154. The impacted element is the function setUploadUserData of the file /cgi-bin/cstecgi.cgi. Executing a manipulation of the argument FileName can lead to command injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-1810	A vulnerability was detected in bolo-blog bolo-solo up to 2.6.4. The impacted element is the function unpackFilteredZip of the file src/main/java/org/b3log/solo/bolo/prop/BackupService.java of the component ZIP File Handler. Performing a manipulation of the argument File results in path traversal. The attack is possible to be carried out 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 responded yet.	6.3	More Details

CVE-2026-1544	A security flaw has been discovered in D-Link DIR-823X 250416. Impacted is the function sub_41E2A0 of the file /goform/set_mode. Performing a manipulation of the argument lan_gateway results in os command injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-1551	A weakness has been identified in itsourcecode School Management System 1.0. This affects an unknown part of the file /ramonsys/course/controller.php. Executing a manipulation of the argument ID can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-1811	A flaw has been found in bolo-blog bolo-solo up to 2.6.4. This affects the function importFromMarkdown of the file src/main/java/org/b3log/solo/bolo/prop/BackupService.java of the component Filename Handler. Executing a manipulation of the argument File can lead to path traversal. The attack may be performed from remote. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-1592	Foxit PDF Editor Cloud (pdfonline) contains a stored cross-site scripting vulnerability in the Create New Layer feature. Unsanitized user input is embedded into the HTML output, allowing arbitrary JavaScript execution when the layer is referenced. This issue affects pdfonline.foxit.com: before 2026-02-03.	6.3	More Details
CVE-2026-1746	A vulnerability was identified in JeecgBoot 3.9.0. This vulnerability affects unknown code of the file /JeecgBoot/sys/api/loadDictItemByKeyword of the component Online Report API. Such manipulation of the argument keyword leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-1547	A vulnerability was detected in Totolink A7000R 4.1cu.4154. This affects the function setUnloadUserData of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument plugin_name results in command injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-1638	A security flaw has been discovered in Tenda AC21 1.1.1.1/1.dmzip/16.03.08.16. The impacted element is the function mDMZSetCfg of the file /goform/mDMZSetCfg. The manipulation of the argument dmzIp results in command injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-1625	A vulnerability was detected in D-Link DWR-M961 1.1.47. The impacted element is the function sub_4250E0 of the file /boafrm/formSmsManage of the component SMS Message. Performing a manipulation of the argument action_value results in command injection. The attack may be initiated remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-1597	A vulnerability has been found in Bdtask SalesERP up to 20260116. This issue affects some unknown processing of the component Administrative Endpoint. Such manipulation of the argument ci_session leads to improper authorization. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-1596	A flaw has been found in D-Link DWR-M961 1.1.47. This vulnerability affects the function sub_419920 of the file /boafrm/formLtefotaUpgradeQuectel. This manipulation of the argument fota_url causes command injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	6.3	More Details
CVE-	A security flaw has been discovered in PHPGurukul Hospital Management System 1.0. Affected by this issue is some unknown functionality of the file /hms/hospital/docappsystem/adminviews.py of the component Admin Dashboard Page.		More

2026-1550	Performing a manipulation results in improper authorization. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	6.3	Details
CVE-2026-24739	Symfony is a PHP framework for web and console applications and a set of reusable PHP components. Prior to versions 5.4.51, 6.4.33, 7.3.11, 7.4.5, and 8.0.5, the Symfony Process component did not correctly treat some characters (notably `=`) as “special” when escaping arguments on Windows. When PHP is executed from an MSYS2-based environment (e.g. Git Bash) and Symfony Process spawns native Windows executables, MSYS2’s argument/path conversion can mis-handle unquoted arguments containing these characters. This can cause the spawned process to receive corrupted/truncated arguments compared to what Symfony intended. If an application (or tooling such as Composer scripts) uses Symfony Process to invoke file-management commands (e.g. `rmdir`, `del`, etc.) with a path argument containing `=`, the MSYS2 conversion layer may alter the argument at runtime. In affected setups this can result in operations being performed on an unintended path, up to and including deletion of the contents of a broader directory or drive. The issue is particularly relevant when untrusted input can influence process arguments (directly or indirectly, e.g. via repository paths, extracted archive paths, temporary directories, or user-controlled configuration). Versions 5.4.51, 6.4.33, 7.3.11, 7.4.5, and 8.0.5 contains a patch for the issue. Some workarounds are available. Avoid running PHP/one's own tooling from MSYS2-based shells on Windows; prefer cmd.exe or PowerShell for workflows that spawn native executables. Avoid passing paths containing `=` (and similar MSYS2-sensitive characters) to Symfony Process when operating under Git Bash/MSYS2. Where applicable, configure MSYS2 to disable or restrict argument conversion (e.g. via `MSYS2_ARG_CONV_EXCL`), understanding this may affect other tooling behavior.	6.3	More Details
CVE-2026-1548	A flaw has been found in Totolink A7000R 4.1cu.4154. This impacts the function CloudACMunualUpdateUserdata of the file /cgi-bin/cstecgi.cgi. This manipulation of the argument url causes command injection. The attack can be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-1812	A vulnerability has been found in bolo-blog bolo-solo up to 2.6.4. This impacts the function importFromCnblogs of the file src/main/java/org/b3log/solo/bolo/prop/BackupService.java of the component Filename Handler. The manipulation of the argument File leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-1702	A vulnerability was detected in SourceCodester Pet Grooming Management Software 1.0. Impacted is an unknown function of the file /admin/operation/user.php of the component User Management. Performing a manipulation of the argument group_id results in improper authorization. The attack can be initiated remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-1623	A weakness has been identified in Totolink A7000R 4.1cu.4154. Impacted is the function setUpgradeFW of the file /cgi-bin/cstecgi.cgi. This manipulation of the argument FileName causes command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-1691	A vulnerability has been found in bolo-solo up to 2.6.4. This impacts the function importMarkdownsSync of the file src/main/java/org/b3log/solo/bolo/prop/BackupService.java of the component SnakeYAML. Such manipulation leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-1552	A security vulnerability has been detected in SEMCMS 5.0. This vulnerability affects unknown code of the file /SEMCMS_Info.php. The manipulation of the argument searchml leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this	6.3	More Details

	disclosure but did not respond in any way.		
CVE-2026-1624	A security vulnerability has been detected in D-Link DWR-M961 1.1.47. The affected element is an unknown function of the file /boafrm/formLtefotaUpgradeFibocom. Such manipulation of the argument fota_url leads to command injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-1591	Foxit PDF Editor Cloud (pdfonline) contains a stored cross-site scripting vulnerability in the file upload feature. A malicious username is embedded into the upload file list without proper escaping, allowing arbitrary JavaScript execution when the list is displayed. This issue affects pdfonline.foxit.com: before 2026-02-03.	6.3	More Details
CVE-2025-71008	A segmentation violation in the oneflow._oneflow_internal.autograd.Function.FunctionCtx.mark_non_differentiable component of OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via a crafted input.	6.2	More Details
CVE-2026-1757	A flaw was identified in the interactive shell of the xmllint utility, part of the libxml2 project, where memory allocated for user input is not properly released under certain conditions. When a user submits input consisting only of whitespace, the program skips command execution but fails to free the allocated buffer. Repeating this action causes memory to continuously accumulate. Over time, this can exhaust system memory and terminate the xmllint process, creating a denial-of-service condition on the local system.	6.2	More Details
CVE-2025-71009	An input validation vulnerability in the flow.scatter/flow.scatter_add component of OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via a crafted indices.	6.2	More Details
CVE-2020-37086	Easy Transfer 1.7 iOS mobile application contains a directory traversal vulnerability that allows remote attackers to access unauthorized file system paths without authentication. Attackers can exploit the vulnerability by manipulating path parameters in GET and POST requests to list or download sensitive system files and inject malicious scripts into application parameters.	6.2	More Details
CVE-2025-71011	An input validation vulnerability in the flow.Tensor.new_empty/flow.Tensor.new_ones/flow.Tensor.new_zeros component of OneFlow v0.9.0 allows attackers to cause a Denial of Service (DoS) via a crafted input.	6.2	More Details
CVE-2025-36353	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 - 11.5.9 and 12.1.0 - 12.1.3 could allow a local user to cause a denial of service due to improper neutralization of special elements in data query logic.	6.2	More Details
CVE-2025-62349	Salt contains an authentication protocol version downgrade weakness that can allow a malicious minion to bypass newer authentication/security features by using an older request payload format, enabling minion impersonation and circumventing protections introduced in response to prior issues.	6.2	More Details
CVE-2020-36994	QlikView 12.50.20000.0 contains a denial of service vulnerability in the FTP server address input field that allows local attackers to crash the application. Attackers can paste a 300-character buffer into the FTP server address field to trigger an application crash and prevent normal functionality.	6.2	More Details
CVE-2025-36123	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5.0 - 11.5.9 and 12.1.0 - 12.1.3 could allow a local user to cause a denial of service when copying large table containing XML data due to improper allocation of system resources.	6.2	More Details
CVE-2026-24671	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, a Stored Cross-Site Scripting (XSS) vulnerability allows authenticated high-privileged users (teachers or administrators) to inject malicious JavaScript into multiple user-controllable input fields across the application, which is executed when other users access affected pages. This issue has been patched in version 4.2.	6.1	More Details

CVE-2026-1513	billboard.js before 3.18.0 allows an attacker to execute malicious JavaScript due to improper sanitization during chart option binding.	6.1	More Details
CVE-2025-67851	A flaw was found in moodle. This formula injection vulnerability occurs when data fields are exported without proper escaping. A remote attacker could exploit this by providing malicious data that, when exported and opened in a spreadsheet, allows arbitrary formulas to execute. This can lead to compromised data integrity and unintended operations within the spreadsheet.	6.1	More Details
CVE-2026-24852	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, a heap buffer over-read when the strlen() function attempts to read a non-null-terminated buffer potentially leaking heap memory contents and causing application termination. This vulnerability affects users of the iccDEV library who process ICC color profiles. ICC Profile Injection vulnerabilities arise when user-controllable input is incorporated into ICC profile data or other structured binary blobs in an unsafe manner. Version 2.3.1.2 contains a fix for the issue. No known workarounds are available.	6.1	More Details
CVE-2025-13984	Permissive Cross-domain Security Policy with Untrusted Domains vulnerability in Drupal Next.Js allows Cross-Site Scripting (XSS).This issue affects Next.Js: from 0.0.0 before 1.6.4, from 2.0.0 before 2.0.1.	6.1	More Details
CVE-2026-1466	Jirafeau normally prevents browser preview for text files due to the possibility that for example SVG and HTML documents could be exploited for cross site scripting. This was done by storing the MIME type of a file and allowing only browser preview for MIME types beginning with image (except for image/svg+xml, see CVE-2022-30110, CVE-2024-12326 and CVE-2025-7066), video and audio. However, it was possible to bypass this check by sending a manipulated HTTP request with an invalid MIME type like image. When doing the preview, the browser tries to automatically detect the MIME type resulting in detecting SVG and possibly executing JavaScript code. To prevent this, MIME sniffing is disabled by sending the HTTP header X-Content-Type-Options: nosniff.	6.1	More Details
CVE-2026-25154	LocalSend is a free, open-source app that allows users to share files and messages with nearby devices over their local network without needing an internet connection. In versions up to and including 1.17.0, when a user initiates a "Share via Link" session, the LocalSend application starts a local HTTP server to host the selected files. The client-side logic for this web interface is contained in `app/assets/web/main.js`. Note that at [0], the `handleFilesDisplay` function constructs the HTML for the file list by iterating over the files received from the server. Commit 8f3cec85aa29b2b13fed9b2f8e499e1ac9b0504c contains a patch.	6.1	More Details
CVE-2025-69749	Cross Site Scripting vulnerability in tale v.2.0.5 allows an attacker to execute arbitrary code.	6.1	More Details
CVE-2025-70958	Multiple reflected cross-site scripting (XSS) vulnerabilities in the installation module of Subrion CMS v4.2.1 allows attackers to execute arbitrary Javascript in the context of the user's browser via injecting a crafted payload into the dbuser, dbpwd, and dbname parameters.	6.1	More Details
CVE-2020-37111	60CycleCMS 2.5.2 contains a cross-site scripting (XSS) vulnerability in news.php that allows attackers to inject malicious scripts through GET parameters. Attackers can craft malicious URLs with XSS payloads targeting the 'etsu' and 'ltsu' parameters to execute arbitrary scripts in victim's browsers. This issue does not involve SQL injection.	6.1	More Details
CVE-2025-14063	The SEO Links Interlinking plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'google_error' parameter in all versions up to, and including, 1.7.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE-2025-36238	IBM PowerVM Hypervisor FW1110.00 through FW1110.03, FW1060.00 through FW1060.51, and FW950.00 through FW950.F0 could allow a local user with administration privileges to obtain sensitive information from a Virtual TPM through a series of PowerVM service procedures.	6.0	More Details
CVE-2026-24938	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ajay Better Search better-search allows Stored XSS.This issue affects Better Search: from n/a through <= 4.2.1.	5.9	More Details
CVE-2026-25155	Qwik is a performance focused javascript framework. Prior to version 1.12.0, a typo in the regular expression within isContentType causes incorrect parsing of certain Content-Type headers. This issue has been patched in version 1.12.0.	5.9	More Details
CVE-2026-25151	Qwik is a performance focused javascript framework. Prior to version 1.19.0, Qwik City's server-side request handler inconsistently interprets HTTP request headers, which can be abused by a remote attacker to circumvent form submission CSRF protections using specially crafted or multi-valued Content-Type headers. This issue has been patched in version 1.19.0.	5.9	More Details
CVE-2026-1778	Amazon SageMaker Python SDK before v3.1.1 or v2.256.0 disables TLS certificate verification for HTTPS connections made by the service when a Triton Python model is imported, incorrectly allowing for requests with invalid and self-signed certificates to succeed.	5.9	More Details
CVE-2025-36253	IBM Concert 1.0.0 through 2.1.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	5.9	More Details
CVE-2026-1539	A flaw was found in the libsoup HTTP library that can cause proxy authentication credentials to be sent to unintended destinations. When handling HTTP redirects, libsoup removes the Authorization header but does not remove the Proxy-Authorization header if the request is redirected to a different host. As a result, sensitive proxy credentials may be leaked to third-party servers. Applications using libsoup for HTTP communication may unintentionally expose proxy authentication data.	5.8	More Details
CVE-2026-1536	A flaw was found in libsoup. An attacker who can control the input for the Content-Disposition header can inject CRLF (Carriage Return Line Feed) sequences into the header value. These sequences are then interpreted verbatim when the HTTP request or response is constructed, allowing arbitrary HTTP headers to be injected. This vulnerability can lead to HTTP header injection or HTTP response splitting without requiring authentication or user interaction.	5.8	More Details
CVE-2025-7014	Session Fixation vulnerability in QR Menu Pro Smart Menu Systems Menu Panel allows Session Hijacking.This issue affects Menu Panel: through 29012026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.7	More Details
CVE-2025-7013	Authorization Bypass Through User-Controlled Key vulnerability in QR Menu Pro Smart Menu Systems Menu Panel allows Exploitation of Trusted Identifiers.This issue affects Menu Panel: through 29012026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.7	More Details
CVE-2026-23563	Improper Link Resolution Before File Access (invoked by 1E-Explorer-TachyonCore-DeleteFileByPath instruction) in TeamViewer DEX - 1E Client before version 26.1 on Windows allows a low-privileged local attacker to delete protected system files via a crafted RPC control junction or symlink that is followed when the delete instruction executes.	5.7	More Details
CVE-2025-7015	Session Fixation vulnerability in Akın Software Computer Import Export Industry and Trade Ltd. QR Menu allows Session Fixation.This issue affects QR Menu: before s1.05.12.	5.7	More Details
CVE-	The issue was addressed with improved bounds checks. This issue is fixed in macOS		More

2025-46306	Tahoe 26, Keynote 15.1, iOS 26 and iPadOS 26. Processing a maliciously crafted Keynote file may disclose memory contents.	5.5	Details
CVE-2026-24846	malcontent discovers supply-chain compromises through. context, differential analysis, and YARA. Starting in version 1.8.0 and prior to version 1.20.3, malcontent could be made to create symlinks outside the intended extraction directory when scanning a specially crafted tar or deb archive. The `handleSymlink` function received arguments in the wrong order, causing the symlink target to be used as the symlink location. Additionally, symlink targets were not validated to ensure they resolved within the extraction directory. Version 1.20.3 introduces fixes that swap handleSymlink arguments, validate symlink location, and validate symlink targets that resolve within an extraction directory.	5.5	More Details
CVE-2025-33237	NVIDIA HD Audio Driver for Windows contains a vulnerability where an attacker could exploit a NULL pointer dereference issue. A successful exploit of this vulnerability might lead to a denial of service.	5.5	More Details
CVE-2025-52627	Root File System Not Mounted as Read-Only configuration vulnerability. This can allow unintended modifications to critical system files, potentially increasing the risk of system compromise or unauthorized changes.This issue affects AION: 2.0.	5.5	More Details
CVE-2026-20415	In imgsys, there is a possible memory corruption due to improper locking. This could lead to local denial of service if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10363254; Issue ID: MSV-5617.	5.5	More Details
CVE-2025-68660	Discourse is an open source discussion platform. In versions prior to 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0, an endpoint lets any authenticated user bypass the ai_discover_persona access controls and gain ongoing DM access to personas that may be wired to staff-only categories, RAG document sets, or automated tooling, enabling unauthorized data disclosure. Because the controller also accepts arbitrary user_id, an attacker can impersonate other accounts to trigger unwanted AI conversations on their behalf, generating confusing or abusive PM traffic. This issue is patched in versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0. No known workarounds are available.	5.4	More Details
CVE-2026-23568	An out-of-bounds read vulnerability in the TeamViewer DEX Client (former 1E Client) - Content Distribution Service (NomadBranch.exe) prior version 26.1 for Windows allows an attacker on the adjacent network to cause information disclosure or denial-of-service via a special crafted packet. The leaked memory could be used to bypass ASLR and facilitate further exploitation.	5.4	More Details
CVE-2025-13983	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Tagify allows Cross-Site Scripting (XSS).This issue affects Tagify: from 0.0.0 before 1.2.44.	5.4	More Details
CVE-2026-24986	Cross-Site Request Forgery (CSRF) vulnerability in wp.insider Simple Membership WP user Import simple-membership-wp-user-import allows Cross Site Request Forgery.This issue affects Simple Membership WP user Import: from n/a through <= 1.9.1.	5.4	More Details
CVE-2026-25021	Missing Authorization vulnerability in Mizan Themes Mizan Demo Importer mizan-demo-importer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Mizan Demo Importer: from n/a through <= 0.1.3.	5.4	More Details
CVE-2026-25024	Cross-Site Request Forgery (CSRF) vulnerability in Blair Williams ThirstyAffiliates thirstyaffiliates allows Cross Site Request Forgery.This issue affects ThirstyAffiliates: from n/a through <= 3.11.9.	5.4	More Details
CVE-2026-24961	Server-Side Request Forgery (SSRF) vulnerability in ThemeGoods Grand Blog grandblog allows Server Side Request Forgery.This issue affects Grand Blog: from n/a through < 3.1.5.	5.4	More Details
CVE-	WebMO Job Manager 20.0 contains a cross-site scripting vulnerability in search parameters that allows remote attackers to inject malicious script code. Attackers can		More

2021-47920	exploit the filterSearch and filterSearchType parameters to perform non-persistent attacks including session hijacking and external redirects.	5.4	Details
CVE-2025-36033	IBM Engineering Lifecycle Management - Global Configuration Management 7.0.3 through 7.0.3 Interim Fix 017, and 7.1.0 through 7.1.0 Interim Fix 004 IBM Global Configuration Management is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details
CVE-2022-50942	Incinga Web 2.8.2 contains a client-side cross-site scripting vulnerability that allows remote attackers to inject malicious script codes through the icinga.min.js file. Attackers can exploit the EventListener.handleEvent method to execute arbitrary scripts, potentially leading to session hijacking and non-persistent phishing attacks.	5.4	More Details
CVE-2021-47911	Affiliate Pro 1.7 contains multiple reflected cross-site scripting vulnerabilities in the index module's input fields. Attackers can inject malicious scripts through fullname, username, and email parameters to execute client-side attacks and manipulate browser requests.	5.4	More Details
CVE-2026-24990	Missing Authorization vulnerability in Fahad Mahmood WP Docs wp-docs allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Docs: from n/a through <= 2.2.8.	5.4	More Details
CVE-2025-14274	The Unlimited Elements for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Border Hero widget's Button Link field in versions up to 2.0.1. This is due to insufficient input sanitization and output escaping on user-supplied URLs. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2025-70959	A stored cross-site scripting (XSS) vulnerability in the Jobs module of Tendenci CMS v15.3.7 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload.	5.4	More Details
CVE-2026-1312	An issue was discovered in 6.0 before 6.0.2, 5.2 before 5.2.11, and 4.2 before 4.2.28. `.QuerySet.order_by()` is subject to SQL injection in column aliases containing periods when the same alias is, using a suitably crafted dictionary, with dictionary expansion, used in `FilteredRelation`. 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 Solomon Kebede for reporting this issue.	5.4	More Details
CVE-2026-1447	The Mail Mint plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.19.2. This is due to missing nonce validation on the create_or_update_note function. This makes it possible for unauthenticated attackers to create or update contact notes via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Due to missing sanitization and escaping this can lead to stored Cross-Site Scripting.	5.4	More Details
CVE-2026-1207	An issue was discovered in 6.0 before 6.0.2, 5.2 before 5.2.11, and 4.2 before 4.2.28. Raster lookups on ``RasterField`` (only implemented on PostGIS) allows remote attackers to inject SQL via the band index parameter. 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 Tarek Nakkouch for reporting this issue.	5.4	More Details
CVE-2025-13979	Privilege Defined With Unsafe Actions vulnerability in Drupal Mini site allows Stored XSS.This issue affects Mini site: from 0.0.0 before 3.0.2.	5.4	More Details
CVE-2020-36993	LimeSurvey 4.3.10 contains a stored cross-site scripting vulnerability in the Survey Menu functionality of the administration panel. Attackers can inject malicious SVG scripts through the Surveymenu[title] and Surveymenu[parent_id] parameters to execute arbitrary JavaScript in administrative contexts.	5.4	More Details

CVE-2020-36988	PDW File Browser version 1.3 contains stored and reflected cross-site scripting vulnerabilities that allow authenticated attackers to inject malicious scripts through file rename and path parameters. Attackers can craft malicious URLs or rename files with XSS payloads to execute arbitrary JavaScript in victims' browsers when they access the file browser.	5.4	More Details
CVE-2025-69207	Khoj is a self-hostable artificial intelligence app. Prior to 2.0.0-beta.23, an IDOR in the Notion OAuth callback allows an attacker to hijack any user's Notion integration by manipulating the state parameter. The callback endpoint accepts any user UUID without verifying the OAuth flow was initiated by that user, allowing attackers to replace victims' Notion configurations with their own, resulting in data poisoning and unauthorized access to the victim's Khoj search index. This attack requires knowing the user's UUID which can be leaked through shared conversations where an AI generated image is present. This vulnerability is fixed in 2.0.0-beta.23.	5.4	More Details
CVE-2020-37044	OpenCTI 3.3.1 is vulnerable to a reflected cross-site scripting (XSS) attack via the /graphql endpoint. An attacker can inject arbitrary JavaScript code by sending a crafted GET request with a malicious payload in the query string, leading to execution of JavaScript in the victim's browser. For example, a request to /graphql?'"--></style></scRipt><scRipt>alert('Raif_Berkay')</scRipt> will trigger an alert. This vulnerability was discovered by Raif Berkay Dincel and confirmed on Linux Mint and Windows 10.	5.4	More Details
CVE-2026-23476	FacturaScripts is open-source enterprise resource planning and accounting software. Prior to 2025.8, there a reflected XSS bug in FacturaScripts. The problem is in how error messages get displayed. Twig's | raw filter is used, which skips HTML escaping. When triggering a database error (like passing a string where an integer is expected), the error message includes the input and gets rendered without sanitization. This vulnerability is fixed in 2025.8.	5.4	More Details
CVE-2025-45160	A HTML injection vulnerability exists in the file upload functionality of Cacti <= 1.2.29. When a file with an invalid format is uploaded, the application reflects the submitted filename back into an error popup without proper sanitization. As a result, attackers can inject arbitrary HTML elements (e.g., <h1>, <b>, <svg>) into the rendered page. NOTE: Multiple third-parties including the maintainer have stated that they cannot reproduce this issue after 1.2.27.	5.4	More Details
CVE-2026-1251	The SupportCandy – Helpdesk & Customer Support Ticket System plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.4.4 via the 'add_reply' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to steal file attachments uploaded by other users by specifying arbitrary attachment IDs in the 'description_attachments' parameter, re-associating those files to their own tickets and removing access from the original owners.	5.4	More Details
CVE-2025-69289	Discourse is an open source discussion platform. A privilege escalation vulnerability in versions prior to 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0 allows a non-admin moderator to bypass email-change restrictions, allowing a takeover of non-staff accounts. This issue is patched in versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0. As a workaround, ensure moderators are trusted or enable the "require_change_email_confirmation" setting.	5.4	More Details
CVE-2026-1287	An issue was discovered in 6.0 before 6.0.2, 5.2 before 5.2.11, and 4.2 before 4.2.28. `FilteredRelation` is subject to SQL injection in column aliases via control characters, using a suitably crafted dictionary, with dictionary expansion, as the `**kwargs` passed to `QuerySet` methods `annotate()`, `aggregate()`, `extra()`, `values()`, `values_list()`, and `alias()`. 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 Solomon Kebede for reporting this issue.	5.4	More Details
CVE-2025-70960	A stored cross-site scripting (XSS) vulnerability in the Forums module of Tendenci CMS v15.3.7 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload.	5.4	More Details

CVE-2025-67855	A flaw was found in moooodle. A remote attacker could exploit a reflected Cross-Site Scripting (XSS) vulnerability in the policy tool return URL. This vulnerability arises from insufficient sanitization of URL parameters, allowing attackers to inject malicious scripts through specially crafted links. Successful exploitation could lead to information disclosure or arbitrary client-side script execution within the user's browser.	5.4	More Details
CVE-2025-67856	A flaw was found in Moodle. An authorization logic flaw, specifically due to incomplete role checks during the badge awarding process, allowed badges to be granted without proper verification. This could enable unauthorized users to obtain badges they are not entitled to, potentially leading to privilege escalation or unauthorized access to certain features.	5.4	More Details
CVE-2025-36094	IBM Cloud Pak for Business Automation 25.0.0 through 25.0.0 Interim Fix 002, 24.0.1 through 24.0.1 Interim Fix 005, and 24.0.0 through 24.0.0 Interim Fix 007 could allow an authenticated user to cause a denial of service or corrupt existing data due to the improper validation of input length.	5.4	More Details
CVE-2026-1389	The Document Embedder – Embed PDFs, Word, Excel, and Other Files plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.0.4. This is due to the plugin not verifying that a user has permission to access the requested resource in the 'bplde_save_document_library', 'bplde_get_single', and 'bplde_delete_document_library' AJAX actions. This makes it possible for authenticated attackers, with Author-level access and above, to read, modify, and delete Document Library entries created by other users, including administrators, via the 'id' parameter.	5.3	More Details
CVE-2026-25019	Missing Authorization vulnerability in Vito Peleg Atarim atarim-visual-collaboration allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Atarim: from n/a through <= 4.3.1.	5.3	More Details
CVE-2026-1522	A weakness has been identified in Open5GS up to 2.7.6. This vulnerability affects the function sgwc_s5c_handle_modify_bearer_response of the file src/sgwc/s5c-handler.c of the component SGWC. Executing a manipulation can lead to denial of service. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. This patch is called b19cf6a. Applying a patch is advised to resolve this issue. The issue report is flagged as already-fixed.	5.3	More Details
CVE-2025-61730	During the TLS 1.3 handshake if multiple messages are sent in records that span encryption level boundaries (for instance the Client Hello and Encrypted Extensions messages), the subsequent messages may be processed before the encryption level changes. This can cause some minor information disclosure if a network-local attacker can inject messages during the handshake.	5.3	More Details
CVE-2025-55704	Hidden functionality issue exists in multiple MFPs provided by Brother Industries, Ltd., which may allow an attacker to obtain the logs of the affected product and obtain sensitive information within the logs.	5.3	More Details
CVE-2026-24904	TrustTunnel is an open-source VPN protocol with a rule bypass issue in versions prior to 0.9.115. In `tls_listener.rs`, `TlsListener::listen()` peeks 1024 bytes and calls `extract_client_random(...)`. If `parse_tls_plaintext` fails (for example, a fragmented/partial ClientHello split across TCP writes), `extract_client_random` returns `None`. In `rules.rs`, `RulesEngine::evaluate` only evaluates `client_random_prefix` when `client_random` is `Some(...)`. As a result, when extraction fails (`client_random == None`), any rule that relies on `client_random_prefix` matching is skipped and evaluation falls through to later rules. As an important semantics note: `client_random_prefix` is a match condition only. It does not mean "block non-matching prefixes" by itself. A rule with `client_random_prefix = ...` triggers its `action` only when the prefix matches (and the field is available to evaluate). Non-matches (or `None`) simply do not match that rule and continue to fall through. The vulnerability is fixed in version 0.9.115.	5.3	More Details

CVE-2026-1739	A vulnerability has been found in Free5GC pcf up to 1.4.1. This affects the function HandleCreateSmPolicyRequest of the file internal/sbi/processor/smpolicy.go. The manipulation leads to null pointer dereference. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is df535f5524314620715e842baf9723efbeb481a7. Applying a patch is the recommended action to fix this issue.	5.3	More Details
CVE-2026-1738	A flaw has been found in Open5GS up to 2.7.6. The impacted element is the function sgwc_tunnel_add of the file /src/sgwc/context.c of the component SGWC. Executing a manipulation of the argument pdr can lead to reachable assertion. The attack can be executed remotely. The exploit has been published and may be used. It is advisable to implement a patch to correct this issue. The issue report is flagged as already-fixed.	5.3	More Details
CVE-2026-0825	The Database for Contact Form 7, WPforms, Elementor forms plugin for WordPress is vulnerable to authorization bypass due to missing capability checks on the CSV export functionality in all versions up to, and including, 1.4.5. This makes it possible for unauthenticated attackers to download sensitive form submission data containing personally identifiable information (PII) by accessing the CSV export endpoint with an export key that is exposed in publicly accessible page source code. The vulnerability is created because while the shortcode properly filters displayed entries by user, the CSV export handler completely bypasses this filtering and exports all entries regardless of user permissions.	5.3	More Details
CVE-2026-1737	A vulnerability was detected in Open5GS up to 2.7.6. The affected element is the function sgwc_s5c_handle_create_bearer_request of the file /src/sgwc/s5c-handler.c of the component CreateBearerRequest Handler. Performing a manipulation results in reachable assertion. Remote exploitation of the attack is possible. The exploit is now public and may be used. To fix this issue, it is recommended to deploy a patch. The issue report is flagged as already-fixed.	5.3	More Details
CVE-2026-1736	A security vulnerability has been detected in Open5GS up to 2.7.6. Impacted is the function sgwc_s11_handle_create_indirect_data_forwarding_tunnel_request of the file /src/sgwc/s11-handler.c of the component SGWC. Such manipulation leads to reachable assertion. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. A patch should be applied to remediate this issue. The issue report is flagged as already-fixed.	5.3	More Details
CVE-2025-13473	An issue was discovered in 6.0 before 6.0.2, 5.2 before 5.2.11, and 4.2 before 4.2.28. The `django.contrib.auth.handlers.modwsgi.check_password()` function for authentication via `mod_wsgi` allows remote attackers to enumerate users via a timing attack. 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 Stackered for reporting this issue.	5.3	More Details
CVE-2026-1734	A security flaw has been discovered in Zhong Bang CRMEB up to 5.6.3. This vulnerability affects unknown code of the file crmeb/app/api/controller/v1/CrontabController.php of the component crontab Endpoint. The manipulation results in missing authorization. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-25010	Missing Authorization vulnerability in ILLID Share This Image share-this-image allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Share This Image: from n/a through <= 2.09.	5.3	More Details
CVE-2026-1298	The Easy Replace Image plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 3.5.2. This is due to missing capability checks on the `image_replacement_from_url` function that is hooked to the `eri_from_url` AJAX action. This makes it possible for authenticated attackers, with Contributor-level access and above, to replace arbitrary image attachments on the site with images from external URLs, potentially enabling site defacement, phishing attacks, or content manipulation.	5.3	More Details
	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable		

CVE-2026-1371	to Sensitive Information Exposure in all versions up to, and including, 3.9.5. This is due to missing authorization checks in the `ajax_coupon_details()` function, which only validates nonces but does not verify user capabilities. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve sensitive coupon information including coupon codes, discount amounts, usage statistics, and course/bundle applications.	5.3	More Details
CVE-2023-37525	A sensitive information disclosure in HCL BigFix Compliance allows a remote attacker to access files under the WEB-INF directory, which may contain Java class files and configuration information, leading to unauthorized access to application internals.	5.3	More Details
CVE-2026-1054	The RegistrationMagic plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 6.0.7.4. This is due to missing nonce verification and capability checks on the rm_set_otp AJAX action handler. This makes it possible for unauthenticated attackers to modify arbitrary plugin settings, including reCAPTCHA keys, security settings, and frontend menu titles.	5.3	More Details
CVE-2026-1682	A flaw has been found in Free5GC SMF up to 4.1.0. Affected is the function HandlePfcpAssociationReleaseRequest of the file internal/pfcp/handler/handler.go of the component PFCP UDP Endpoint. Executing a manipulation can lead to null pointer dereference. The attack may be launched remotely. The exploit has been published and may be used. A patch should be applied to remediate this issue.	5.3	More Details
CVE-2026-24994	Missing Authorization vulnerability in sunshinephotocart Sunshine Photo Cart sunshine-photo-cart allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sunshine Photo Cart: from n/a through <= 3.5.7.2.	5.3	More Details
CVE-2026-1586	A flaw has been found in Open5GS up to 2.7.5. Impacted is the function ogs_gtp2_f_teid_to_ip of the file /sgwc/s11-handler.c of the component SGWC. Executing a manipulation can lead to denial of service. The attack may be performed from remote. The exploit has been published and may be used. It is advisable to implement a patch to correct this issue. The issue report is flagged as already-fixed.	5.3	More Details
CVE-2026-25012	Missing Authorization vulnerability in gfazioli WP Bannerize Pro wp-bannerize-pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Bannerize Pro: from n/a through <= 1.11.0.	5.3	More Details
CVE-2026-24992	Insertion of Sensitive Information Into Sent Data vulnerability in WPFactory Advanced WooCommerce Product Sales Reporting webd-woocommerce-advanced-reporting-statistics allows Retrieve Embedded Sensitive Data.This issue affects Advanced WooCommerce Product Sales Reporting: from n/a through <= 4.1.2.	5.3	More Details
CVE-2026-1310	The Simple calendar for Elementor plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.6.6. This is due to missing capability checks on the `miga_ajax_editor_cal_delete` function that is hooked to the `miga_editor_cal_delete` AJAX action with both authenticated and unauthenticated access enabled. This makes it possible for unauthenticated attackers to delete arbitrary calendar entries by sending a request with a valid nonce and the calendar entry ID.	5.3	More Details
CVE-2026-24991	Authorization Bypass Through User-Controlled Key vulnerability in HT Plugins Extensions For CF7 extensions-for-cf7 allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Extensions For CF7: from n/a through <= 3.4.0.	5.3	More Details
CVE-2026-1760	A flaw was found in SoupServer. This HTTP request smuggling vulnerability occurs because SoupServer improperly handles requests that combine Transfer-Encoding: chunked and Connection: keep-alive headers. A remote, unauthenticated client can exploit this by sending specially crafted requests, causing SoupServer to fail to close the connection as required by RFC 9112. This allows the attacker to smuggle additional requests over the persistent connection, leading to unintended request processing and potential denial-of-service (DoS) conditions.	5.3	More Details
	The ML-DSA crate is a Rust implementation of the Module-Lattice-Based Digital Signature		

CVE-2026-24850	Standard (ML-DSA). Starting in version 0.0.4 and prior to version 0.1.0-rc.4, the ML-DSA signature verification implementation in the RustCrypto `ml-dsa` crate incorrectly accepts signatures with repeated (duplicate) hint indices. According to the ML-DSA specification (FIPS 204 / RFC 9881), hint indices within each polynomial must be **strictly increasing**. The current implementation uses a non-strict monotonic check (`<=` instead of `<`), allowing duplicate indices. This is a regression bug. The original implementation was correct, but a commit in version 0.0.4 inadvertently changed the strict `<` comparison to `<=`, introducing the vulnerability. Version 0.1.0-rc.4 fixes the issue.	5.3	More Details
CVE-2026-1683	A vulnerability has been found in Free5GC SMF up to 4.1.0. Affected by this vulnerability is the function HandlePfcpSessionReportRequest of the file internal/pfcp/handler/handler.go of the component PFCP. The manipulation leads to denial of service. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. To fix this issue, it is recommended to deploy a patch.	5.3	More Details
CVE-2025-15550	birkir prime <= 0.4.0.beta.0 contains a cross-site request forgery vulnerability in its GraphQL endpoint that allows attackers to exploit GET-based query requests. Attackers can craft malicious GET requests to trigger unauthorized actions against privileged users by manipulating GraphQL query parameters.	5.3	More Details
CVE-2026-1684	A vulnerability was found in Free5GC SMF up to 4.1.0. Affected by this issue is the function HandleReports of the file /internal/context/pfcp_reports.go of the component PFCP UDP Endpoint. The manipulation results in denial of service. The attack can be executed remotely. It is advisable to implement a patch to correct this issue.	5.3	More Details
CVE-2025-13980	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal CKEditor 5 Premium Features allows Functionality Bypass.This issue affects CKEditor 5 Premium Features: from 0.0.0 before 1.2.10, from 1.3.0 before 1.3.6, from 1.4.0 before 1.4.3, from 1.5.0 before 1.5.1, from 1.6.0 before 1.6.4.	5.3	More Details
CVE-2025-13985	Incorrect Authorization vulnerability in Drupal Entity Share allows Forceful Browsing.This issue affects Entity Share: from 0.0.0 before 3.13.0.	5.3	More Details
CVE-2026-20417	In pcie, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10314946 / ALPS10340155; Issue ID: MSV-5154.	5.3	More Details
CVE-2026-1587	A vulnerability has been found in Open5GS up to 2.7.6. The affected element is the function sgwc_s11_handle_modify_bearer_request of the file /sgwc/s11-handler.c of the component SGWC. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Applying a patch is the recommended action to fix this issue. The issue report is flagged as already-fixed.	5.3	More Details
CVE-2026-24998	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in WPMU DEV - Your All-in-One WordPress Platform Hustle wordpress-popup allows Retrieve Embedded Sensitive Data.This issue affects Hustle: from n/a through <= 7.8.9.2.	5.3	More Details
CVE-2025-15510	The NEX-Forms – Ultimate Forms Plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the NF5_Export_Forms class constructor in all versions up to, and including, 9.1.8. This makes it possible for unauthenticated attackers to export form configurations, that may include sensitive data, such as email addresses, PayPal API credentials, and third-party integration keys by enumerating the nex_forms_Id parameter.	5.3	More Details
CVE-2026-	CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to version 0.28.5.0, the authentication implementation in CI4MS is vulnerable to email enumeration. An unauthenticated attacker can determine whether an email address is registered in the	5.3	More Details

25509	system by analyzing the application's response during the password reset process. This issue has been patched in version 0.28.5.0.		
CVE-2026-24889	soroban-sdk is a Rust SDK for Soroban contracts. Arithmetic overflow can be triggered in the `Bytes::slice`, `Vec::slice`, and `Prng::gen_range` (for `u64`) methods in the `soroban-sdk` in versions up to and including `25.0.1`, `23.5.1`, and `25.0.2`. Contracts that pass user-controlled or computed range bounds to `Bytes::slice`, `Vec::slice`, or `Prng::gen_range` may silently operate on incorrect data ranges or generate random numbers from an unintended range, potentially resulting in corrupted contract state. Note that the best practice when using the `soroban-sdk` and building Soroban contracts is to always enable `overflow-checks = true`. The `stellar contract init` tool that prepares the boiler plate for a Soroban contract, as well as all examples and docs, encourage the use of configuring `overflow-checks = true` on `release` profiles so that these arithmetic operations fail rather than silently wrap. Contracts are only impacted if they use `overflow-checks = false` either explicitly or implicitly. It is anticipated the majority of contracts could not be impacted because the best practice encouraged by tooling is to enable `overflow-checks`. The fix available in `25.0.1`, `23.5.1`, and `25.0.2` replaces bare arithmetic with `checked_add` / `checked_sub`, ensuring overflow traps regardless of the `overflow-checks` profile setting. As a workaround, contract workspaces can be configured with a profile available in the GitHub Securtity Advisory to enable overflow checks on the arithmetic operations. This is the best practice when developing Soroban contracts, and the default if using the contract boilerplate generated using `stellar contract init`. Alternatively, contracts can validate range bounds before passing them to `slice` or `gen_range` to ensure the conversions cannot overflow.	5.3	More Details
CVE-2026-0909	The WP ULike plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.8.3.1. This is due to the `wp_ulike_delete_history_api` AJAX action not verifying that the log entry being deleted belongs to the current user. This makes it possible for authenticated attackers, with Subscriber-level access and above (granted the 'stats' capability is assigned to their role), to delete arbitrary log entries belonging to other users via the 'id' parameter.	5.3	More Details
CVE-2026-25144	Talishar is a fan-made Flesh and Blood project. A Stored XSS exists in the chat in-game system. The playerID parameter in SubmitChat.php and is saved without sanitization and executed whenever a user view the current page game. This vulnerability is fixed by 09dd00e5452e3cd998eb1406a88e5b0fa868e6b4.	5.3	More Details
CVE-2026-24664	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, a username enumeration vulnerability allows unauthenticated attackers to identify valid user accounts by analyzing differences in the login response behavior. This issue has been patched in version 4.2.	5.3	More Details
CVE-2026-24945	Missing Authorization vulnerability in Themefic Ultimate Addons for Contact Form 7 ultimate-addons-for-contact-form-7 allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ultimate Addons for Contact Form 7: from n/a through <= 3.5.34.	5.3	More Details
CVE-2026-24997	Missing Authorization vulnerability in Wired Impact Wired Impact Volunteer Management wired-impact-volunteer-management allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Wired Impact Volunteer Management: from n/a through <= 2.8.	5.3	More Details
CVE-2026-1431	The Booking Calendar plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the wpbc_ajax_WPBC_FLEXTIMELINE_NAV() function in all versions up to, and including, 10.14.13. This makes it possible for unauthenticated attackers to retrieve booking information including customer names, phones and emails.	5.3	More Details
CVE-2020-37007	Liman 0.7 contains a cross-site request forgery vulnerability that allows attackers to manipulate user account settings without proper request validation. Attackers can craft malicious HTML forms to change user passwords or modify account information by tricking logged-in users into submitting unauthorized requests.	5.3	More Details

CVE-2025-15525	The Ajax Load More – Infinite Scroll, Load More, & Lazy Load plugin for WordPress is vulnerable to unauthorized access of data due to incorrect authorization on the parse_custom_args() function in all versions up to, and including, 7.8.1. This makes it possible for unauthenticated attackers to expose the titles and excerpts of private, draft, pending, scheduled, and trashed posts.	5.3	More Details
CVE-2020-37091	Maian Support Helpdesk 4.3 contains a cross-site request forgery vulnerability that allows attackers to create administrative accounts without authentication. Attackers can craft malicious HTML forms to add admin users and upload PHP files with unrestricted file upload capabilities through the FAQ attachment system.	5.3	More Details
CVE-2020-37096	Edimax EW-7438RPn 1.13 contains a cross-site request forgery vulnerability in the MAC filtering configuration interface. Attackers can craft malicious web pages to trick users into adding unauthorized MAC addresses to the device's filtering rules without their consent.	5.3	More Details
CVE-2020-37046	Sistem Informasi Pengumuman Kelulusan Online 1.0 contains a cross-site request forgery vulnerability that allows attackers to add unauthorized admin users through the tambahuser.php endpoint. Attackers can craft a malicious HTML form to submit admin credentials and create new administrative accounts without the victim's consent.	5.3	More Details
CVE-2025-13471	The User Activity Log WordPress plugin through 2.2 does not properly handle failed login attempts in some cases, allowing unauthenticated users to set arbitrary options to 1 (for example to enable User Registration when it has been turned off)	5.3	More Details
CVE-2026-1391	The Vzaar Media Management plugin for WordPress is vulnerable to Reflected Cross-Site Scripting in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping on the $_SERVER['PHP_SELF'] variable. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	5.3	More Details
CVE-2026-25023	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in mdedev Run Contests, Raffles, and Giveaways with ContestsWP contest-code-checker allows Retrieve Embedded Sensitive Data.This issue affects Run Contests, Raffles, and Giveaways with ContestsWP: from n/a through <= 2.0.7.	5.3	More Details
CVE-2026-24982	Missing Authorization vulnerability in Brainstorm Force Spectra ultimate-addons-for-gutenberg allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Spectra: from n/a through <= 2.19.17.	5.3	More Details
CVE-2026-24967	Missing Authorization vulnerability in ameliabooking Amelia ameliabooking allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Amelia: from n/a through <= 1.2.38.	5.3	More Details
CVE-2025-15511	The Rupantorpay plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the handle_webhook() function in all versions up to, and including, 2.0.0. This makes it possible for unauthenticated attackers to modify WooCommerce order statuses by sending crafted requests to the WooCommerce API endpoint.	5.3	More Details
CVE-2020-37026	Sickbeard alpha contains a cross-site request forgery vulnerability that allows attackers to disable authentication by submitting crafted configuration parameters. Attackers can trick users into submitting a malicious form that clears web username and password, effectively removing authentication protection.	5.3	More Details
CVE-2026-1801	A flaw was found in libsoup, an HTTP client/server library. This HTTP Request Smuggling vulnerability arises from non-RFC-compliant parsing in the soup_filter_input_stream_read_line() logic, where libsoup accepts malformed chunk headers, such as lone line feed (LF) characters instead of the required carriage return and line feed (CRLF). A remote attacker can exploit this without authentication or user interaction by sending specially crafted chunked requests. This allows libsoup to parse and process multiple HTTP requests from a single network message, potentially leading to information disclosure.	5.3	More Details

CVE-2026-0950	The Spectra Gutenberg Blocks – Website Builder for the Block Editor plugin for WordPress is vulnerable to Information Disclosure in all versions up to, and including, 2.19.17. This is due to the plugin failing to check `post_password_required()` before rendering post excerpts in the `render_excerpt()` function and the `uagb_get_excerpt()` helper function. This makes it possible for unauthenticated attackers to read excerpts of password-protected posts by simply viewing any page that contains a Spectra Post Grid, Post Masonry, Post Carousel, or Post Timeline block.	5.3	More Details
CVE-2026-1060	The WP Adminify plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.0.7.7 via the /wp-json/adminify/v1/get-addons-list REST API endpoint. The endpoint is registered with permission_callback set to __return_true, allowing unauthenticated attackers to retrieve the complete list of available addons, their installation status, version numbers, and download URLs.	5.3	More Details
CVE-2026-1521	A security flaw has been discovered in Open5GS up to 2.7.6. This affects the function sgwc_s5c_handle_bearer_resource_failure_indication of the file src/sgwc/s5c-handler.c of the component SGWC. Performing a manipulation results in denial of service. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. The patch is named 69b53add90a9479d7960b822fc60601d659c328b. It is recommended to apply a patch to fix this issue.	5.3	More Details
CVE-2025-36428	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 - 11.5.9 and 12.1.0 - 12.1.3 could allow an authenticated user to cause a denial of service due to improper neutralization of special elements in data query logic when the RPSCAN feature is enabled.	5.3	More Details
CVE-2026-25152	Backstage is an open framework for building developer portals, and @backstage/plugin-techdocs-node provides common node.js functionalities for TechDocs. In versions of @backstage/plugin-techdocs-node prior to 1.13.11 and 1.14.1, a path traversal vulnerability in the TechDocs local generator allows attackers to read arbitrary files from the host filesystem when Backstage is configured with `techdocs.generator.runIn: local`. When processing documentation from untrusted sources, symlinks within the docs directory are followed by MkDocs during the build process. File contents are embedded into generated HTML and exposed to users who can view the documentation. This vulnerability is fixed in` @backstage/plugin-techdocs-node` versions 1.13.11 and 1.14.1. Some workarounds are available. Switch to `runIn: docker` in `app-config.yaml` and/or restrict write access to TechDocs source repositories to trusted users only.	5.3	More Details
CVE-2026-0936	An Insertion of Sensitive Information into Log File vulnerability in B&R PVI client versions prior to 6.5 may be abused by an authenticated local attacker to gather credential information which is processed by the PVI client application. The logging function of the PVI client application is disabled by default and must be explicitly enabled by the user.	5.0	More Details
CVE-2026-25228	Signal K Server is a server application that runs on a central hub in a boat. Prior to 2.20.3, a path traversal vulnerability in SignalK Server's applicationData API allows authenticated users on Windows systems to read, write, and list arbitrary files and directories on the filesystem. The validateAppId() function blocks forward slashes (/) but not backslashes (\), which are treated as directory separators by path.join() on Windows. This enables attackers to escape the intended applicationData directory. This vulnerability is fixed in 2.20.3.	5.0	More Details
CVE-2026-24667	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, failure to invalidate active user sessions after a password change allows existing session tokens to remain valid, potentially enabling unauthorized continued access to user accounts. This issue has been patched in version 4.2.	5.0	More Details
CVE-2026-	Improper Restriction of XML External Entity Reference vulnerability in Apache Syncope Console. An administrator with adequate entitlements to create or edit Keymaster parameters via Console can construct malicious XML text to launch an XXE attack,	4.9	More

23795	thereby causing sensitive data leakage occurs. This issue affects Apache Syncope: from 3.0 through 3.0.15, from 4.0 through 4.0.3. Users are recommended to upgrade to version 3.0.16 / 4.0.4, which fix this issue.		Details
CVE-2026-24767	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.0, a blind Server-Side Request Forgery (SSRF) vulnerability exists in the `uploadViaURL` functionality due to an unprotected `HEAD` request. While the subsequent file retrieval logic correctly enforces SSRF protections, the initial metadata request executes without validation. This allows limited outbound requests to arbitrary URLs before SSRF controls are applied. Version 0.301.0 contains a patch for the issue.	4.9	More Details
CVE-2026-24766	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.0, an authenticated user with org-level-creator permissions can exploit prototype pollution in the `/api/v2/meta/connection/test` endpoint, causing all database write operations to fail application-wide until server restart. While the pollution technically bypasses SUPER_ADMIN authorization checks, no practical privileged actions can be performed because database operations fail immediately after pollution. Version 0.301.0 patches the issue.	4.9	More Details
CVE-2026-22626	Due to insufficient input parameter validation on the interface, authenticated users of certain HIKSEMI NAS products can cause abnormal device behavior by crafting specific messages.	4.9	More Details
CVE-2025-70336	A Stored cross-site scripting (XSS) vulnerability in 'Create New Live Item' in PodcastGenerator 3.2.9 allows remote attackers to inject arbitrary script or HTML via the 'TITLE', 'SHORT DESCRIPTION' and 'LONG DESCRIPTION' parameters. The saved payload gets executed on 'View All Live Items' and 'Live Stream' pages.	4.8	More Details
CVE-2026-1533	A security flaw has been discovered in code-projects Online Music Site 1.0. The impacted element is an unknown function of the file /Administrator/PHP/AdminAddCategory.php. The manipulation results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	4.7	More Details
CVE-2025-6595	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MultimediaViewer.This issue affects MultimediaViewer: from * before 1.39.13, 1.42.7, 1.43.2, 1.44.0.	4.7	More Details
CVE-2026-24839	Dokploy is a free, self-hostable Platform as a Service (PaaS). In versions prior to 0.26.6, the Dokploy web interface is vulnerable to Clickjacking attacks due to missing frame-busting headers. This allows attackers to embed Dokploy pages in malicious iframes and trick authenticated users into performing unintended actions. Version 0.26.6 patches the issue.	4.7	More Details
CVE-2025-6594	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files resources/src/mediawiki.Special.Apisandbox/ApiSandbox.Js. This issue affects MediaWiki: from 1.27.0 before 1.39.13, 1.42.7 1.43.2, 1.44.0.	4.7	More Details
CVE-2026-25616	Blesta 3.x through 5.x before 5.13.3 mishandles input validation, aka CORE-5665.	4.7	More Details
CVE-2026-1690	A flaw has been found in Tenda HG10 US_HG7_HG9_HG10re_300001138_en_xpon. This affects the function system of the file /boaform/formSysCmd. This manipulation of the argument sysCmd causes command injection. The attack may be initiated remotely. The exploit has been published and may be used.	4.7	More Details
CVE-2026-24674	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, a Reflected Cross-Site Scripting (XSS) vulnerability allows remote attackers to execute arbitrary JavaScript in the context of authenticated users by crafting malicious URLs and tricking victims into visiting them. This issue has been patched in version 4.2.	4.7	More Details

CVE-2026-1742	A vulnerability was identified in EFM ipTIME A8004T 14.18.2. Affected by this vulnerability is the function commit_vpncli_file_upload of the file /cgi/timepro.cgi of the component VPN Service. Such manipulation leads to unrestricted upload. 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 but did not respond in any way.	4.7	More Details
CVE-2025-66488	Discourse is an open source discussion platform. A vulnerability present in versions prior to 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0 affects anyone who uses S3 for uploads. While scripts may be executed, they will only be run in the context of the S3/CDN domain, with no site credentials. Versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0 fix the issue. As a workaround, disallow html or xml files for uploads in authorized_extensions. For existing html xml uploads, site owners can consider deleting them.	4.6	More Details
CVE-2025-52628	HCL AION is affected by a Cookie with Insecure, Improper, or Missing SameSite vulnerability. This can allow cookies to be sent in cross-site requests, potentially increasing exposure to cross-site request forgery and related security risks. This issue affects AION: 2.0.	4.6	More Details
CVE-2026-24007	Tuleap is an Open Source Suite for management of software development and collaboration. Tuleap is missing CSRF protection in the Overview inconsistent items. An attacker could use this vulnerability to trick victims into repairing inconsistent items (creating artifact links from the release). This vulnerability is fixed in Tuleap Community Edition 17.0.99.1768924735 and Tuleap Enterprise Edition 17.2-5, 17.1-6, and 17.0-9.	4.6	More Details
CVE-2025-67723	Discourse is an open source discussion platform. Versions prior to 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0 have a content-security-policy-mitigated cross-site scriptinv vulnerability on the Discourse Math plugin when using its KaTeX variant. This issue is patched in versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0. As a workaround, the Discourse Math plugin can be disabled, or the Mathjax provider can be used instead of KaTeX.	4.6	More Details
CVE-2026-22625	Improper handling of filenames in certain HIKSEMI NAS products may lead to the exposure of sensitive system files.	4.6	More Details
CVE-2025-9226	Zohocorp ManageEngine OpManager, NetFlow Analyzer, and OpUtils versions prior to 128582 are affected by a stored cross-site scripting vulnerability in the Subnet Details.	4.6	More Details
CVE-2025-52626	A Potential Command Injection vulnerability in HCL AION. An This can allow unintended command execution, potentially leading to unauthorized actions on the underlying system.This issue affects AION: 2.0	4.5	More Details
CVE-2026-1083	The Appointment Hour Booking – Booking Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via form field configuration parameters in all versions up to, and including, 1.5.60 due to insufficient input sanitization and output escaping on the 'Min length/characters' and 'Max length/characters' field configuration values. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the form builder interface. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-22780	Rizin is a UNIX-like reverse engineering framework and command-line toolset. Prior to 0.8.2, a heap overflow can be exploited when a malicious mach0 file, having bogus entries for the dyld chained segments, is parsed by rizin. This vulnerability is fixed in 0.8.2.	4.4	More Details
CVE-2025-13981	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal AI (Artificial Intelligence) allows Cross-Site Scripting (XSS).This issue affects AI (Artificial Intelligence): from 0.0.0 before 1.0.7, from 1.1.0 before 1.1.7, from 1.2.0 before 1.2.4.	4.4	More Details

CVE-2026-1053	The Ivory Search – WordPress Search Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 5.5.13 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-1381	The Order Minimum/Maximum Amount Limits for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via settings in all versions up to, and including, 4.6.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Shop Manager-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-1399	The WP Google Ad Manager Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-13919	Symantec Endpoint Protection, prior to 14.3 RU10 Patch 1, RU9 Patch 2, and RU8 Patch 3, may be susceptible to a COM Hijacking vulnerability, which is a type of issue whereby an attacker attempts to establish persistence and evade detection by hijacking COM references in the Windows Registry.	4.4	More Details
CVE-2025-33081	IBM Concert 1.0.0 through 2.1.0 stores potentially sensitive information in log files that could be read by a local user.	4.3	More Details
CVE-2026-24996	Missing Authorization vulnerability in wpelemento WPElemento Importer wpelemento-importer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPElemento Importer: from n/a through <= 0.6.4.	4.3	More Details
CVE-2026-24965	Missing Authorization vulnerability in Wasiliy Strecker / ContestGallery developer Contest Gallery contest-gallery allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Contest Gallery: from n/a through <= 28.1.1.	4.3	More Details
CVE-2026-1600	A vulnerability was identified in Bdtask Bhojon All-In-One Restaurant Management System up to 20260116. The impacted element is an unknown function of the file /hungry/addtocart of the component Add-to-Cart Submission Endpoint. The manipulation of the argument price/allprice leads to business logic errors. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-1549	A vulnerability was identified in jishenghua jshERP up to 3.6. Affected by this vulnerability is an unknown functionality of the file /jshERP-boot/plugin/uploadPluginConfigFile of the component PluginController. Such manipulation of the argument configFile leads to path traversal. The attack may be launched remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-24951	Missing Authorization vulnerability in Saad Iqbal myCred mycred allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects myCred: from n/a through <= 2.9.7.3.	4.3	More Details
CVE-2026-24947	Missing Authorization vulnerability in LA-Studio LA-Studio Element Kit for Elementor lastudio-element-kit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects LA-Studio Element Kit for Elementor: from n/a through < 1.5.6.3.	4.3	More Details
	Discourse is an open source discussion platform. Versions prior to 3.5.4, 2025.11.2,		

CVE-2025-68659	2025.12.1, and 2026.1.0 have an application level denial of service vulnerabilityin the username change functionality at try.discourse.org. The vulnerability allows attackers to cause noticeable server delays and resource exhaustion by sending large JSON payloads to the username preference endpoint PUT /u//preferences/username, resulting in degraded performance for other users and endpoints. This issue is patched in versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0. No known workarounds are available.	4.3	More Details
CVE-2026-24673	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, a file upload validation bypass vulnerability allows attackers to upload files with prohibited extensions by embedding them inside ZIP archives and extracting them using the application’s built-in decompression functionality. This issue has been patched in version 4.2.	4.3	More Details
CVE-2026-24774	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, a business logic vulnerability allows authenticated students to improperly mark themselves as present in attendance activities, including activities that have already expired, by directly accessing a crafted URL. This issue has been patched in version 4.2.	4.3	More Details
CVE-2025-14795	The Stop Spammers Classic plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2026.1. This is due to missing nonce validation in the ss_addtoallowlist class. This makes it possible for unauthenticated attackers to add arbitrary email addresses to the spam allowlist via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. The vulnerability was partially patched in version 2026.1.	4.3	More Details
CVE-2025-14616	The Recooty – Job Widget (Old Dashboard) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.6. This is due to missing nonce validation on the recooty_save_maybe() function. This makes it possible for unauthenticated attackers to update the recooty_key option and inject malicious content into iframe src attributes via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-24942	Cross-Site Request Forgery (CSRF) vulnerability in magepeopleteam WpEvently mage-eventpress allows Cross Site Request Forgery.This issue affects WpEvently: from n/a through <= 5.1.1.	4.3	More Details
CVE-2026-24940	Missing Authorization vulnerability in Themefic Travelfic Toolkit travelfic-toolkit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Travelfic Toolkit: from n/a through <= 1.3.3.	4.3	More Details
CVE-2026-24939	Missing Authorization vulnerability in WP Chill Modula Image Gallery modula-best-grid-gallery allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Modula Image Gallery: from n/a through <= 2.13.6.	4.3	More Details
CVE-2026-1398	The Change WP URL plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing or incorrect nonce validation on the 'change-wp-url' page. This makes it possible for unauthenticated attackers to change the WP Login URL via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-37114	GUnet OpenEclass 1.7.3 allows unauthenticated and authenticated users to access sensitive information, including system information, application version, and other students' uploaded assessments, due to improper access controls and information disclosure flaws in various modules. Attackers can retrieve system info, version info, and view or download other users' files without proper authorization.	4.3	More Details
CVE-2020-37054	Navigate CMS 2.8.7 contains a cross-site request forgery vulnerability that allows attackers to upload malicious extensions through a crafted HTML page. Attackers can trick authenticated administrators into executing arbitrary file uploads by leveraging the extension upload functionality without additional validation.	4.3	More Details

CVE-2025-46316	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 26.1 and iPadOS 26.1, Pages 15.1, macOS Tahoe 26.1. Processing a maliciously crafted Pages document may result in unexpected termination or disclosure of process memory.	4.3	More Details
CVE-2026-1377	The imwptip plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1. This is due to missing nonce validation on the settings update functionality. This makes it possible for unauthenticated attackers to update the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-1380	The Bitcoin Donate Button plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing or incorrect nonce validation on the settings page. This makes it possible for unauthenticated attackers to modify the plugin's settings, including donation addresses and display configurations, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-24966	Cross-Site Request Forgery (CSRF) vulnerability in Copyscape Copyscape Premium copyscape-premium allows Cross Site Request Forgery.This issue affects Copyscape Premium: from n/a through <= 1.4.1.	4.3	More Details
CVE-2026-1165	The Popup Box plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.1.1. This is due to a flawed nonce implementation in the 'publish_unpublish_popupbox' function that verifies a self-created nonce rather than one submitted in the request. This makes it possible for unauthenticated attackers to change the publish status of popups via a forged request, granted they can trick a site administrator into performing an action such as clicking a link.	4.3	More Details
CVE-2026-1733	A vulnerability was identified in Zhong Bang CRMEB up to 5.6.3. This affects the function detail/tidyOrder of the file /api/store_integral/order/detail/:uni. The manipulation of the argument order_id leads to improper authorization. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-1745	A vulnerability was determined in SourceCodester Medical Certificate Generator App 1.0. This affects an unknown part. This manipulation causes cross-site request forgery. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	4.3	More Details
CVE-2026-24995	Missing Authorization vulnerability in Iulia Cazan Latest Post Shortcode latest-post-shortcode allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Latest Post Shortcode: from n/a through <= 14.2.0.	4.3	More Details
CVE-2026-25011	Missing Authorization vulnerability in Northern Beaches Websites WP Custom Admin Interface wp-custom-admin-interface allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Custom Admin Interface: from n/a through <= 7.41.	4.3	More Details
CVE-2026-0818	When a user explicitly requested Thunderbird to decrypt an inline OpenPGP message that was embedded in a text section of an email that was formatted and styled with HTML and CSS, then the decrypted contents were rendered in a context in which the CSS styles from the outer messages were active. If the user had additionally allowed loading of the remote content referenced by the outer email message, and the email was crafted by the sender using a combination of CSS rules and fonts and animations, then it was possible to extract the secret contents of the email. This vulnerability affects Thunderbird < 147.0.1 and Thunderbird < 140.7.1.	4.3	More Details
CVE-2026-25014	Cross-Site Request Forgery (CSRF) vulnerability in themelooks Enter Addons enteraddons allows Cross Site Request Forgery.This issue affects Enter Addons: from n/a through <= 2.3.2.	4.3	More Details
CVE-			

2026-25015	Cross-Site Request Forgery (CSRF) vulnerability in Stiofan UsersWP userswp allows Cross Site Request Forgery.This issue affects UsersWP: from n/a through <= 1.2.53.	4.3	More Details
CVE-2026-22764	Dell OpenManage Network Integration, versions prior to 3.9, contains an Improper Authentication vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	4.3	More Details
CVE-2025-67857	A flaw was found in moodle. During anonymous assignment submissions, user identifiers were inadvertently exposed in URLs. This data exposure allows unauthorized viewers to see internal user IDs, compromising the intended anonymity and potentially leading to information disclosure.	4.3	More Details
CVE-2026-25016	Missing Authorization vulnerability in Nelio Software Nelio Popups nelio-popups allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Nelio Popups: from n/a through <= 1.3.5.	4.3	More Details
CVE-2026-0658	The Five Star Restaurant Reservations WordPress plugin before 2.7.9 does not have CSRF checks in some bulk actions, which could allow attackers to make logged in admins perform unwanted actions, such as deleting bookings via CSRF attacks.	4.3	More Details
CVE-2026-1735	A weakness has been identified in Yealink MeetingBar A30 133.321.0.3. This issue affects some unknown processing of the component Diagnostic Handler. This manipulation causes command injection. It is feasible to perform the attack on the physical device. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-1599	A vulnerability was determined in Bdtask Bhojon All-In-One Restaurant Management System up to 20260116. The affected element is an unknown function of the file /hungry/placeorder of the component Checkout. Executing a manipulation of the argument orggrandTotal/vat/service_charge/grandtotal can lead to business logic errors. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-22624	Due to inadequate access control, authenticated users of certain HIKSEMI NAS products can manipulate other users' file resources without proper authorization.	4.3	More Details
CVE-2025-15322	Tanium addressed an improper access controls vulnerability in Tanium Server.	4.3	More Details
CVE-2026-24985	Missing Authorization vulnerability in approveme WP Forms Signature Contract Add-On wp-forms-signature-contract-add-on allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Forms Signature Contract Add-On: from n/a through <= 1.8.2.	4.3	More Details
CVE-2026-25020	Missing Authorization vulnerability in WP connect WP Sync for Notion wp-sync-for-notion allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Sync for Notion: from n/a through <= 1.7.0.	4.3	More Details
CVE-2025-15395	IBM Jazz Foundation 7.0.3 through 7.0.3 iFix019 and 7.1.0 through 7.1.0 iFix005 is vulnerable to access control violations that allows the users to view or access/perform actions beyond their expected capability.	4.3	More Details
CVE-2025-13986	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal Disable Login Page allows Functionality Bypass.This issue affects Disable Login Page: from 0.0.0 before 1.1.3.	4.2	More Details
CVE-2020-36944	ILIAS Learning Management System 4.3 contains a server-side request forgery vulnerability that allows attackers to read local files through portfolio PDF export functionality. Attackers can inject a script that uses XMLHttpRequest to retrieve local file contents when the portfolio is exported to PDF.	4.0	More Details

CVE-2025-52631	HCL AION is affected by a Missing or Insecure HTTP Strict-Transport-Security (HSTS) Header vulnerability. This can allow insecure connections, potentially exposing the application to man-in-the-middle and protocol downgrade attacks.. This issue affects AION: 2.0.	3.7	More Details
CVE-2025-53869	Multiple MFPs provided by Brother Industries, Ltd. does not properly validate server certificates, which may allow a man-in-the-middle attacker to replace the set of root certificates used by the product with a set of arbitrary certificates.	3.7	More Details
CVE-2026-1685	A vulnerability was identified in D-Link DIR-823X 250416. This vulnerability affects the function sub_40AC74 of the component Login. Such manipulation leads to improper restriction of excessive authentication attempts. The attack may be performed from remote. This attack is characterized by high complexity. It is stated that the exploitability is difficult. The exploit is publicly available and might be used.	3.7	More Details
CVE-2025-52629	HCL AION is susceptible to Missing Content-Security-Policy. An The absence of a CSP header may increase the risk of cross-site scripting and other content injection attacks by allowing unsafe scripts or resources to execute..This issue affects AION: 2.0.	3.7	More Details
CVE-2026-25224	Fastify is a fast and low overhead web framework, for Node.js. Prior to version 5.7.3, a denial-of-service vulnerability in Fastify's Web Streams response handling can allow a remote client to exhaust server memory. Applications that return a ReadableStream (or Response with a Web Stream body) via reply.send() are impacted. A slow or non-reading client can trigger unbounded buffering when backpressure is ignored, leading to process crashes or severe degradation. This issue has been patched in version 5.7.3.	3.7	More Details
CVE-2025-52623	HCL AION is affected by an Autocomplete HTML Attribute Not Disabled for Password Field vulnerability. This can allow autocomplete on password fields may lead to unintended storage or disclosure of sensitive credentials, potentially increasing the risk of unauthorized access. This issue affects AION: 2.0.	3.7	More Details
CVE-2026-1700	A weakness has been identified in projectworlds House Rental and Property Listing 1.0. This vulnerability affects unknown code of the file /app/sms.php. This manipulation of the argument Message causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	3.5	More Details
CVE-2025-67852	A flaw was found in Moodle. An open redirect vulnerability in the OAuth login flow allows a remote attacker to redirect users to attacker-controlled pages after they have successfully authenticated. This occurs due to insufficient validation of redirect parameters, which could lead to phishing attacks or information disclosure.	3.5	More Details
CVE-2026-1598	A vulnerability was found in Bdtask Bhojon All-In-One Restaurant Management System up to 20260116. Impacted is an unknown function of the file /dashboard/home/profile of the component User Information Module. Performing a manipulation of the argument fullname results in 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 disclosure but did not respond in any way.	3.5	More Details
CVE-2026-25211	Llama Stack (aka llama-stack) before 0.4.0rc3 does not censor the pgvector password in the initialization log.	3.2	More Details
CVE-2025-15288	Tanium addressed an improper access controls vulnerability in Interact.	3.1	More Details
CVE-2026-24513	A security issue was discovered in ingress-nginx where the protection afforded by the `auth-url` Ingress annotation may not be effective in the presence of a specific misconfiguration. If the ingress-nginx controller is configured with a default custom-errors configuration that includes HTTP errors 401 or 403, and if the configured default custom-errors backend is defective and fails to respect the X-Code HTTP header, then an Ingress	3.1	More Details

	with the `auth-url` annotation may be accessed even when authentication fails. Note that the built-in custom-errors backend works correctly. To trigger this issue requires an administrator to specifically configure ingress-nginx with a broken external component.		
CVE-2026-1751	A vulnerability has been discovered in GitLab CE/EE affecting all versions starting with 16.8 before 18.5.0 that could have allowed unauthorized edits to merge request approval rules under certain conditions.	3.1	More Details
CVE-2025-52633	HCL AION is affected by a Permanent Cookie Containing Sensitive Session Information vulnerability. It is storing sensitive session data in persistent cookies may increase the risk of unauthorized access if the cookies are intercepted or compromised. This issue affects AION: 2.0.	3.1	More Details
CVE-2026-1743	A vulnerability has been found in DJI Mavic Mini, Air, Spark and Mini SE up to 01.00.0500. Affected by this vulnerability is an unknown functionality of the component Enhanced Wi-Fi Pairing. The manipulation leads to authentication bypass by capture-replay. The attack must be carried out from within the local network. A high degree of complexity is needed for the attack. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2026-23553	In the context switch logic Xen attempts to skip an IBPB in the case of a vCPU returning to a CPU on which it was the previous vCPU to run. While safe for Xen's isolation between vCPUs, this prevents the guest kernel correctly isolating between tasks. Consider: 1) vCPU runs on CPU A, running task 1. 2) vCPU moves to CPU B, idle gets scheduled on A. Xen skips IBPB. 3) On CPU B, guest kernel switches from task 1 to 2, issuing IBPB. 4) vCPU moves back to CPU A. Xen skips IBPB again. Now, task 2 is running on CPU A with task 1's training still in the BTB.	2.9	More Details
CVE-2026-25046	Kimi Agent SDK is a set of libraries that expose the Kimi Code (Kimi CLI) agent runtime in applications. The vsix-publish.js and ovsx-publish.js scripts pass filenames to execSync() as shell command strings. Prior to version 0.1.6, filenames containing shell metacharacters like $(cmd) could execute arbitrary commands. Note: This vulnerability exists only in the repository's development scripts. The published VSCode extension does not include these files and end users are not affected. This is fixed in version 0.1.6 by replacing execSync with execFileSync using array arguments. As a workaround, ensure .vsix files in the project directory have safe filenames before running publish scripts.	2.9	More Details
CVE-2025-36194	IBM PowerVM Hypervisor FW1110.00 through FW1110.03, FW1060.00 through FW1060.51, and FW950.00 through FW950.F0 may expose a limited amount of data to a peer partition in specific shared processor configurations during certain operations.	2.8	More Details
CVE-2026-1588	A vulnerability was found in jishenghua jshERP up to 3.6. The impacted element is the function install of the file /jshERP-boot/plugin/installByPath of the component com.gitee.starblues.integration.operator.DefaultPluginOperator. The manipulation of the argument path results in path traversal. It is possible to launch the attack remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	2.7	More Details
CVE-2026-1518	A flaw was found in Keycloak’s CIBA feature where insufficient validation of client-configured backchannel notification endpoints could allow blind server-side requests to internal services.	2.7	More Details
CVE-2025-13881	A flaw was found in Keycloak Admin API. This vulnerability allows an administrator with limited privileges to retrieve sensitive custom attributes via the /unmanagedAttributes endpoint, bypassing User Profile visibility settings.	2.7	More Details
CVE-2026-1520	A vulnerability was identified in rethinkdb up to 2.4.3. Affected by this issue is some unknown functionality of the component Secondary Index Handler. Such manipulation leads to cross site scripting. 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 but did not respond in any way.	2.4	More Details

CVE-2026-1705	A vulnerability was detected in D-Link DSL-6641K N8.TR069.20131126. Affected by this issue is the function ad_virtual_server_vdsl of the component Web Interface. Performing a manipulation of the argument Name results in cross site scripting. It is possible to initiate the attack remotely. The exploit is now public and may be used.	2.4	More Details
CVE-2026-1532	A vulnerability was identified in D-Link DCS-700L 1.03.09. The affected element is the function uploadmusic of the file /setUploadMusic of the component Music File Upload Service. The manipulation of the argument UploadMusic leads to path traversal. The attack can only be initiated within the local network. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	2.4	More Details
CVE-2026-1744	A vulnerability was found in D-Link DSL-6641K N8.TR069.20131126. Affected by this issue is the function doSubmitPPP of the file sp_pppoe_user.js. The manipulation of the argument Username results in cross site scripting. The attack may be launched remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	2.4	More Details
CVE-2026-1814	Rapid7 Nexpose versions 6.4.50 and later are vulnerable to an insufficient entropy issue in the CredentialsKeyStorePassword.generateRandomPassword() method. When updating legacy keystore passwords, the application generates a new password with insufficient length (7-12 characters) and a static prefix 'p', resulting in a weak keyspace. An attacker with access to the nsc.ks file can brute-force this password using consumer-grade hardware to decrypt stored credentials.	N/A	More Details
CVE-2026-24988	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brian Hogg The Events Calendar Shortcode & Block the-events-calendar-shortcode allows Stored XSS.This issue affects The Events Calendar Shortcode & Block: from n/a through <= 3.1.1.	N/A	More Details
CVE-2026-25027	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove Unicamp unicamp allows PHP Local File Inclusion.This issue affects Unicamp: from n/a through <= 2.7.1.	N/A	More Details
CVE-2026-24984	Missing Authorization vulnerability in Brecht Visual Link Preview visual-link-preview allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Visual Link Preview: from n/a through <= 2.2.9.	N/A	More Details
CVE-2026-24962	Cross-Site Request Forgery (CSRF) vulnerability in Brainstorm Force Sigmize sigmize allows Cross Site Request Forgery.This issue affects Sigmize: from n/a through <= 0.0.9.	N/A	More Details
CVE-2026-25028	Missing Authorization vulnerability in Element Invader ElementInvader Addons for Elementor elementinvader-addons-for-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ElementInvader Addons for Elementor: from n/a through <= 1.4.1.	N/A	More Details
CVE-2026-25036	Missing Authorization vulnerability in WP Chill Passster content-protector allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Passster: from n/a through <= 4.2.25.	N/A	More Details
CVE-2025-65017	Decidim is a participatory democracy framework. In versions from 0.30.0 to before 0.30.4 and from 0.31.0.rc1 to before 0.31.0, the private data exports can lead to data leaks in case the UUID generation, causing collisions for the generated UUIDs. This issue has been patched in versions 0.30.4 and 0.31.0.	N/A	More Details
CVE-2026-24762	RustFS is a distributed object storage system built in Rust. From versions alpha.13 to alpha.81, RustFS logs sensitive credential material (access key, secret key, session token) to application logs at INFO level. This results in credentials being recorded in plaintext in log output, which may be accessible to internal or external log consumers and could lead to compromise of sensitive credentials. This issue has been patched in version alpha.82.	N/A	More Details

CVE-2026-21862	RustFS is a distributed object storage system built in Rust. Prior to version alpha.78, IP-based access control can be bypassed: get_condition_values trusts client-supplied X-Forwarded-For/X-Real-Ip without verifying a trusted proxy, so any reachable client can spoof aws:SourceIp and satisfy IP-allowlist policies. This issue has been patched in version alpha.78.	N/A	More Details
CVE-2026-25522	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored XSS vulnerability in Craft Commerce allows attackers to execute malicious JavaScript in an administrator's browser. This occurs because the Shipping Zone (Name & Description) fields in the Store Management section are not properly sanitized before being displayed in the admin panel. This issue has been patched in versions 4.10.1 and 5.5.2.	N/A	More Details
CVE-2020-37087	Easy Transfer Wifi Transfer v1.7 for iOS contains a persistent cross-site scripting vulnerability that allows remote attackers to inject malicious scripts by manipulating the oldPath, newPath, and path parameters in Create Folder and Move/Edit functions. Attackers can exploit improper input validation via POST requests to execute arbitrary JavaScript in the context of the mobile web application.	N/A	More Details
CVE-2025-65081	An out-of-bounds read vulnerability has been identified in the Postscript interpreter in various Lexmark devices. This vulnerability can be leveraged by an attacker to execute arbitrary code as an unprivileged user.	N/A	More Details
CVE-2026-24427	Shenzhen Tenda AC7 firmware version V03.03.03.01_cn and prior expose sensitive information in web management responses. Administrative credentials, including the router and/or admin panel password, are included in plaintext within configuration response bodies. In addition, responses lack appropriate Cache-Control directives, which may permit web browsers to cache pages containing these credentials and enable subsequent disclosure to an attacker with access to the client system or browser profile.	N/A	More Details
CVE-2026-24426	Shenzhen Tenda AC7 firmware version V03.03.03.01_cn and prior contain an improper output encoding vulnerability in the web management interface. User-supplied input is reflected in HTTP responses without adequate escaping, allowing injection of arbitrary HTML or JavaScript in a victim's browser context.	N/A	More Details
CVE-2026-0620	When configured as L2TP/IPSec VPN server, Archer AXE75 V1 may accept connections using L2TP without IPSec protection, even when IPSec is enabled. This allows VPN sessions without encryption, exposing data in transit and compromising confidentiality.	N/A	More Details
CVE-2026-24434	Shenzhen Tenda AC7 firmware version V03.03.03.01_cn and prior does not implement CSRF protections for administrative functions in the web management interface. The interface does not enforce anti-CSRF tokens or robust origin validation, which can allow an attacker to induce a logged-in administrator to perform unintended state-changing requests and modify router settings.	N/A	More Details
CVE-2026-24441	Shenzhen Tenda AC7 firmware version V03.03.03.01_cn and prior expose account credentials in plaintext within HTTP responses, allowing an on-path attacker to obtain sensitive authentication material.	N/A	More Details
CVE-2025-65077	A relative path traversal vulnerability has been identified in the Embedded Solutions Framework in various Lexmark devices. This vulnerability can be leveraged by an attacker to execute arbitrary code as an unprivileged user.	N/A	More Details
CVE-2025-65078	An untrusted search path vulnerability has been identified in the Embedded Solutions Framework in various Lexmark devices. This vulnerability can be leveraged by an attacker to execute arbitrary code.	N/A	More Details
CVE-2025-65079	A heap-based buffer overflow vulnerability has been identified in the Postscript interpreter in various Lexmark devices. This vulnerability can be leveraged by an attacker to execute arbitrary code as an unprivileged user.	N/A	More Details
CVE-2025-	A type confusion vulnerability has been identified in the Postscript interpreter in various Lexmark devices. This vulnerability can be leveraged by an attacker to execute arbitrary	N/A	More

65080	code as an unprivileged user.		Details
CVE-2025-62673	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tdpserver modules) allows adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted network packet containing a maliciously formed field.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	N/A	More Details
CVE-2026-25234	PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, a SQL injection vulnerability in category deletion can allow an attacker with access to the category manager workflow to inject SQL via a category id. This issue has been patched in version 1.33.0.	N/A	More Details
CVE-2025-62600	Fast DDS is a C++ implementation of the DDS (Data Distribution Service) standard of the OMG (Object Management Group). Prior to versions 3.4.1, 3.3.1, and 2.6.11, when the security mode is enabled, modifying the DATA Submessage within an SPDP packet sent by a publisher causes an Out-Of-Memory (OOM) condition, resulting in remote termination of Fast-DDS. If t he fields of PID_IDENTITY_TOKEN or PID_PERMISSION_TOKEN in the DATA Submessage — specifically by tampering with the length field in readBinaryPropertySeq — are modified, an integer overflow occurs, leading to an OOM during the resize operation. Versions 3.4.1, 3.3.1, and 2.6.11 patch the issue.	N/A	More Details
CVE-2025-62501	SSH Hostkey misconfiguration vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows attackers to obtain device credentials through a specially crafted man-in-the-middle (MITM) attack. This could enable unauthorized access if captured credentials are reused.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	N/A	More Details
CVE-2025-62405	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted network packet containing a field whose length exceeds the maximum expected value.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	N/A	More Details
CVE-2025-62404	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted network packet whose length exceeds the maximum expected value.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	N/A	More Details
CVE-2025-61983	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted network packet containing an excessive number of fields with zero-length values.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	N/A	More Details
CVE-2025-61944	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted network packet containing an excessive number of fields with zero-length values.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	N/A	More Details
CVE-2025-59487	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code. The vulnerability arises from improper validation of a packet field whose offset is used to determine the write location in memory. By crafting a packet with a manipulated field offset, an attacker can redirect writes to arbitrary memory locations.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	N/A	More Details
CVE-2025-	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted network packet containing a	N/A	More Details

59482	field whose length exceeds the maximum expected value.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.		
CVE-2025-58077	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted set of network packets containing an excessive number of host entries This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	N/A	More Details
CVE-2026-25233	PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, logic bug in the roadmap role check allows non-lead maintainers to create, update, or delete roadmaps. This issue has been patched in version 1.33.0.	N/A	More Details
CVE-2026-25235	PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, predictable verification hashes may allow attackers to guess verification tokens and potentially verify election account requests without authorization. This issue has been patched in version 1.33.0.	N/A	More Details
CVE-2026-22220	A lack of proper input validation in the HTTP processing path in TP-Link Archer BE230 v1.2 (web modules) may allow a crafted request to cause the device’s web service to become unresponsive, resulting in a denial of service condition. A network adjacent attacker with high privileges could cause the device’s web interface to temporarily stop responding until it recovers or is rebooted. This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	N/A	More Details
CVE-2025-62603	Fast DDS is a C++ implementation of the DDS (Data Distribution Service) standard of the OMG (Object Management Group). ParticipantGenericMessage is the DDS Security control-message container that carries not only the handshake but also on going security-control traffic after the handshake, such as crypto-token exchange, rekeying, re-authentication, and token delivery for newly appearing endpoints. On receive, the CDR parser is invoked first and deserializes the `message_data` (i .e., the `DataHolderSeq`) via the `readParticipantGenericMessage → readDataHolderSeq` path. The `DataHolderSeq` is parsed sequentially: a sequence count (`uint32`), and for each DataHolder the `class_id` string (e.g. `DDS:Auth:PKI-DH:1.0+Req`), string properties (a sequence of key/value pairs), and binary properties (a name plus an octet-vector). The parser operat es at a stateless level and does not know higher-layer state (for example, whether the handshake has already completed), s o it fully unfolds the structure before distinguishing legitimate from malformed traffic. Because RTPS permits duplicates, delays, and retransmissions, a receiver must perform at least minimal structural parsing to check identity and sequence n umbers before discarding or processing a message; the current implementation, however, does not "peek" only at a minimal header and instead parses the entire `DataHolderSeq`. As a result, prior to versions 3.4.1, 3.3.1, and 2.6.11, this parsi ng behavior can trigger an out-of-memory condition and remotely terminate the process. Versions 3.4.1, 3.3.1, and 2.6.11 p atch the issue.	N/A	More Details
CVE-2026-25489	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored XSS vulnerability in Craft Commerce allows attackers to execute malicious JavaScript in an administrator’s browser. This occurs because the Name & Description fields in Tax Zones are not properly sanitized before being displayed in the admin panel. This issue has been patched in versions 4.10.1 and 5.5.2.	N/A	More Details
CVE-2026-25488	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored XSS vulnerability in Craft Commerce allows attackers to execute malicious JavaScript in an administrator’s browser. This occurs because the Tax Categories (Name & Description) fields in the Store Management section are not properly sanitized before being displayed in the admin panel. This issue has been patched in versions 4.10.1 and 5.5.2.	N/A	More Details
CVE-	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored XSS vulnerability in Craft Commerce allows attackers to execute malicious JavaScript in an administrator's browser. This occurs		More

2026-25487	because the Tax Rates 'Name' field in the Store Management section is not properly sanitized before being displayed in the admin panel. This issue has been patched in versions 4.10.1 and 5.5.2.	N/A	Details
CVE-2026-25486	Craft Commerce is an ecommerce platform for Craft CMS. From version 5.0.0 to 5.5.1, a stored XSS vulnerability in Craft Commerce allows attackers to execute malicious JavaScript in an administrator’s browser. This occurs because the Shipping Methods Name field in the Store Management section is not properly sanitized before being displayed in the admin panel. This issue has been patched in version 5.5.2.	N/A	More Details
CVE-2026-25485	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored XSS vulnerability in Craft Commerce allows attackers to execute malicious JavaScript in an administrator’s browser. This occurs because the Shipping Categories (Name & Description) fields in the Store Management section are not properly sanitized before being displayed in the admin panel. This issue has been patched in versions 4.10.1 and 5.5.2.	N/A	More Details
CVE-2026-25484	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, there is a Stored XSS via Product Type names. The name is not sanitized when displayed in user permissions settings. The vulnerable input (source) is in Commerce (Product Type settings), but the sink is in CMS user permissions settings. This issue has been patched in versions 4.10.1 and 5.5.2.	N/A	More Details
CVE-2025-62601	Fast DDS is a C++ implementation of the DDS (Data Distribution Service) standard of the OMG (Object Management Group). Prior to versions 3.4.1, 3.3.1, and 2.6.11, when the security mode is enabled, modifying the DATA Submessage within an SPDP packet sent by a publisher causes a heap buffer overflow, resulting in remote termination of Fast-DDS. If the fields of `PID_IDENTITY_TOKEN` or `PID_PERMISSIONS_TOKEN` in the DATA Submessage — specifically by tampering with the `str_size` value read by `readString` (called from `readBinaryProperty`) — are modified, a 32-bit integer overflow can occur, causing `std::vector::resize` to use an attacker-controlled size and quickly trigger heap buffer overflow and remote process term ination. Versions 3.4.1, 3.3.1, and 2.6.11 patch the issue.	N/A	More Details
CVE-2026-25483	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored XSS vulnerability exists in Craft Commerce’s Order Status History Message. The message is rendered using the |md filter, which permits raw HTML, enabling malicious script execution. If a user has database backup utility permissions (which do not require an elevated session), an attacker can exfiltrate the entire database, including all user credentials, customer PII, order history, and 2FA recovery codes. This issue has been patched in versions 4.10.1 and 5.5.2.	N/A	More Details
CVE-2025-62602	Fast DDS is a C++ implementation of the DDS (Data Distribution Service) standard of the OMG (Object Management Group). Prior to versions 3.4.1, 3.3.1, and 2.6.11, when the security mode is enabled, modifying the DATA Submessage within an SPDP packet sent by a publisher causes a heap buffer overflow, resulting in remote termination of Fast-DDS. If the fields of `PID_IDENTITY_TOKEN` or `PID_PERMISSIONS_TOKEN` in the DATA Submessage are tampered with — specially `readOctetVector` reads an unchecked `vecsize` that is propagated unchanged into `readData` as the `length` parameter — the attacker-contro lled `vecsize` can trigger a 32-bit integer overflow during the `length` calculation. That overflow can cause large alloca tion attempt that quickly leads to OOM, enabling a remotely-triggerable denial-of-service and remote process termination. Versions 3.4.1, 3.3.1, and 2.6.11 patch the issue.	N/A	More Details
CVE-2026-25482	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored DOM XSS vulnerability exists in the "Recent Orders" dashboard widget. The Order Status Name is rendered via JavaScript string concatenation without proper escaping, allowing script execution when any admin visits the dashboard. This issue has been patched in versions 4.10.1 and 5.5.2.	N/A	More Details
CVE-	PEAR is a framework and distribution system for reusable PHP components. Prior to		More

2026-25236	version 1.33.0, a SQL injection risk exists in karma queries due to unsafe literal substitution for an IN (...) list. This issue has been patched in version 1.33.0.	N/A	Details
CVE-2025-62799	Fast DDS is a C++ implementation of the DDS (Data Distribution Service) standard of the OMG (Object Management Group). Prior to versions 3.4.1, 3.3.1, and 2.6.11, a heap buffer overflow exists in the Fast-DDS DATA_FRAG receive path. An un authenticated sender can transmit a single malformed RTPS DATA_FRAG packet where `fragmentSize` and `sampleSize` are craft ed to violate internal assumptions. Due to a 4-byte alignment step during fragment metadata initialization, the code write s past the end of the allocated payload buffer, causing immediate crash (DoS) and potentially enabling memory corruption (RCE risk). Versions 3.4.1, 3.3.1, and 2.6.11 patch the issue.	N/A	More Details
CVE-2026-25241	PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, an unauthenticated SQL injection in the /get/<package>/<version> endpoint allows remote attackers to execute arbitrary SQL via a crafted package version. This issue has been patched in version 1.33.0.	N/A	More Details
CVE-2026-25240	PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, a SQL injection vulnerability can occur in user::maintains() when role filters are provided as an array and interpolated into an IN (...) clause. This issue has been patched in version 1.33.0.	N/A	More Details
CVE-2026-25239	PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, a SQL injection vulnerability in apidoc queue insertion can allow query manipulation if an attacker can influence the inserted filename value. This issue has been patched in version 1.33.0.	N/A	More Details
CVE-2025-64098	Fast DDS is a C++ implementation of the DDS (Data Distribution Service) standard of the OMG (Object Management Group). Prior to versions 3.4.1, 3.3.1, and 2.6.11, when the security mode is enabled, modifying the DATA Submessage within an SPDP packet sent by a publisher causes an Out-Of-Memory (OOM) condition, resulting in remote termination of Fast-DDS. If t he fields of `PID_IDENTITY_TOKEN` or `PID_PERMISSIONS_TOKEN` in the DATA Submessage are tampered with — specifically by ta mpering with the the `vecsize` value read by `readOctetVector` — a 32-bit integer overflow can occur, causing `std::vector ::resize` to request an attacker-controlled size and quickly trigger OOM and remote process termination. Versions 3.4.1, 3 .3.1, and 2.6.11 patch the issue.	N/A	More Details
CVE-2025-64438	Fast DDS is a C++ implementation of the DDS (Data Distribution Service) standard of the OMG (Object Management Group). Prior to versions 3.4.1, 3.3.1, and 2.6.11, a remotely triggerable Out-of-Memory (OOM) denial-of-service exists in Fast -DDS when processing RTPS GAP submessages under RELIABLE QoS. By sending a tiny GAP packet with a huge gap range (`gapList .base - gapStart`), an attacker drives `StatefulReader::processGapMsg()` into an unbounded loop that inserts millions of s equence numbers into `WriterProxy::changes_received_` (`std::set`), causing multi-GB heap growth and process termination. No authentication is required beyond network reachability to the reader on the DDS domain. In environments without an RSS limit (non-ASan / unlimited), memory consumption was observed to rise to ~64 GB. Versions 3.4.1, 3.3.1, and 2.6.11 patch t he issue.	N/A	More Details
CVE-2026-25238	PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, a SQL injection vulnerability in bug subscription deletion may allow attackers to inject SQL via a crafted email value. This issue has been patched in version 1.33.0.	N/A	More Details
CVE-2026-1846	Rejected reason: loading template...	N/A	More Details
CVE-2026-	PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, use of preg_replace() with the /e modifier in bug update email handling can enable PHP code execution if attacker-controlled content reaches the evaluated	N/A	More Details

25237	replacement. This issue has been patched in version 1.33.0.		
CVE-2026-22228	An authenticated user with high privileges may trigger a denial-of-service condition in TP-Link Archer BE230 v1.2 by restoring a crafted configuration file containing an excessively long parameter. Restoring such a file can cause the device to become unresponsive, requiring a reboot to restore normal operation. This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	N/A	More Details
CVE-2025-71179	Creativeitem Academy LMS 7.0 contains reflected Cross-Site Scripting (XSS) vulnerabilities via the search parameter to the /academy/blogs endpoint, and the string parameter to the /academy/course_bundles/search/query endpoint. These vulnerabilities are distinct from the patch for CVE-2023-4119, which only fixed XSS in query and sort_by parameters to the /academy/home/courses endpoint.	N/A	More Details
CVE-2020-37084	School ERP Pro 1.0 contains a remote code execution vulnerability that allows authenticated admin users to upload arbitrary PHP files as profile photos by bypassing file extension checks. Attackers can exploit improper file validation in pre-editstudent.inc.php to execute arbitrary code on the server.	N/A	More Details
CVE-2025-58348	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 2200, 1330, 1380, 1480, 1580, W920, W930, and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/confg_tspec write operation, leading to kernel memory exhaustion.	N/A	More Details
CVE-2025-65924	ERPNext thru 15.88.1 does not sanitize or remove certain HTML tags specifically `<a>` hyperlinks in fields that are intended for plain text. Although JavaScript is blocked (preventing XSS), the HTML is still preserved in the generated PDF document. As a result, an attacker can inject malicious clickable links into an ERP-generated PDF. Since PDF files generated by the ERP system are generally considered trustworthy, users are highly likely to click these links, potentially enabling phishing attacks or malware delivery. This issue occurs in the Add Quality Goal' function.	N/A	More Details
CVE-2025-65923	A Stored Cross-Site Scripting (XSS) vulnerability was discovered within the CSV import mechanism of ERPNext thru 15.88.1 when using the Update Existing Recordsoption. An attacker can embed malicious JavaScript code into a CSV field, which is then stored in the database and executed whenever the affected record is viewed by a user within the ERPNext web interface. This exposure may allow an attacker to compromise user sessions or perform unauthorized actions under the context of a victim's account.	N/A	More Details
CVE-2025-63624	SQL Injection vulnerability in Shandong Kede Electronics Co., Ltd IoT smart water meter monitoring platform v.1.0 allows a remote attacker to execute arbitrary code via the imei_list.aspx file.	N/A	More Details
CVE-2026-24887	Claude Code is an agentic coding tool. Prior to version 2.0.72, due to an error in command parsing, it was possible to bypass the Claude Code confirmation prompt to trigger execution of untrusted commands through the find command. Reliably exploiting this required the ability to add untrusted content into a Claude Code context window. This issue has been patched in version 2.0.72.	N/A	More Details
CVE-2025-63372	Articentgroup Zip Rar Extractor Tool 1.345.93.0 is vulnerable to Directory Traversal. The vulnerability resides in the ZIP file processing component, specifically in the functionality responsible for extracting and handling ZIP archive contents.	N/A	More Details
CVE-2025-62599	Fast DDS is a C++ implementation of the DDS (Data Distribution Service) standard of the OMG (Object Management Group). Prior to versions 3.4.1, 3.3.1, and 2.6.11, when the security mode is enabled, modifying the DATA Submessage within an SPDP packet sent by a publisher causes an Out-Of-Memory (OOM) condition, resulting in remote termination of Fast-DDS. If t he fields of PID_IDENTITY_TOKEN or PID_PERMISSION_TOKEN in the DATA Submessage — specifically by tampering with the length field in readPropertySeq — are modified, an integer overflow occurs, leading to an OOM during the resize operation. Versi ons 3.4.1, 3.3.1, and 2.6.11 patch the issue.	N/A	More Details

CVE-2025-61506	An issue was discovered in MediaCrush thru 1.0.1 allowing remote unauthenticated attackers to upload arbitrary files of any size to the /upload endpoint.	N/A	More Details
CVE-2025-60865	Insecure Permissions vulnerability in avanquest Driver Updater v.9.1.57803.1174 allows a local attacker to escalate privileges via the Driver Updater Service windows component.	N/A	More Details
CVE-2025-59439	An issue was discovered in Samsung Modem Exynos through 2025-08-29. Incorrect handling of NAS Registration messages leads to a Denial of Service because of Improper Handling of Exceptional Conditions.	N/A	More Details
CVE-2025-58347	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 2200, 1330, 1380, 1480, 1580, W920, W930, and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/p2p_certif write operation, leading to kernel memory exhaustion.	N/A	More Details
CVE-2025-67186	TOTOLINK A950RG V4.1.2cu.5204_B20210112 contains a buffer overflow vulnerability in the setUrlFilterRules interface of /lib/cste_modules/firewall.so. The vulnerability occurs because the `url` 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.	N/A	More Details
CVE-2025-58346	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 2200, 1330, 1380, 1480, 1580, W920, W930, and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/send_addts write operation, leading to kernel memory exhaustion.	N/A	More Details
CVE-2025-58345	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 2200, 1330, 1380, 1480, 1580, W920, W930, and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/ap_certif_11ax_mode write operation, leading to kernel memory exhaustion.	N/A	More Details
CVE-2025-58344	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 2200, 1330, 1380, 1480, 1580, W920, W930, and W1000. There is unbounded memory allocation in a /proc/driver/unifi0/conn_log_event_burst_to_us write operation, leading to kernel memory exhaustion.	N/A	More Details
CVE-2025-58343	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 2200, 1330, 1380, 1480, 1580, W920, W930, and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/create_tspec write operation, leading to kernel memory exhaustion.	N/A	More Details
CVE-2025-58342	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 2200, 1330, 1380, 1480, 1580, W920, W930, and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/uapsd write operation, leading to kernel memory exhaustion.	N/A	More Details
CVE-2025-58341	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 2200, 1330, 1380, 1480, 1580, W920, W930, and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/ap_cert_disable_ht_vht write operation, leading to kernel memory exhaustion.	N/A	More Details
CVE-2025-58340	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 2200, 1330, 1380, 1480, 1580, W920, W930, and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/send_delts write operation, leading to kernel memory exhaustion.	N/A	More Details
	YouDataSum CPAS Audit Management System <=v4.9 is vulnerable to SQL Injection in		

CVE-2025-57529	/cpasList/findArchiveReportByDah due to insufficient input validation. This allows remote unauthenticated attackers to execute arbitrary SQL commands via crafted input to the parameter. Successful exploitation could lead to unauthorized data access	N/A	More Details
CVE-2025-46651	Tiny File Manager through 2.6 contains a server-side request forgery (SSRF) vulnerability in the URL upload feature. Due to insufficient validation of user-supplied URLs, an attacker can send crafted requests to localhost by using http://www.127.0.0.1.example.com/ or a similarly constructed domain name. This may lead to unauthorized port scanning or access to internal-only services.	N/A	More Details
CVE-2025-66374	CyberArk Endpoint Privilege Manager Agent through 25.10.0 allows a local user to achieve privilege escalation through policy elevation of an Administration task.	N/A	More Details
CVE-2025-67187	A stack-based buffer overflow vulnerability was identified in TOTOLINK A950RG V4.1.2cu.5204_B20210112. The flaw exists in the setIpQosRules interface of /lib/cste_modules/firewall.so where the comment parameter is not properly validated for length.	N/A	More Details
CVE-2025-70849	Arbitrary File Upload in podinfo thru 6.9.0 allows unauthenticated attackers to upload arbitrary files via crafted POST request to the /store endpoint. The application renders uploaded content without a restrictive Content-Security-Policy (CSP) or adequate Content-Type validation, leading to Stored Cross-Site Scripting (XSS).	N/A	More Details
CVE-2025-69971	FUXA v1.2.7 contains a hard-coded credential vulnerability in server/api/jwt-helper.js. The application uses a hard-coded secret key to sign and verify JWT Tokens. This allows remote attackers to forge valid admin tokens and bypass authentication to gain full administrative access.	N/A	More Details
CVE-2025-70758	chetans9 core-php-admin-panel through commit a94a780d6 contains an authentication bypass vulnerability in includes/auth_validate.php. The application sends an HTTP redirect via header(Location:login.php) when a user is not authenticated but fails to call exit() afterward. This allows remote unauthenticated attackers to access protected pages.customer database.	N/A	More Details
CVE-2025-70560	Boltz 2.0.0 contains an insecure deserialization vulnerability in its molecule loading functionality. The application uses Python pickle to deserialize molecule data files without validation. An attacker with the ability to place a malicious pickle file in a directory processed by boltz can achieve arbitrary code execution when the file is loaded.	N/A	More Details
CVE-2025-70559	pdfminer.six before 20251230 contains an insecure deserialization vulnerability in the CMap loading mechanism. The library uses Python pickle to deserialize CMap cache files without validation. An attacker with the ability to place a malicious pickle file in a location accessible to the application can trigger arbitrary code execution or privilege escalation when the file is loaded by a trusted process. This is caused by an incomplete patch to CVE-2025-64512.	N/A	More Details
CVE-2025-70311	JEEWMS 1.0 is vulnerable to SQL Injection. Attackers can inject malicious SQL statements through the id1 and id2 parameters in the /systemControl.do interface for attack.	N/A	More Details
CVE-2025-69983	FUXA v1.2.7 allows Remote Code Execution (RCE) via the project import functionality. The application does not properly sanitize or sandbox user-supplied scripts within imported project files. An attacker can upload a malicious project containing system commands, leading to full system compromise.	N/A	More Details
CVE-2025-69981	FUXA v1.2.7 contains an Unrestricted File Upload vulnerability in the `/api/upload` API endpoint. The endpoint lacks authentication mechanisms, allowing unauthenticated remote attackers to upload arbitrary files. This can be exploited to overwrite critical system files (such as the SQLite user database) to gain administrative access, or to upload malicious scripts to execute arbitrary code.	N/A	More Details

CVE-2026-1341	Avation Light Engine Pro exposes its configuration and control interface without any authentication or access control.	N/A	More Details
CVE-2026-25148	Qwik is a performance focused javascript framework. Prior to version 1.19.0, a Cross-Site Scripting vulnerability in Qwik.js' server-side rendering virtual attribute serialization allows a remote attacker to inject arbitrary web scripts into server-rendered pages via virtual attributes. Successful exploitation permits script execution in a victim's browser in the context of the affected origin. This issue has been patched in version 1.19.0.	N/A	More Details
CVE-2026-25149	Qwik is a performance focused javascript framework. Prior to version 1.19.0, an Open Redirect vulnerability in Qwik City's default request handler middleware allows a remote attacker to redirect users to arbitrary protocol-relative URLs. Successful exploitation permits attackers to craft convincing phishing links that appear to originate from the trusted domain but redirect the victim to an attacker-controlled site. This issue has been patched in version 1.19.0.	N/A	More Details
CVE-2025-69970	FUXA v1.2.7 contains an insecure default configuration vulnerability in server/settings.default.js. The 'secureEnabled' flag is commented out by default, causing the application to initialize with authentication disabled. This allows unauthenticated remote attackers to access sensitive API endpoints, modify projects, and control industrial equipment immediately after installation.	N/A	More Details
CVE-2025-67188	A buffer overflow vulnerability exists in TOTOLINK A950RG V4.1.2cu.5204_B20210112. The issue resides in the setRadvdCfg interface of the /lib/cste_modules/ipv6.so module. The function fails to properly validate the length of the user-controlled radvdinterfacename parameter, allowing remote attackers to trigger a stack buffer overflow.	N/A	More Details
CVE-2026-25490	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored XSS vulnerability in Craft Commerce allows attackers to execute malicious JavaScript in an administrator’s browser. This occurs because the 'Address Line 1' field in Inventory Locations is not properly sanitized before being displayed in the admin panel. This issue has been patched in versions 4.10.1 and 5.5.2.	N/A	More Details
CVE-2025-69875	A vulnerability exists in Quick Heal Total Security 23.0.0 in the quarantine management component where insufficient validation of restore paths and improper permission handling allow a low-privileged local user to restore quarantined files into protected system directories. This behavior can be abused by a local attacker to place files in high-privilege locations, potentially leading to privilege escalation.	N/A	More Details
CVE-2025-69848	NetBox is an open-source infrastructure resource modeling and IP address management platform. A reflected cross-site scripting (XSS) vulnerability exists in versions 2.11.0 through 3.7.x in the ProtectedError handling logic, where object names are included in HTML error messages without proper escaping. This allows user-controlled content to be rendered in the web interface when a delete operation fails due to protected relationships, potentially enabling execution of arbitrary client-side code in the context of a privileged user.	N/A	More Details
CVE-2025-69431	The ZSPACE Q2C NAS contains a vulnerability related to incorrect symbolic link following. Attackers can format a USB drive to ext4, create a symbolic link to its root directory, insert the drive into the NAS device's slot, and then access the USB drive's directory mounted on the NAS using the Samba protocol. This allows them to obtain all files within the NAS system and tamper with those files.	N/A	More Details
CVE-2025-69430	An Incorrect Symlink Follow vulnerability exists in multiple Yottamaster NAS devices, including DM2 (version equal to or prior to V1.9.12), DM3 (version equal to or prior to V1.9.12), and DM200 (version equal to or prior to V1.2.23) that could be exploited by attackers to leak or tamper with the internal file system. Attackers can format a USB drive to ext4, create a symbolic link to its root directory, insert the drive into the NAS device's slot, then access the USB drive's symlink directory mounted on the NAS to	N/A	More Details

	obtain all files within the NAS system and tamper with those files.		
CVE-2026-24052	Claude Code is an agentic coding tool. Prior to version 1.0.111, Claude Code contained insufficient URL validation in its trusted domain verification mechanism for WebFetch requests. The application used a startsWith() function to validate trusted domains (e.g., docs.python.org, modelcontextprotocol.io), this could have enabled attackers to register domains like modelcontextprotocol.io.example.com that would pass validation. This could enable automatic requests to attacker-controlled domains without user consent, potentially leading to data exfiltration. This issue has been patched in version 1.0.111.	N/A	More Details
CVE-2026-24053	Claude Code is an agentic coding tool. Prior to version 2.0.74, due to a Bash command validation flaw in parsing ZSH clobber syntax, it was possible to bypass directory restrictions and write files outside the current working directory without user permission prompts. Exploiting this required the user to use ZSH and the ability to add untrusted content into a Claude Code context window. This issue has been patched in version 2.0.74.	N/A	More Details
CVE-2025-69429	The ORICO NAS CD3510 (version V1.9.12 and below) contains an Incorrect Symlink Follow vulnerability that could be exploited by attackers to leak or tamper with the internal file system. Attackers can format a USB drive to ext4, create a symbolic link to its root directory, insert the drive into the NAS device's slot, then access the USB drive's symlink directory mounted on the NAS to obtain all files within the NAS system and tamper with those files.	N/A	More Details
CVE-2025-67189	A buffer overflow vulnerability exists in the setParentalRules interface of TOTOLINK A950RG V4.1.2cu.5204_B20210112. The urlKeyword parameter is not properly validated, and the function concatenates multiple user-controlled fields into a fixed-size stack buffer without performing boundary checks. A remote attacker can exploit this flaw to cause denial of service or potentially achieve arbitrary code execution.	N/A	More Details
CVE-2025-58455	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted network packet whose length exceeds the maximum expected value.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	N/A	More Details
CVE-2025-54373	OpenEMR is a free and open source electronic health records and medical practice management application. Versions prior to 7.0.4 have a vulnerability where sensitive data is unintentionally revealed to unauthorized parties. Contents of Clinical Notes and Care Plan, where an encounter has Sensitivity=high, can be viewed and changed by users who do not have Sensitivities=high privilege. Version 7.0.4 fixes the issue.	N/A	More Details
CVE-2026-1664	Summary An Insecure Direct Object Reference has been found to exist in `createHeaderBasedEmailResolver()` function within the Cloudflare Agents SDK. The issue occurs because the `Message-ID` and `References` headers are parsed to derive the target agentName and agentId without proper validation or origin checks, allowing an external attacker with control of these headers to route inbound mail to arbitrary Durable Object instances and namespaces . Root cause The `createHeaderBasedEmailResolver()` function lacks cryptographic verification or origin validation for the headers used in the routing logic, effectively allowing external input to dictate internal object routing. Impact Insecure Direct Object Reference (IDOR) in email routing lets an attacker steer inbound mail to arbitrary Agent instances via spoofed Message-ID. Mitigation: * PR: https://github.com/cloudflare/agents/blob/main/docs/email.md] provides the necessary architectural context for coding agents to mitigate the issue by refactoring the resolver to enforce strict identity boundaries. * Agents-sdk users should upgrade to agents@0.3.7	N/A	More Details
CVE-2025-	Johnson Controls Metasys component listed below have Improper Neutralization of Special Elements used in a Command (Command Injection) Vulnerability . Successful exploitation of this vulnerability could allow remote SQL execution This issue affects * Metasys: Application and Data Server (ADS) installed with SQL Express deployed as part of the Metasys 14.1 and prior installation, * Extended Application and Data Server (ADX) installed with SQL Express deployed as part of the Metasys 14.1 installation, * LCS8500	N/A	More

26385	or NAE8500 installed with SQL Express deployed as part of the Metasys installation Releases 12.0 through 14.1, * System Configuration Tool (SCT) installed with SQL Express deployed as part of the SCT installation 17.1 and prior, * Controller Configuration Tool (CCT) installed with SQL Express deployed as part of the CCT installation 17.0 and prior.		Details
CVE-2026-1723	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in TOTOLINK X6000R allows OS Command Injection.This issue affects X6000R: through V9.4.0cu.1498_B20250826.	N/A	More Details
CVE-2025-24293	# Active Storage allowed transformation methods potentially unsafe Active Storage attempts to prevent the use of potentially unsafe image transformation methods and parameters by default. The default allowed list contains three methods allow for the circumvention of the safe defaults which enables potential command injection vulnerabilities in cases where arbitrary user supplied input is accepted as valid transformation methods or parameters. Impact ------ This vulnerability impacts applications that use Active Storage with the image_processing processing gem in addition to mini_magick as the image processor. Vulnerable code will look something similar to this: ``` <%= image_tag blob.variant(params[:t] => params[:v]) %> ``` Where the transformation method or its arguments are untrusted arbitrary input. All users running an affected release should either upgrade or use one of the workarounds immediately. Workarounds ---------- Consuming user supplied input for image transformation methods or their parameters is unsupported behavior and should be considered dangerous. Strict validation of user supplied methods and parameters should be performed as well as having a strong [ImageMagick security policy](https://imagemagick.org/script/security-policy.php) deployed. Credits ------- Thank you [lio346](https://hackerone.com/lio346) for reporting this!	N/A	More Details
CVE-2026-23835	LobeHub is an open source human-and-AI-agent network. Prior to version 1.143.3, the file upload feature in `Knowledge Base > File Upload` does not validate the integrity of the upload request, allowing users to intercept and modify the request parameters. As a result, it is possible to create arbitrary files in abnormal or unintended paths. In addition, since `lobechat.com` relies on the size parameter from the request to calculate file usage, an attacker can manipulate this value to misrepresent the actual file size, such as uploading a `1 GB` file while reporting it as `10 MB`, or falsely declaring a `10 MB` file as a `1 GB` file. By manipulating the size value provided in the client upload request, it is possible to bypass the monthly upload quota enforced by the server and continuously upload files beyond the intended storage and traffic limits. This abuse can result in a discrepancy between actual resource consumption and billing calculations, causing direct financial impact to the service operator. Additionally, exhaustion of storage or related resources may lead to degraded service availability, including failed uploads, delayed content delivery, or temporary suspension of upload functionality for legitimate users. A single malicious user can also negatively affect other users or projects sharing the same subscription plan, effectively causing an indirect denial of service (DoS). Furthermore, excessive and unaccounted-for uploads can distort monitoring metrics and overload downstream systems such as backup processes, malware scanning, and media processing pipelines, ultimately undermining overall operational stability and service reliability. Version 1.143.3 contains a patch for the issue.	N/A	More Details
CVE-2025-11175	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') vulnerability in The Wikimedia Foundation Mediawiki - DiscussionTools Extension allows Regular Expression Exponential Blowup.This issue affects Mediawiki - DiscussionTools Extension: 1.44, 1.43.	N/A	More Details
CVE-2024-9432	Cleartext Storage of Sensitive Information vulnerability in OpenText™ Vertica allows Retrieve Embedded Sensitive Data. The vulnerability could read Vertica agent plaintext apikey.This issue affects Vertica versions: 23.X, 24.X, 25.X.	N/A	More Details
CVE-2025-	Insufficient epoch key slot processing in OpenVPN 2.7_alpha1 through 2.7_rc5 allows remote authenticated users to trigger an assert resulting in a denial of service	N/A	More Details

15497			
CVE-2026-25050	Vendure is an open-source headless commerce platform. Prior to version 3.5.3, the `NativeAuthenticationStrategy.authenticate()` method is vulnerable to a timing attack that allows attackers to enumerate valid usernames (email addresses). In `packages/core/src/config/auth/native-authentication-strategy.ts`, the authenticate method returns immediately if a user is not found. The significant timing difference (~200-400ms for bcrypt vs ~1-5ms for DB miss) allows attackers to reliably distinguish between existing and non-existing accounts. Version 3.5.3 fixes the issue.	N/A	More Details
CVE-2026-24855	ChurchCRM is an open-source church management system. Versions prior to 6.7.2 have a Stored Cross-Site Scripting (XSS) vulnerability occurs in Create Events in Church Calendar. Users with low privileges can create XSS payloads in the Description field. This payload is stored in the database, and when other users view that event (including the admin), the payload is triggered, leading to account takeover. Version 6.7.2 fixes the vulnerability.	N/A	More Details
CVE-2025-7964	After receiving a malformed 802.15.4 MAC Data Request the Zigbee Coordinator sends a ‘network leave’ request to Zigbee router resulting in the Zigbee Router getting stuck in a non-rejoinable state. If a suitable parent is not available, the end devices will be unable to rejoin. A manual recommissioning is required to recover the Zigbee Router.	N/A	More Details
CVE-2025-6723	Chef InSpec up to version 5.23 creates named pipes with overly permissive default Windows access controls. A local attacker may interfere with the pipe connection process and exploit the insufficient access restrictions to assume the InSpec execution context, potentially resulting in elevated privileges or operational disruption. This issue affects Chef Inspec: through 5.23.	N/A	More Details
CVE-2026-1498	An LDAP Injection vulnerability in WatchGuard Fireware OS may allow a remote unauthenticated attacker to retrieve sensitive information from a connected LDAP authentication server through an exposed authentication or management web interface. This vulnerability may also allow a remote attacker to authenticate as an LDAP user with a partial identifier if they additionally have that user's valid passphrase.This issue affects Fireware OS: from 12.0 through 12.11.6, from 12.5 through 12.5.15, from 2025.1 through 2026.0.	N/A	More Details
CVE-2025-13176	Planting a custom configuration file in ESET Inspect Connector allow load a malicious DLL.	N/A	More Details
CVE-2026-1680	Improper access control in the WCF endpoint in Edgemo (now owned by Danoffice IT) Local Admin Service 1.2.7.23180 on Windows allows a local user to escalate their privileges to local administrator via direct communication with the LocalAdminService.exe named pipe, bypassing client-side group membership restrictions.	N/A	More Details
CVE-2025-71180	In the Linux kernel, the following vulnerability has been resolved: counter: interrupt-cnt: Drop IRQF_NO_THREAD flag An IRQ handler can either be IRQF_NO_THREAD or acquire spinlock_t, as CONFIG_PROVE_RAW_LOCK_NESTING warns: ============================= [BUG: Invalid wait context] 6.18.0-rc1+git... #1 ----------------------------- some-user-space-process/1251 is trying to lock: (&counter->events_list_lock){....}-{3:3}, at: counter_push_event [counter] other info that might help us debug this: context-{2:2} no locks held by some-user-space-process/.... stack backtrace: CPU: 0 UID: 0 PID: 1251 Comm: some-user-space-process 6.18.0-rc1+git... #1 PREEMPT Call trace: show_stack (C) dump_stack_lvl dump_stack __lock_acquire lock_acquire _raw_spin_lock_irqsave counter_push_event [counter] interrupt_cnt_isr [interrupt_cnt] __handle_irq_event_percpu handle_irq_event handle_simple_irq handle_irq_desc generic_handle_domain_irq gpio_irq_handler handle_irq_desc generic_handle_domain_irq gic_handle_irq call_on_irq_stack do_interrupt_handler el0_interrupt __el0_irq_handler_common el0t_64_irq_handler el0t_64_irq ... and Sebastian correctly points out. Remove IRQF_NO_THREAD as an alternative to switching to raw_spinlock_t, because the latter would limit all potential nested locks to raw_spinlock_t only.	N/A	More Details

CVE-2026-25097	Rejected reason: Not used	N/A	More Details
CVE-2026-25096	Rejected reason: Not used	N/A	More Details
CVE-2026-25095	Rejected reason: Not used	N/A	More Details
CVE-2026-25094	Rejected reason: Not used	N/A	More Details
CVE-2026-25093	Rejected reason: Not used	N/A	More Details
CVE-2026-25092	Rejected reason: Not used	N/A	More Details
CVE-2026-25091	Rejected reason: Not used	N/A	More Details
CVE-2026-25090	Rejected reason: Not used	N/A	More Details
CVE-2026-24729	An unrestricted upload of file with dangerous type vulnerability in the file upload function of Interinfo DreamMaker versions before 2025/10/22 allows remote attackers to execute arbitrary system commands via a malicious class file.	N/A	More Details
CVE-2026-24728	A missing authentication for critical function vulnerability in the /servlet/baServer3 endpoint of Interinfo DreamMaker versions before 2025/10/22 allows remote attackers to access exposed administrative functionality without prior authentication.	N/A	More Details
CVE-2026-24714	Some end of service NETGEAR products provide "TelnetEnable" functionality, which allows a magic packet to activate telnet service on the box.	N/A	More Details
CVE-2026-1665	A command injection vulnerability exists in nvm (Node Version Manager) versions 0.40.3 and below. The nvm_download() function uses eval to execute wget commands, and the NVM_AUTH_HEADER environment variable was not sanitized in the wget code path (though it was sanitized in the curl code path). An attacker who can set environment variables in a victim's shell environment (e.g., via malicious CI/CD configurations, compromised dotfiles, or Docker images) can inject arbitrary shell commands that execute when the victim runs nvm commands that trigger downloads, such as 'nvm install' or 'nvm ls-remote'.	N/A	More Details
CVE-2026-25141	Orval generates type-safe JS clients (TypeScript) from any valid OpenAPI v3 or Swagger v2 specification. Versions starting with 7.19.0 and prior to 7.21.0 and 8.2.0 have an incomplete fix for CVE-2026-23947. While the jsStringEscape function properly handles single quotes ('), double quotes (") and so on, it is still possible to achieve code injection using only a limited set of characters that are currently not escaped. The vulnerability lies in the fact that the application can be forced to execute arbitrary JavaScript using characters such as []()!+. By using a technique known as JSFuck, an attacker can bypass the current sanitization logic and run arbitrary code without needing any alphanumeric characters or quotes. Version 7.21.0 and 8.2.0 contain an updated fix.	N/A	More Details

CVE-2025-71181	In the Linux kernel, the following vulnerability has been resolved: rust_binder: remove spin_lock() in rust_shrink_free_page() When forward-porting Rust Binder to 6.18, I neglected to take commit fb56fdf8b9a2 ("mm/list_lru: split the lock to per-cgroup scope") into account, and apparently I did not end up running the shrinker callback when I sanity tested the driver before submission. This leads to crashes like the following: == WARNING: possible recursive locking detected 6.18.0-mainline-maybe-dirty #1 Tainted: G IO ---------- ---------- kswapd0/68 is trying to acquire lock: ffff956000fa18b0 (&l->lock){+.+.}-{2:2}, at: lock_list_lru_of_memcg+0x128/0x230 but task is already holding lock: ffff956000fa18b0 (&l->lock){+.+.}-{2:2}, at: rust_helper_spin_lock+0xd/0x20 other info that might help us debug this: Possible unsafe locking scenario: CPU0 ---- lock(&l->lock); lock(&l->lock); *** DEADLOCK *** May be due to missing lock nesting notation 3 locks held by kswapd0/68: #0: ffffffff90d2e260 (fs_reclaim){+.+.}-{0:0}, at: kswapd+0x597/0x1160 #1: ffff956000fa18b0 (&l->lock){+.+.}-{2:2}, at: rust_helper_spin_lock+0xd/0x20 #2: ffffffff90cf3680 (rcu_read_lock){....}-{1:2}, at: lock_list_lru_of_memcg+0x2d/0x230 To fix this, remove the spin_lock() call from rust_shrink_free_page().	N/A	More Details
CVE-2026-25063	gradle-completion provides Bash and Zsh completion support for Gradle. A command injection vulnerability was found in gradle-completion up to and including 9.3.0 that allows arbitrary code execution when a user triggers Bash tab completion in a project containing a malicious Gradle build file. The `gradle-completion` script for Bash fails to adequately sanitize Gradle task names and task descriptions, allowing command injection via a malicious Gradle build file when the user completes a command in Bash (without them explicitly running any task in the build). For example, given a task description that includes a string between backticks, then that string would be evaluated as a command when presenting the task description in the completion list. While task execution is the core feature of Gradle, this inherent execution may lead to unexpected outcomes. The vulnerability does not affect zsh completion. The first patched version is 9.3.1. As a workaround, it is possible and effective to temporarily disable bash completion for Gradle by removing `gradle-completion` from `.bashrc` or `.bash_profile`.	N/A	More Details
CVE-2026-23019	In the Linux kernel, the following vulnerability has been resolved: net: marvell: prestera: fix NULL dereference on devlink_alloc() failure devlink_alloc() may return NULL on allocation failure, but prestera_devlink_alloc() unconditionally calls devlink_priv() on the returned pointer. This leads to a NULL pointer dereference if devlink allocation fails. Add a check for a NULL devlink pointer and return NULL early to avoid the crash.	N/A	More Details
CVE-2026-23031	In the Linux kernel, the following vulnerability has been resolved: can: gs_usb: gs_usb_receive_bulk_callback(): fix URB memory leak In gs_can_open(), the URBs for USB-in transfers are allocated, added to the parent->rx_submitted anchor and submitted. In the complete callback gs_usb_receive_bulk_callback(), the URB is processed and resubmitted. In gs_can_close() the URBs are freed by calling usb_kill_anchored_urbs(parent->rx_submitted). However, this does not take into account that the USB framework unanchors the URB before the complete function is called. This means that once an in-URB has been completed, it is no longer anchored and is ultimately not released in gs_can_close(). Fix the memory leak by anchoring the URB in the gs_usb_receive_bulk_callback() to the parent->rx_submitted anchor.	N/A	More Details
CVE-2026-23030	In the Linux kernel, the following vulnerability has been resolved: phy: rockchip: inno-usb2: Fix a double free bug in rockchip_usb2phy_probe() The for_each_available_child_of_node() calls of_node_put() to release child_np in each success loop. After breaking from the loop with the child_np has been released, the code will jump to the put_child label and will call the of_node_put() again if the devm_request_threaded_irq() fails. These cause a double free bug. Fix by returning directly to avoid the duplicate of_node_put().	N/A	More Details
CVE-2026-23029	In the Linux kernel, the following vulnerability has been resolved: LoongArch: KVM: Fix kvm_device leak in kvm_eiointc_destroy() In kvm_ioctl_create_device(), kvm_device has allocated memory, kvm_device->destroy() seems to be supposed to free its kvm_device struct, but kvm_eiointc_destroy() is not currently doing this, that would lead to a memory	N/A	More Details

	leak. So, fix it.		
CVE-2026-23028	In the Linux kernel, the following vulnerability has been resolved: LoongArch: KVM: Fix kvm_device leak in kvm_ipi_destroy() In kvm_ioctl_create_device(), kvm_device has allocated memory, kvm_device->destroy() seems to be supposed to free its kvm_device struct, but kvm_ipi_destroy() is not currently doing this, that would lead to a memory leak. So, fix it.	N/A	More Details
CVE-2026-23027	In the Linux kernel, the following vulnerability has been resolved: LoongArch: KVM: Fix kvm_device leak in kvm_pch_pic_destroy() In kvm_ioctl_create_device(), kvm_device has allocated memory, kvm_device->destroy() seems to be supposed to free its kvm_device struct, but kvm_pch_pic_destroy() is not currently doing this, that would lead to a memory leak. So, fix it.	N/A	More Details
CVE-2026-23026	In the Linux kernel, the following vulnerability has been resolved: dmaengine: qcom: gpi: Fix memory leak in gpi_peripheral_config() Fix a memory leak in gpi_peripheral_config() where the original memory pointed to by gchan->config could be lost if krealloc() fails. The issue occurs when: 1. gchan->config points to previously allocated memory 2. krealloc() fails and returns NULL 3. The function directly assigns NULL to gchan->config, losing the reference to the original memory 4. The original memory becomes unreachable and cannot be freed Fix this by using a temporary variable to hold the krealloc() result and only updating gchan->config when the allocation succeeds. Found via static analysis and code review.	N/A	More Details
CVE-2026-23025	In the Linux kernel, the following vulnerability has been resolved: mm/page_alloc: prevent pcp corruption with SMP=n The kernel test robot has reported: BUG: spinlock trylock failure on UP on CPU#0, kcompactd0/28 lock: 0xffff888807e35ef0, .magic: dead4ead, .owner: kcompactd0/28, .owner_cpu: 0 CPU: 0 UID: 0 PID: 28 Comm: kcompactd0 Not tainted 6.18.0-rc5-00127-ga06157804399 #1 PREEMPT 8cc09ef94dcec767faa911515ce9e609c45db470 Call Trace: <IRQ> __dump_stack (lib/dump_stack.c:95) dump_stack_lvl (lib/dump_stack.c:123) dump_stack (lib/dump_stack.c:130) spin_dump (kernel/locking/spinlock_debug.c:71) do_raw_spin_trylock (kernel/locking/spinlock_debug.c:?) _raw_spin_trylock (include/linux/spinlock_api_smp.h:89 kernel/locking/spinlock.c:138) __free_frozen_pages (mm/page_alloc.c:2973) ___free_pages (mm/page_alloc.c:5295) __free_pages (mm/page_alloc.c:5334) tlb_remove_table_rcu (include/linux/mm.h:? include/linux/mm.h:3122 include/asm-generic/tlb.h:220 mm/mmu_gather.c:227 mm/mmu_gather.c:290) ? __cfi_tlb_remove_table_rcu (mm/mmu_gather.c:289) ? rcu_core (kernel/rcu/tree.c:?) rcu_core (include/linux/rcupdate.h:341 kernel/rcu/tree.c:2607 kernel/rcu/tree.c:2861) rcu_core_si (kernel/rcu/tree.c:2879) handle_softirqs (arch/x86/include/asm/jump_label.h:36 include/trace/events/irq.h:142 kernel/softirq.c:623) __irq_exit_rcu (arch/x86/include/asm/jump_label.h:36 kernel/softirq.c:725) irq_exit_rcu (kernel/softirq.c:741) sysvec_apic_timer_interrupt (arch/x86/kernel/apic/apic.c:1052) </IRQ> <TASK> RIP: 0010:_raw_spin_unlock_irqrestore (arch/x86/include/asm/preempt.h:95 include/linux/spinlock_api_smp.h:152 kernel/locking/spinlock.c:194) free_pcppages_bulk (mm/page_alloc.c:1494) drain_pages_zone (include/linux/spinlock.h:391 mm/page_alloc.c:2632) __drain_all_pages (mm/page_alloc.c:2731) drain_all_pages (mm/page_alloc.c:2747) kcompactd (mm/compaction.c:3115) kthread (kernel/kthread.c:465) ? __cfi_kcompactd (mm/compaction.c:3166) ? __cfi_kthread (kernel/kthread.c:412) ret_from_fork (arch/x86/kernel/process.c:164) ? __cfi_kthread (kernel/kthread.c:412) ret_from_fork_asm (arch/x86/entry/entry_64.S:255) </TASK> Matthew has analyzed the report and identified that in drain_page_zone() we are in a section protected by spin_lock(&pcp->lock) and then get an interrupt that attempts spin_trylock() on the same lock. The code is designed to work this way without disabling IRQs and occasionally fail the trylock with a fallback. However, the SMP=n spinlock implementation assumes spin_trylock() will always succeed, and thus it's normally a no-op. Here the enabled lock debugging catches the problem, but otherwise it could cause a corruption of the pcp structure. The problem has been introduced by commit 574907741599 ("mm/page_alloc: leave IRQs enabled for per-cpu page allocations"). The pcp locking scheme recognizes the need for disabling IRQs to prevent nesting	N/A	More Details

	spin_trylock() sections on SMP=n, but the need to prevent the nesting in spin_lock() has not been recognized. Fix it by introducing local wrappers that change the spin_lock() to spin_lock_iqsave() with SMP=n and use them in all places that do spin_lock(&pcp->lock). [vbabka@suse.cz: add pcp_ prefix to the spin_lock_irqsave wrappers, per Steven]		
CVE-2026-23024	In the Linux kernel, the following vulnerability has been resolved: idpf: fix memory leak of flow steer list on rmmod The flow steering list maintains entries that are added and removed as ethtool creates and deletes flow steering rules. Module removal with active entries causes memory leak as the list is not properly cleaned up. Prevent this by iterating through the remaining entries in the list and freeing the associated memory during module removal. Add a spinlock (flow_steer_list_lock) to protect the list access from multiple threads.	N/A	More Details
CVE-2026-23023	In the Linux kernel, the following vulnerability has been resolved: idpf: fix memory leak in idpf_vport_rel() Free vport->rx_ptype_lkup in idpf_vport_rel() to avoid leaking memory during a reset. Reported by kmemleak: unreferenced object 0xff450acac838a000 (size 4096): comm "kworker/u258:5", pid 7732, jiffies 4296830044 hex dump (first 32 bytes): 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 ..... backtrace (crc 3da81902): __kmalloc_cache_noprof+0x469/0x7a0 idpf_send_get_rx_ptype_msg+0x90/0x570 [idpf] idpf_init_task+0x1ec/0x8d0 [idpf] process_one_work+0x226/0x6d0 worker_thread+0x19e/0x340 kthread+0x10f/0x250 ret_from_fork+0x251/0x2b0 ret_from_fork_asm+0x1a/0x30	N/A	More Details
CVE-2026-23022	In the Linux kernel, the following vulnerability has been resolved: idpf: fix memory leak in idpf_vc_core_deinit() Make sure to free hw->lan_regs. Reported by kmemleak during reset: unreferenced object 0xff1b913d02a936c0 (size 96): comm "kworker/u258:14", pid 2174, jiffies 4294958305 hex dump (first 32 bytes): 00 00 00 c0 a8 ba 2d ff 00 00 00 00 00 00 00 00 ......-..... 00 00 40 08 00 00 00 00 00 00 25 b3 a8 ba 2d ff ..@.....%...-. backtrace (crc 36063c4f): __kmalloc_noprof+0x48f/0x890 idpf_vc_core_init+0x6ce/0x9b0 [idpf] idpf_vc_event_task+0x1fb/0x350 [idpf] process_one_work+0x226/0x6d0 worker_thread+0x19e/0x340 kthread+0x10f/0x250 ret_from_fork+0x251/0x2b0 ret_from_fork_asm+0x1a/0x30	N/A	More Details
CVE-2026-23021	In the Linux kernel, the following vulnerability has been resolved: net: usb: pegasus: fix memory leak in update_eth_regs_async() When asynchronously writing to the device registers and if usb_submit_urb() fail, the code fail to release allocated to this point resources.	N/A	More Details
CVE-2026-23020	In the Linux kernel, the following vulnerability has been resolved: net: 3com: 3c59x: fix possible null dereference in vortex_probe1() pdev can be null and free_ring: can be called in 1297 with a null pdev.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: btrfs: release path before initializing extent tree in btrfs_read_locked_inode() In btrfs_read_locked_inode() we are calling btrfs_init_file_extent_tree() while holding a path with a read locked leaf from a subvolume tree, and btrfs_init_file_extent_tree() may do a GFP_KERNEL allocation, which can trigger reclaim. This can create a circular lock dependency which lockdep warns about with the following splat: [6.1433] == [6.1574] WARNING: possible circular locking dependency detected [6.1583] 6.18.0+ #4 Tainted: G U [6.1591] -- [6.1599] kswapd0/117 is trying to acquire lock: [6.1606] ffff8d9b6333c5b8 (&delayed_node->mutex){+.+.}-{3:3}, at: __btrfs_release_delayed_node.part.0+0x39/0x2f0 [6.1625] but task is already holding lock: [6.1633] ffffffffa4ab8ce0 (fs_reclaim){+.+.}-{0:0}, at: balance_pgdat+0x195/0xc60 [6.1646] which lock already depends on the new lock. [6.1657] the existing dependency chain (in reverse order) is: [6.1667] -> #2 (fs_reclaim){+.+.}-{0:0}: [6.1677] fs_reclaim_acquire+0x9d/0xd0 [6.1685] __kmalloc_cache_noprof+0x59/0x750 [6.1694] btrfs_init_file_extent_tree+0x90/0x100 [6.1702] btrfs_read_locked_inode+0xc3/0x6b0 [6.1710] btrfs_iget+0xbb/0xf0 [6.1716] btrfs_lookup_dentry+0x3c5/0x8e0 [6.1724] btrfs_lookup+0x12/0x30 [6.1731] lookup_open.isra.0+0x1aa/0x6a0 [6.1739] path_openat+0x5f7/0xc60 [6.1746] do_filp_open+0xd6/0x180 [6.1753]		

CVE-2026-23018	do_sys_openat2+0x8b/0xe0 [6.1760] __x64_sys_openat+0x54/0xa0 [6.1768] do_syscall_64+0x97/0x3e0 [6.1776] entry_SYSCALL_64_after_hwframe+0x76/0x7e [6.1784] -> #1 (btrfs-tree-00){++++}-{3:3}: [6.1794] lock_release+0x127/0x2a0 [6.1801] up_read+0x1b/0x30 [6.1808] btrfs_search_slot+0x8e0/0xff0 [6.1817] btrfs_lookup_inode+0x52/0xd0 [6.1825] __btrfs_update_delayed_inode+0x73/0x520 [6.1833] btrfs_commit_inode_delayed_inode+0x11a/0x120 [6.1842] btrfs_log_inode+0x608/0x1aa0 [6.1849] btrfs_log_inode_parent+0x249/0xf80 [6.1857] btrfs_log_dentry_safe+0x3e/0x60 [6.1865] btrfs_sync_file+0x431/0x690 [6.1872] do_fsync+0x39/0x80 [6.1879] __x64_sys_fsync+0x13/0x20 [6.1887] do_syscall_64+0x97/0x3e0 [6.1894] entry_SYSCALL_64_after_hwframe+0x76/0x7e [6.1903] -> #0 (&delayed_node->mutex){+.+.}-{3:3}: [6.1913] __lock_acquire+0x15e9/0x2820 [6.1920] lock_acquire+0xc9/0x2d0 [6.1927] __mutex_lock+0xcc/0x10a0 [6.1934] __btrfs_release_delayed_node.part.0+0x39/0x2f0 [6.1944] btrfs_evict_inode+0x20b/0x4b0 [6.1952] evict+0x15a/0x2f0 [6.1958] prune_icache_sb+0x91/0xd0 [6.1966] super_cache_scan+0x150/0x1d0 [6.1974] do_shrink_slab+0x155/0x6f0 [6.1981] shrink_slab+0x48e/0x890 [6.1988] shrink_one+0x11a/0x1f0 [6.1995] shrink_node+0xbfd/0x1320 [6.1002] balance_pgdat+0x67f/0xc60 [6.1321] kswapd+0x1dc/0x3e0 [6.1643] kthread+0xff/0x240 [6.1965] ret_from_fork+0x223/0x280 [6.1287] ret_from_fork_asm+0x1a/0x30 [6.1616] other info that might help us debug this: [6.1561] Chain exists of: &delayed_node->mutex --> btrfs-tree-00 --> fs_reclaim [6.1503] Possible unsafe locking scenario: [6.1110] CPU0 CPU1 [6.1411] ---- ---- [6.1707] lock(fs_reclaim); [6.1998] lock(btrfs-tree-00); [6.1291] lock(fs_reclaim); [6.1581] lock(&del ---truncated---	N/A	More Details
CVE-2025-71182	In the Linux kernel, the following vulnerability has been resolved: can: j1939: make j1939_session_activate() fail if device is no longer registered syzbot is still reporting unregister_netdevice: waiting for vcan0 to become free. Usage count = 2 even after commit 93a27b5891b8 ("can: j1939: add missing calls in NETDEV_UNREGISTER notification handler") was added. A debug printk() patch found that j1939_session_activate() can succeed even after j1939_cancel_active_session() from j1939_netdev_notify(NETDEV_UNREGISTER) has completed. Since j1939_cancel_active_session() is processed with the session list lock held, checking ndev->reg_state in j1939_session_activate() with the session list lock held can reliably close the race window.	N/A	More Details
CVE-2026-23017	In the Linux kernel, the following vulnerability has been resolved: idpf: fix error handling in the init_task on load If the init_task fails during a driver load, we end up without vports and netdevs, effectively failing the entire process. In that state a subsequent reset will result in a crash as the service task attempts to access uninitialized resources. Following trace is from an error in the init_task where the CREATE_VPORT (op 501) is rejected by the FW: [40922.763136] idpf 0000:83:00.0: Device HW Reset initiated [40924.449797] idpf 0000:83:00.0: Transaction failed (op 501) [40958.148190] idpf 0000:83:00.0: HW reset detected [40958.161202] BUG: kernel NULL pointer dereference, address: 00000000000000a8 ... [40958.168094] Workqueue: idpf-0000:83:00.0-vc_event idpf_vc_event_task [idpf] [40958.168865] RIP: 0010:idpf_vc_event_task+0x9b/0x350 [idpf] ... [40958.177932] Call Trace: [40958.178491] <TASK> [40958.179040] process_one_work+0x226/0x6d0 [40958.179609] worker_thread+0x19e/0x340 [40958.180158] ? __pfx_worker_thread+0x10/0x10 [40958.180702] kthread+0x10f/0x250 [40958.181238] ? __pfx_kthread+0x10/0x10 [40958.181774] ret_from_fork+0x251/0x2b0 [40958.182307] ? __pfx_kthread+0x10/0x10 [40958.182834] ret_from_fork_asm+0x1a/0x30 [40958.183370] </TASK> Fix the error handling in the init_task to make sure the service and mailbox tasks are disabled if the error happens during load. These are started in idpf_vc_core_init(), which spawns the init_task and has no way of knowing if it failed. If the error happens on reset, following successful driver load, the tasks can still run, as that will allow the netdevs to attempt recovery through another reset. Stop the PTP callbacks either way as those will be restarted by the call to idpf_vc_core_init() during a successful reset.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: inet: frags: drop fraglist		

CVE-2026-23016	conntrack references Jakub added a warning in nf_conntrack_cleanup_net_list() to make debugging leaked skbs/conntrack references more obvious. syzbot reports this as triggering, and I can also reproduce this via ip_defrag.sh selftest: conntrack cleanup blocked for 60s WARNING: net/netfilter/nf_conntrack_core.c:2512 [..] conntrack clenups gets stuck because there are skbs with still hold nf_conn references via their frag_list. net.core.skb_defer_max=0 makes the hang disappear. Eric Dumazet points out that skb_release_head_state() doesn't follow the fraglist. ip_defrag.sh can only reproduce this problem since commit 6471658dc66c ("udp: use skb_attempt_defer_free()"), but AFAICS this problem could happen with TCP as well if pmtu discovery is off. The relevant problem path for udp is: 1. netns emits fragmented packets 2. nf_defrag_v6_hook reassembles them (in output hook) 3. reassembled skb is tracked (skb owns nf_conn reference) 4. ip6_output refragments 5. refragmented packets also own nf_conn reference (ip6_fragment calls ip6_copy_metadata()) 6. on input path, nf_defrag_v6_hook skips defragmentation: the fragments already have skb->nf_conn attached 7. skbs are reassembled via ipv6_frag_rcv() 8. skb_consume_udp -> skb_attempt_defer_free() -> skb ends up in pcpu freelist, but still has nf_conn reference. Possible solutions: 1 let defrag engine drop nf_conn entry, OR 2 export kick_defer_list_purge() and call it from the conntrack netns exit callback, OR 3 add skb_has_frag_list() check to skb_attempt_defer_free() 2 & 3 also solve ip_defrag.sh hang but share same drawback: Such reassembled skbs, queued to socket, can prevent conntrack module removal until userspace has consumed the packet. While both tcp and udp stack do call nf_reset_ct() before placing skb on socket queue, that function doesn't iterate frag_list skbs. Therefore drop nf_conn entries when they are placed in defrag queue. Keep the nf_conn entry of the first (offset 0) skb so that reassembled skb retains nf_conn entry for sake of TX path. Note that fixes tag is incorrect; it points to the commit introducing the 'ip_defrag.sh reproducible problem': no need to backport this patch to every stable kernel.	N/A	More Details
CVE-2026-23015	In the Linux kernel, the following vulnerability has been resolved: gpio: mpsse: fix reference leak in gpio_mpsse_probe() error paths The reference obtained by calling usb_get_dev() is not released in the gpio_mpsse_probe() error paths. Fix that by using device managed helper functions. Also remove the usb_put_dev() call in the disconnect function since now it will be released automatically.	N/A	More Details
CVE-2025-71191	In the Linux kernel, the following vulnerability has been resolved: dmaengine: at_hdmac: fix device leak on of_dma_xlate() Make sure to drop the reference taken when looking up the DMA platform device during of_dma_xlate() when releasing channel resources. Note that commit 3832b78b3ec2 ("dmaengine: at_hdmac: add missing put_device() call in at_dma_xlate()") fixed the leak in a couple of error paths but the reference is still leaking on successful allocation.	N/A	More Details
CVE-2025-71190	In the Linux kernel, the following vulnerability has been resolved: dmaengine: bcm-sba-raid: fix device leak on probe Make sure to drop the reference taken when looking up the mailbox device during probe on probe failures and on driver unbind.	N/A	More Details
CVE-2025-71189	In the Linux kernel, the following vulnerability has been resolved: dmaengine: dw: dmamux: fix OF node leak on route allocation failure Make sure to drop the reference taken to the DMA master OF node also on late route allocation failures.	N/A	More Details
CVE-2025-71188	In the Linux kernel, the following vulnerability has been resolved: dmaengine: lpc18xx-dmamux: fix device leak on route allocation Make sure to drop the reference taken when looking up the DMA mux platform device during route allocation. Note that holding a reference to a device does not prevent its driver data from going away so there is no point in keeping the reference.	N/A	More Details
CVE-2025-71187	In the Linux kernel, the following vulnerability has been resolved: dmaengine: sh: rz-dmac: fix device leak on probe failure Make sure to drop the reference taken when looking up the ICU device during probe also on probe failures (e.g. probe deferral).	N/A	More Details
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: dmaengine: stm32: dmamux: fix device leak on route allocation Make sure to drop the reference taken when looking up the DMA mux platform device during route allocation. Note that holding a	N/A	More Details

71186	reference to a device does not prevent its driver data from going away so there is no point in keeping the reference.		
CVE-2025-71185	In the Linux kernel, the following vulnerability has been resolved: dmaengine: ti: dma-crossbar: fix device leak on am335x route allocation Make sure to drop the reference taken when looking up the crossbar platform device during am335x route allocation.	N/A	More Details
CVE-2025-71184	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix NULL dereference on root when tracing inode eviction When evicting an inode the first thing we do is to setup tracing for it, which implies fetching the root's id. But in btrfs_evict_inode() the root might be NULL, as implied in the next check that we do in btrfs_evict_inode(). Hence, we either should set the ->root_objectid to 0 in case the root is NULL, or we move tracing setup after checking that the root is not NULL. Setting the rootid to 0 at least gives us the possibility to trace this call even in the case when the root is NULL, so that's the solution taken here.	N/A	More Details
CVE-2025-71183	In the Linux kernel, the following vulnerability has been resolved: btrfs: always detect conflicting inodes when logging inode refs After rename exchanging (either with the rename exchange operation or regular renames in multiple non-atomic steps) two inodes and at least one of them is a directory, we can end up with a log tree that contains only of the inodes and after a power failure that can result in an attempt to delete the other inode when it should not because it was not deleted before the power failure. In some case that delete attempt fails when the target inode is a directory that contains a subvolume inside it, since the log replay code is not prepared to deal with directory entries that point to root items (only inode items). 1) We have directories "dir1" (inode A) and "dir2" (inode B) under the same parent directory; 2) We have a file (inode C) under directory "dir1" (inode A); 3) We have a subvolume inside directory "dir2" (inode B); 4) All these inodes were persisted in a past transaction and we are currently at transaction N; 5) We rename the file (inode C), so at btrfs_log_new_name() we update inode C's last_unlink_trans to N; 6) We get a rename exchange for "dir1" (inode A) and "dir2" (inode B), so after the exchange "dir1" is inode B and "dir2" is inode A. During the rename exchange we call btrfs_log_new_name() for inodes A and B, but because they are directories, we don't update their last_unlink_trans to N; 7) An fsync against the file (inode C) is done, and because its inode has a last_unlink_trans with a value of N we log its parent directory (inode A) (through btrfs_log_all_parents(), called from btrfs_log_inode_parent()). 8) So we end up with inode B not logged, which now has the old name of inode A. At copy_inode_items_to_log(), when logging inode A, we did not check if we had any conflicting inode to log because inode A has a generation lower than the current transaction (created in a past transaction); 9) After a power failure, when replaying the log tree, since we find that inode A has a new name that conflicts with the name of inode B in the fs tree, we attempt to delete inode B... this is wrong since that directory was never deleted before the power failure, and because there is a subvolume inside that directory, attempting to delete it will fail since replay_dir_deletes() and btrfs_unlink_inode() are not prepared to deal with dir items that point to roots instead of inodes. When that happens the mount fails and we get a stack trace like the following: [87.2314] BTRFS info (device dm-0): start tree-log replay [87.2318] BTRFS critical (device dm-0): failed to delete reference to subvol, root 5 inode 256 parent 259 [87.2332] ----------[cut here]------------ [87.2338] BTRFS: Transaction aborted (error -2) [87.2346] WARNING: CPU: 1 PID: 638968 at fs/btrfs/inode.c:4345 __btrfs_unlink_inode+0x416/0x440 [btrfs] [87.2368] Modules linked in: btrfs loop dm_thin_pool (...) [87.2470] CPU: 1 UID: 0 PID: 638968 Comm: mount Tainted: G W 6.18.0-rc7-btrfs-next-218+ #2 PREEMPT(full) [87.2489] Tainted: [W]=WARN [87.2494] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.2-0-gea1b7a073390-prebuilt.qemu.org 04/01/2014 [87.2514] RIP: 0010:__btrfs_unlink_inode+0x416/0x440 [btrfs] [87.2538] Code: c0 89 04 24 (...) [87.2568] RSP: 0018:ffffc0e741f4b9b8 EFLAGS: 00010286 [87.2574] RAX: 0000000000000000 RBX: ffff9d3ec8a6cf60 RCX: 0000000000000000 [87.2582] RDX: 0000000000000002 RSI: ffffffff84ab45a1 RDI: 00000000ffffffff [87.2591] RBP: ffff9d3ec8a6ef20 R08: 0000000000000000 R09: ffffc0e741f4b840 [87.2599] R10: ffff9d45dc1fffa8 R11: 0000000000000003 R12: ffff9d3ee26d77e0 [87.2608] R13: ffffc0e741f4ba98 R14: ffff9d4458040800 R15: ffff9d44b6b7ca10 [87.2618] FS:	N/A	More Details

	00007f7b9603a840(0000) GS:ffff9d4658982000(0000) knlGS:0000000000000000 [87. ---truncated---		
CVE-2026-25117	pwn.college DOJO is an education platform for learning cybersecurity. Prior to commit e33da14449a5abcff507e554f66e2141d6683b0a, missing sandboxing on `/workspace/*` routes allows challenge authors to inject arbitrary javascript which runs on the same origin as `http[:]//dojo[.]website`. This is a sandbox escape leading to arbitrary javascript execution as the dojo's origin. A challenge author can craft a page that executes any dangerous actions that the user could. Version e33da14449a5abcff507e554f66e2141d6683b0a patches the issue.	N/A	More Details
CVE-2026-25061	tcpflow is a TCP/IP packet demultiplexer. In versions up to and including 1.61, wifipcap parses 802.11 management frame elements and performs a length check on the wrong field when handling the TIM element. A crafted frame with a large TIM length can cause a 1-byte out-of-bounds write past `tim.bitmap[251]`. The overflow is small and DoS is the likely impact; code execution is potential, but still up in the air. The affected structure is stack-allocated in `handle_beacon()` and related handlers. As of time of publication, no known patches are available.	N/A	More Details
CVE-2026-1432	SQL injection vulnerability in the Buroweb platform version 2505.0.12, specifically in the 'tablon' component. This vulnerability is present in several parameters that do not correctly sanitize user input in the endpoint '/sta/CarpetaPublic/doEvent?APP_CODE=STA&PAGE_CODE=TABLON'. Exploiting this vulnerability could allow an attacker to execute queries on the database and gain access to confidential information.	N/A	More Details
CVE-2025-26386	Johnson Controls iSTAR Configuration Utility (ICU) has Stack-based Buffer Overflow vulnerability. This issue affects iSTAR Configuration Utility (ICU) version 6.9.7 and prior. Successful exploitation of this vulnerability could result in failure within the operating system of the machine hosting the ICU tool.	N/A	More Details
CVE-2026-0483	Stored Cross-Site Scripting (XSS) vulnerability in the PDF file upload functionality of Live Helper Chat, versions prior to 4.72. An attacker can upload a malicious PDF file containing an XSS payload, which will be executed in the user's context when they download and open the file via the link generated by the application. The vulnerability allows arbitrary JavaScript code to be executed in the user's local context.	N/A	More Details
CVE-2025-59901	Disk Pulse Enterprise v10.4.18 has an authenticated reflected XSS vulnerability in the '/monitor_directory?sid=' endpoint, caused by insufficient validation of the 'monitor_directory' parameter sent by POST. An attacker could exploit this weakness to send malicious content to an authenticated user and steal information from their session.	N/A	More Details
CVE-2025-59900	Sync Breeze Enterprise Server v10.4.18 and Disk Pulse Enterprise v10.4.18 contain a persistent authenticated Cross-Site Scripting (XSS) vulnerability. An attacker could send malicious content to an authenticated user and steal information from their session due to insufficient validation of user input in '/server_options?sid=', affecting the 'tasks_logs_dir', 'errors_logs_dir', 'error_notifications_address', 'status_notifications_address', and 'status_reports_address' parameters.	N/A	More Details
CVE-2025-59899	Sync Breeze Enterprise Server v10.4.18 and Disk Pulse Enterprise v10.4.18 contain a persistent authenticated Cross-Site Scripting (XSS) vulnerability. An attacker could send malicious content to an authenticated user and steal information from their session due to insufficient validation of user input in '/server_options?sid=', affecting the 'tasks_logs_dir', 'errors_logs_dir', 'error_notifications_address', 'status_notifications_address', and 'status_reports_address' parameters.	N/A	More Details
CVE-2025-59898	Sync Breeze Enterprise Server v10.4.18 and Disk Pulse Enterprise v10.4.18 contain a persistent authenticated Cross-Site Scripting (XSS) vulnerability. An attacker could send malicious content to an authenticated user and steal information from their session due to insufficient validation of user input in '/add_exclude_dir?sid=', affecting the 'exclude_dir' parameter.	N/A	More Details
	Sync Breeze Enterprise Server v10.4.18 and Disk Pulse Enterprise v10.4.18 contain a		

CVE-2025-59897	persistent authenticated Cross-Site Scripting (XSS) vulnerability. An attacker could send malicious content to an authenticated user and steal information from their session due to insufficient validation of user input in '/edit_command?sid=', affecting the 'source_dir' and ‘dest_dir’ parameters.	N/A	More Details
CVE-2025-59896	Sync Breeze Enterprise Server v10.4.18 and Disk Pulse Enterprise v10.4.18 contain a persistent authenticated Cross-Site Scripting (XSS) vulnerability. An attacker could send malicious content to an authenticated user and steal information from their session due to insufficient validation of user input in '/add_command?sid=', affecting the 'command_name' parameter.	N/A	More Details
CVE-2025-59895	Sync Breeze Enterprise Server v10.4.18 and Disk Pulse Enterprise v10.4.18 contain a remote denial-of-service (DoS) vulnerability in the configuration restore functionality. The issue is due to insufficient validation of user-supplied data during this process. An attacker could send malicious requests to alter the configuration file, causing the application to become unresponsive. In a successful scenario, the service may not recover on its own and require a complete reinstallation, as the configuration becomes corrupted and prevents the service from restarting, even manually.	N/A	More Details
CVE-2025-59894	Cross-Site request forgery (CSRF) vulnerability in Sync Breeze Enterprise Server v10.4.18 and Disk Pulse Enterprise v10.4.18. An authenticated user could cause another user to perform unwanted actions within the application they are logged into. This vulnerability is possible due to the lack of proper CSRF token implementation. Among other things, it is possible, using a POST request to delete all commands via '/delete_all_commands?sid='.	N/A	More Details
CVE-2025-59893	Cross-Site request forgery (CSRF) vulnerability in Sync Breeze Enterprise Server v10.4.18 and Disk Pulse Enterprise v10.4.18. An authenticated user could cause another user to perform unwanted actions within the application they are logged into. This vulnerability is possible due to the lack of proper CSRF token implementation. Among other things, it is possible, using a POST request to rename commands via '/rename_command?sid=', affecting the 'command_name' parameter.	N/A	More Details
CVE-2025-59892	Cross-Site request forgery (CSRF) vulnerability in Sync Breeze Enterprise Server v10.4.18 and Disk Pulse Enterprise v10.4.18. An authenticated user could cause another user to perform unwanted actions within the application they are logged into. This vulnerability is possible due to the lack of proper CSRF token implementation. Among other things, it is possible, using a POST request to delete commands individually via '/delete_command?sid=', using the 'cid' parameter.	N/A	More Details
CVE-2025-59891	Cross-Site request forgery (CSRF) vulnerability in Sync Breeze Enterprise Server v10.4.18 and Disk Pulse Enterprise v10.4.18. An authenticated user could cause another user to perform unwanted actions within the application they are logged into. This vulnerability is possible due to the lack of proper CSRF token implementation. Among other things, it is possible, using a POST request to change a user's password or create users via '/setup_login?sid=', affecting the 'username', 'password', and 'cpassword' parameters.	N/A	More Details
CVE-2025-41351	Vulnerability that allows a Padding Oracle Attack to be performed on the Funambol v30.0.0.20 cloud server. The thumbnail display URL allows an attacker to decrypt and encrypt the parameters used by the application to generate ‘self-signed’ access URLs.	N/A	More Details
CVE-2026-23014	In the Linux kernel, the following vulnerability has been resolved: perf: Ensure swevent hrtimer is properly destroyed With the change to hrtimer_try_to_cancel() in perf_swevent_cancel_hrtimer() it appears possible for the hrtimer to still be active by the time the event gets freed. Make sure the event does a full hrtimer_cancel() on the free path by installing a perf_event::destroy handler.	N/A	More Details
CVE-2025-7740	Default credentials vulnerability exists in SuprOS product. If exploited, this could allow an authenticated local attacker to use an admin account created during product deployment.	N/A	More Details
CVE-2026-	Rejected reason: Not used	N/A	More

24867			Details
CVE-2026-24866	Rejected reason: Not used	N/A	More Details
CVE-2026-24865	Rejected reason: Not used	N/A	More Details
CVE-2026-24864	Rejected reason: Not used	N/A	More Details
CVE-2026-24863	Rejected reason: Not used	N/A	More Details
CVE-2026-24862	Rejected reason: Not used	N/A	More Details
CVE-2026-24861	Rejected reason: Not used	N/A	More Details
CVE-2026-24860	Rejected reason: Not used	N/A	More Details
CVE-2026-24859	Rejected reason: Not used	N/A	More Details
CVE-2026-21569	This High severity XXE (XML External Entity Injection) vulnerability was introduced in version 7.1.0 of Crowd Data Center and Server. This XXE (XML External Entity Injection) vulnerability, with a CVSS Score of 7.9, allows an authenticated attacker to access local and remote content which has high impact to confidentiality, low impact to integrity, high impact to availability, and requires no user interaction. Atlassian recommends that Crowd Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Crowd Data Center and Server 7.1: Upgrade to a release greater than or equal to 7.1.3 See the release notes (https://confluence.atlassian.com/crowd/crowd-release-notes-199094.html). You can download the latest version of Crowd Data Center and Server from the download center (https://www.atlassian.com/software/crowd/download-archive). This vulnerability was reported via our Atlassian (Internal) program.	N/A	More Details
CVE-2026-24785	Clatter is a no_std compatible, pure Rust implementation of the Noise protocol framework with post-quantum support. Versiosn prior to2.2.0 have a protocol compliance vulnerability. The library allowed post-quantum handshake patterns that violated the PSK validity rule (Noise Protocol Framework Section 9.3). This could allow PSK-derived keys to be used for encryption without proper randomization by self-chosen ephemeral randomness, weakening security guarantees and potentially allowing catastrophic key reuse. Affected default patterns include `noise_pqkk_psk0`, `noise_pqkn_psk0`, `noise_pqnk_psk0`, `noise_pqnn_psk0``, and some hybrid variants. Users of these patterns may have been using handshakes that do not meet the intended security properties. The issue is fully patched and released in Clatter v2.2.0. The fixed version includes runtime checks to detect offending handshake patterns. As a workaround, avoid using offending `*_psk0` variants of post-quantum patterns. Review custom handshake patterns carefully.	N/A	More Details
	Vulnerable cross-model authorization in juju. If a charm's cross-model permissions are		

CVE-2026-1237	revoked or expire, a malicious user who is able to update database records can mint an invalid macaroon that is incorrectly validated by the juju controller, enabling a charm to maintain otherwise revoked or expired permissions. This allows a charm to continue relating to another charm in a cross-model relation, and use their workload without their permission. No fix is available as of the time of writing.	N/A	More Details
CVE-2026-22243	EGroupware is a Web based groupware server written in PHP. A SQL Injection vulnerability exists in the core components of EGroupware prior to versions 23.1.20260113 and 26.0.20260113, specifically in the `Nextmatch` filter processing. The flaw allows authenticated attackers to inject arbitrary SQL commands into the `WHERE` clause of database queries. This is achieved by exploiting a PHP type juggling issue where JSON decoding converts numeric strings into integers, bypassing the `is_int()` security check used by the application. Versions 23.1.20260113 and 26.0.20260113 patch the vulnerability.	N/A	More Details
CVE-2026-25047	deepHas provides a test for the existence of a nested object key and optionally returns that key. A prototype pollution vulnerability exists in version 1.0.7 of the deephas npm package that allows an attacker to modify global object behavior. This issue was fixed in version 1.0.8.	N/A	More Details
CVE-2026-24414	The Icinga PowerShell Framework provides configuration and check possibilities to ensure integration and monitoring of Windows environments. In versions prior to 1.13.4, 1.12.4, and 1.11.2, permissions of the Icinga for Windows `certificate` directory grant every user read access, which results in the exposure of private key of the Icinga certificate for the given host. All installations are affected. Versions 1.13.4, 1.12.4, and 1.11.2 contains a patch. Please note that upgrading to a fixed version of Icinga for Windows will also automatically fix a similar issue present in Icinga 2, CVE-2026-24413. As a workaround, the permissions can be restricted manually by updating the ACL for the given folder `C:\Program Files\WindowsPowerShell\modules\icinga-powershell-framework\certificate` (and `C:\ProgramData\icinga2\var` to fix the issue for the Icinga 2 agent as well) including every sub-folder and item to restrict access for general users, only allowing the Icinga service user and administrators access.	N/A	More Details
CVE-2026-25040	Budibase is a low code platform for creating internal tools, workflows, and admin panels. In versions up to and including 3.26.3, a Creator-level user, who normally has no UI permission to invite users, can manipulate API requests to invite new users with any role, including Admin, Creator, or App Viewer, and assign them to any group in the organization. This allows full privilege escalation, bypassing UI restrictions, and can lead to complete takeover of the workspace or organization. As of time of publication, no known fixed versions are available.	N/A	More Details
CVE-2026-24905	Inspektor Gadget is a set of tools and framework for data collection and system inspection on Kubernetes clusters and Linux hosts using eBPF. The `ig` binary provides a subcommand for image building, used to generate custom gadget OCI images. A part of this functionality is implemented in the file `inspektor-gadget/cmd/common/image/build.go`. The `Makefile.build` file is the Makefile template employed during the building process. This file includes user-controlled data in an unsafe fashion, specifically some parameters are embedded without an adequate escaping in the commands inside the Makefile. Prior to version 0.48.1, this implementation is vulnerable to command injection: an attacker able to control values in the `buildOptions` structure would be able to execute arbitrary commands during the building process. An attacker able to exploit this vulnerability would be able to execute arbitrary command on the Linux host where the `ig` command is launched, if images are built with the `--local` flag or on the build container invoked by `ig`, if the `--local` flag is not provided. The `buildOptions` structure is extracted from the YAML gadget manifest passed to the `ig image build` command. Therefore, the attacker would need a way to control either the full `build.yml` file passed to the `ig image build` command, or one of its options. Typically, this could happen in a CI/CD scenario that builds untrusted gadgets to verify correctness. Version 0.48.1 fixes the issue.	N/A	More Details
	alsa-lib versions 1.2.2 up to and including 1.2.15.2, prior to commit 5f7fe33, contain a		

CVE-2026-25068	heap-based buffer overflow in the topology mixer control decoder. The tplg_decode_control_mixer1() function reads the num_channels field from untrusted .tplg data and uses it as a loop bound without validating it against the fixed-size channel array (SND_TPLG_MAX_CHAN). A crafted topology file with an excessive num_channels value can cause out-of-bounds heap writes, leading to a crash.	N/A	More Details
CVE-2026-24687	Umbraco Forms is a form builder that integrates with the Umbraco content management system. It's possible for an authenticated backoffice-user to enumerate and traverse paths/files on the systems filesystem and read their contents, on Mac/Linux Umbraco installations using Forms. As Umbraco Cloud runs in a Windows environment, Cloud users aren't affected. This issue affects versions 16 and 17 of Umbraco Forms and is patched in 16.4.1 and 17.1.1. If upgrading is not immediately possible, users can mitigate this vulnerability by configuring a WAF or reverse proxy to block requests containing path traversal sequences (`../`, `..\`) in the `fileName` parameter of the export endpoint, restricting network access to the Umbraco backoffice to trusted IP ranges, and/or blocking the `/umbraco/forms/api/v1/export` endpoint entirely if the export feature is not required. However, upgrading to the patched version is strongly recommended.	N/A	More Details
CVE-2025-15549	FluentCMS 2026 contains a stored cross-site scripting vulnerability that allows authenticated administrators to upload SVG files with embedded JavaScript via the File Management module. Attackers can upload malicious SVG files that execute JavaScript in the browser of any user accessing the uploaded file URL.	N/A	More Details
CVE-2026-1457	An authenticated buffer handling flaw in TP-Link VIGI C385 V1 Web API lacking input sanitization, may allow memory corruption leading to remote code execution. Authenticated attackers may trigger buffer overflow and potentially execute arbitrary code with elevated privileges.	N/A	More Details
CVE-2025-15548	Some VX800v v1.0 web interface endpoints transmit sensitive information over unencrypted HTTP due to missing application layer encryption, allowing a network adjacent attacker to intercept this traffic and compromise its confidentiality.	N/A	More Details
CVE-2025-15543	Improper link resolution in USB HTTP access path in VX800v v1.0 allows a crafted USB device to expose root filesystem contents, giving an attacker with physical access read-only access to system files.	N/A	More Details
CVE-2025-15542	Improper handling of exceptional conditions in VX800v v1.0 in SIP processing allows an attacker to flood the device with crafted INVITE messages, blocking all voice lines and causing a denial of service on incoming calls.	N/A	More Details
CVE-2025-15541	Improper link resolution in the VX800v v1.0 SFTP service allows authenticated adjacent attackers to use crafted symbolic links to access system files, resulting in high confidentiality impact and limited integrity risk.	N/A	More Details
CVE-2025-13399	A weakness in the web interface’s application layer encryption in VX800v v1.0 allows an adjacent attacker to brute force the weak AES key and decrypt intercepted traffic. Successful exploitation requires network proximity but no authentication, and may result in high impact to confidentiality, integrity, and availability of transmitted data.	N/A	More Details
CVE-2026-24780	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows. Prior to autogpt-platform-beta-v0.6.44, AutoGPT Platform's block execution endpoints (both main web API and external API) allow executing blocks by UUID without checking the `disabled` flag. Any authenticated user can execute the disabled `BlockInstallationBlock`, which writes arbitrary Python code to the server filesystem and executes it via `__import__()`, achieving Remote Code Execution. In default self-hosted deployments where Supabase signup is enabled, an attacker can self-register; if signup is disabled (e.g., hosted), the attacker needs an existing account. autogpt-platform-beta-v0.6.44 contains a fix.	N/A	More Details
	Icinga 2 is an open source monitoring system. Starting in version 2.3.0 and prior to versions 2.13.14, 2.14.8, and 2.15.2, the Icinga 2 MSI did not set appropriate permissions for the `%ProgramData%\icinga2\var` folder on Windows. This resulted in the its contents		

CVE-2026-24413	- including the private key of the user and synced configuration - being readable by all local users. All installations on Windows are affected. Versions 2.13.14, 2.14.8, and 2.15.2 contains a fix. There are two possibilities to work around the issue without upgrading Icinga 2. Upgrade Icinga for Windows to at least version v1.13.4, v1.12.4, or v1.11.2. These version will automatically fix the ACLs for the Icinga 2 agent as well. Alternatively, manually update the ACL for the given folder `C:\ProgramData\icinga2\var` (and `C:\Program Files\WindowsPowerShell\modules\icinga-powershell-framework\certificate` to fix the issue for the Icinga for Windows as well) including every sub-folder and item to restrict access for general users, only allowing the Icinga service user and administrators access.	N/A	More Details
CVE-2026-24685	OpenProject is an open-source, web-based project management software. Versions prior to 16.6.6 and 17.0.2 have an arbitrary file write vulnerability in OpenProject's repository diff download endpoint (`/projects/:project_id/repository/diff.diff`) when rendering a single revision via git show. By supplying a specially crafted rev value (for example, `rev=--output=/tmp/poc.txt)`, an attacker can inject git show command-line options. When OpenProject executes the SCM command, Git interprets the attacker-controlled rev as an option and writes the output to an attacker-chosen path. As a result, any user with the `:browse_repository` permission on the project can create or overwrite arbitrary files that the OpenProject process user is permitted to write. The written contents consist of git show output (commit metadata and patch), but overwriting application or configuration files still leads to data loss and denial of service, impacting integrity and availability. The issue has been fixed in OpenProject 17.0.2 and 16.6.6.	N/A	More Details
CVE-2026-24054	Kata Containers is an open source project focusing on a standard implementation of lightweight Virtual Machines (VMs) that perform like containers. In versions prior to 3.26.0, when a container image is malformed or contains no layers, containerd falls back to bind-mounting an empty snapshotter directory for the container rootfs. When the Kata runtime attempts to mount the container rootfs, the bind mount causes the rootfs to be detected as a block device, leading to the underlying device being hotplugged to the guest. This can cause filesystem-level errors on the host due to double inode allocation, and may lead to the host's block device being mounted as read-only. Version 3.26.0 contains a patch for the issue.	N/A	More Details
CVE-2025-15545	The backup restore function does not properly validate unexpected or unrecognized tags within the backup file. When such a crafted file is restored, the injected tag is interpreted by a shell, allowing execution of arbitrary commands with root privileges. Successful exploitation allows the attacker to gain root-level command execution, compromising confidentiality, integrity and availability.	N/A	More Details
CVE-2025-13905	CWE-276: Incorrect Default Permissions vulnerability exists that could cause privilege escalation through the reverse shell when one or more executable service binaries are modified in the installation folder by a local user with normal privilege upon service restart.	N/A	More Details
CVE-2026-1469	Stored Cross-Site Scripting (XSS) in RLE NOVA's PlanManager. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by injecting malicious payload through the 'comment' and 'brand' parameters in '/index.php'. The payload is stored by the application and subsequently displayed without proper sanitization when other users access it. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user.	N/A	More Details
CVE-2026-1188	In the Eclipse OMR port library component since release 0.2.0, an API function to return the textual names of all supported processor features was not accounting for the separator inserted between processor features. If the output buffer supplied to this function was incorrectly sized, failing to account for the separator when determining when a write to the buffer was safe could lead to a buffer overflow. This issue is fixed in Eclipse OMR version 0.8.0.	N/A	More Details
	SmarterTools SmarterMail versions prior to build 9518 contain an unauthenticated path coercion vulnerability in the background-of-the-day preview endpoint. The application		

CVE-2026-25067	base64-decodes attacker-supplied input and uses it as a filesystem path without validation. On Windows systems, this allows UNC paths to be resolved, causing the SmarterMail service to initiate outbound SMB authentication attempts to attacker-controlled hosts. This can be abused for credential coercion, NTLM relay attacks, and unauthorized network authentication.	N/A	More Details
CVE-2026-24857	`bulk_extractor` is a digital forensics exploitation tool. Starting in version 1.4, `bulk_extractor`'s embedded unrar code has a heap-buffer-overflow in the RAR PPM LZ decoding path. A crafted RAR inside a disk image causes an out-of-bounds write in `Unpack::CopyString`, leading to a crash under ASAN (and likely a crash or memory corruption in production builds). There's potential for using this for RCE. As of time of publication, no known patches are available.	N/A	More Details
CVE-2026-24835	Podman Desktop is a graphical tool for developing on containers and Kubernetes. A critical authentication bypass vulnerability in Podman Desktop prior to version 1.25.1 allows any extension to completely circumvent permission checks and gain unauthorized access to all authentication sessions. The `isAccessAllowed()` function unconditionally returns `true`, enabling malicious extensions to impersonate any user, hijack authentication sessions, and access sensitive resources without authorization. This vulnerability affects all versions of Podman Desktop. Version 1.25.1 contains a patch for the issue.	N/A	More Details
CVE-2026-24769	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.0, a stored cross-site scripting (XSS) vulnerability exists in NocoDB's attachment handling mechanism. Authenticated users can upload malicious SVG files containing embedded JavaScript, which are later rendered inline and executed in the browsers of other users who view the attachment. Because the malicious payload is stored server-side and executed under the application's origin, successful exploitation can lead to account compromise, data exfiltration and unauthorized actions performed on behalf of affected users. Version 0.301.0 patches the issue.	N/A	More Details
CVE-2026-24768	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.0, an unvalidated redirect (open redirect) vulnerability exists in NocoDB's login flow due to missing validation of the `continueAfterSignIn` parameter. During authentication, NocoDB processes a user-controlled redirect value and conditionally performs client-side navigation without enforcing any restrictions on the destination's origin, domain or protocol. This allows attackers to redirect authenticated users to arbitrary external websites after login. This vulnerability enables phishing attacks by leveraging user trust in the legitimate NocoDB login flow. While it does not directly expose credentials or bypass authentication, it increases the likelihood of credential theft through social engineering. The issue does not allow arbitrary code execution or privilege escalation, but it undermines authentication integrity. Version 0.301.0 fixes the issue.	N/A	More Details
CVE-2026-0750	Improper Verification of Cryptographic Signature vulnerability in Drupal Drupal Commerce Paybox Commerce Paybox on Drupal 7.X allows Authentication Bypass.This issue affects Drupal Commerce Paybox: from 7-x-1.0 through 7.X-1.5.	N/A	More Details
CVE-2026-0749	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Form Builder allows Cross-Site Scripting (XSS).This issue affects Drupal: from 7.X-1.0 through 7.X-1.22.	N/A	More Details
CVE-2026-23032	In the Linux kernel, the following vulnerability has been resolved: null_blk: fix kmemleak by releasing references to fault configfs items When CONFIG_BLK_DEV_NULL_BLK_FAULT_INJECTION is enabled, the null-blk driver sets up fault injection support by creating the timeout_inject, requeue_inject, and init_hctx_fault_inject configfs items as children of the top-level nullbX configfs group. However, when the nullbX device is removed, the references taken to these fault-config configfs items are not released. As a result, kmemleak reports a memory leak, for example: unreferenced object 0xc00000021ff25c40 (size 32): comm "mkdir", pid 10665, jiffies 4322121578 hex dump (first 32 bytes): 69 6e 69 74 5f 68 63 74 78 5f 66 61 75 6c 74 5f init_hctx_fault_ 69 6e 6a 65 63 74 00 88 00 00 00 00 00 00 00 00 inject..... backtrace (crc 1a018c86):	N/A	More Details

	__kmalloc_node_track_caller_noprof+0x494/0xbd8 kvasprintf+0x74/0xf4 config_item_set_name+0xf0/0x104 config_group_init_type_name+0x48/0xfc fault_config_init+0x48/0xf0 0xc0080000180559e4 configfs_mkdir+0x304/0x814 vfs_mkdir+0x49c/0x604 do_mkdirat+0x314/0x3d0 sys_mkdir+0xa0/0xd8 system_call_exception+0x1b0/0x4f0 system_call_vectored_common+0x15c/0x2ec Fix this by explicitly releasing the references to the fault-config configfs items when dropping the reference to the top-level nullbX configfs group.		
CVE-2026-23033	In the Linux kernel, the following vulnerability has been resolved: dmaengine: omap-dma: fix dma_pool resource leak in error paths The dma_pool created by dma_pool_create() is not destroyed when dma_async_device_register() or of_dma_controller_register() fails, causing a resource leak in the probe error paths. Add dma_pool_destroy() in both error paths to properly release the allocated dma_pool resource.	N/A	More Details
CVE-2026-23034	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/userq: Fix fence reference leak on queue teardown v2 The user mode queue keeps a pointer to the most recent fence in userq->last_fence. This pointer holds an extra dma_fence reference. When the queue is destroyed, we free the fence driver and its xarray, but we forgot to drop the last_fence reference. Because of the missing dma_fence_put(), the last fence object can stay alive when the driver unloads. This leaves an allocated object in the amdgpu_userq_fence slab cache and triggers This is visible during driver unload as: BUG amdgpu_userq_fence: Objects remaining on __kmem_cache_shutdown() kmem_cache_destroy amdgpu_userq_fence: Slab cache still has objects Call Trace: kmem_cache_destroy amdgpu_userq_fence_slab_fini amdgpu_exit __do_sys_delete_module Fix this by putting userq->last_fence and clearing the pointer during amdgpu_userq_fence_driver_free(). This makes sure the fence reference is released and the slab cache is empty when the module exits. v2: Update to only release userq->last_fence with dma_fence_put() (Christian) (cherry picked from commit 8e051e38a8d45caf6a866d4ff842105b577953bb)	N/A	More Details
CVE-2025-61648	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation CheckUser. This vulnerability is associated with program files modules/ext.CheckUser.TempAccounts/components/ShowIPButton.Vue, modules/ext.CheckUser.TempAccounts/SpecialBlock.Js. This issue affects CheckUser: from * before 1.44.1.	N/A	More Details
CVE-2025-61656	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation VisualEditor. This vulnerability is associated with program files src/ce/ve.Ce.ClipboardHandler.Js. This issue affects VisualEditor: from * before 1.39.14, 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-61655	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation VisualEditor. This vulnerability is associated with program files includes/ApiVisualEditorEdit.Php, modules/ve-mw/init/targets/ve.Init.Mw.DesktopArticleTarget.Js, modules/ve-mw/ui/dialogs/ve.Ui.MWSaveDialog.Js. This issue affects VisualEditor: from * before 1.39.14, 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-61654	Vulnerability in Wikimedia Foundation Thanks. This vulnerability is associated with program files includes/ThanksQueryHelper.Php. This issue affects Thanks: from * before 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-61653	Vulnerability in Wikimedia Foundation TextExtracts. This vulnerability is associated with program files includes/ApiQueryExtracts.Php. This issue affects TextExtracts: from * before 1.39.14, 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-61652	Vulnerability in Wikimedia Foundation DiscussionTools.This issue affects DiscussionTools: from * before 1.43.4, 1.44.1.	N/A	More Details
	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site		

CVE-2025-61651	Scripting') vulnerability in Wikimedia Foundation CheckUser. This vulnerability is associated with program files modules/ext.CheckUser/checkuser/checkUserHelper/buildUserElement.Js. This issue affects CheckUser: from * before 1.44.1.	N/A	More Details
CVE-2025-58383	A vulnerability in Brocade Fabric OS versions before 9.2.1c2 could allow an administrator-level user to execute the bind command, to escalate privileges and bypass security controls allowing the execution of arbitrary commands.	N/A	More Details
CVE-2025-58382	A vulnerability in the secure configuration of authentication and management services in Brocade Fabric OS before Fabric OS 9.2.1c2 could allow an authenticated, remote attacker with administrative credentials to execute arbitrary commands as root using “supportsave”, “seccertmgmt”, “configupload” command.	N/A	More Details
CVE-2025-58379	Brocade Fabric OS before 9.2.1 has a vulnerability that could allow a local authenticated attacker to reveal command line passwords using commands that may expose higher privilege sensitive information by a lower privileged user.	N/A	More Details
CVE-2025-12774	A vulnerability in the migration script for Brocade SANnav before 3.0 could allow the collection of database sql queries in the SANnav support save file. An attacker with access to Brocade SANnav supportsave file, could open the file and then obtain sensitive information such as details of database tables and encrypted passwords.	N/A	More Details
CVE-2025-61650	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation CheckUser. This vulnerability is associated with program files src/Services/CheckUserUserInfoCardService.Php. This issue affects CheckUser: from * before 795bf333272206a0189050d975e94b70eb7dc507.	N/A	More Details
CVE-2025-61649	Vulnerability in Wikimedia Foundation CheckUser. This vulnerability is associated with program files src/Services/CheckUserUserInfoCardService.Php. This issue affects CheckUser: from 7cedd58781d261f110651b6af4f41d2d11ae7309.	N/A	More Details
CVE-2025-61646	Vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/RecentChanges/EnhancedChangesList.Php. This issue affects MediaWiki: from * before 1.39.14, 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-61658	Vulnerability in Wikimedia Foundation CheckUser. This vulnerability is associated with program files src/GlobalContributions/GlobalContributionsPager.Php. This issue affects CheckUser: from * before 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-61645	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/pager/CodexTablePager.Php. This issue affects MediaWiki: from * before 1.44.1.	N/A	More Details
CVE-2025-15556	Notepad++ versions prior to 8.8.9, when using the WinGUp updater, contain an update integrity verification vulnerability where downloaded update metadata and installers are not cryptographically verified. An attacker able to intercept or redirect update traffic can cause the updater to download and execute an attacker-controlled installer, resulting in arbitrary code execution with the privileges of the user.	N/A	More Details
CVE-2025-12773	A vulnerability in update-reports-purge-settings.sh script logging for Brocade SANnav before 2.4.0a could allow the collection of SANnav database password in the system audit logs. The vulnerability could allow a remote authenticated attacker with access to the audit logs to access the Brocade SANnav database password.	N/A	More Details
CVE-2025-11261	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files resources/src/mediawiki.Language/mediawiki.Language.Js. This issue affects MediaWiki: from * before 1.39.15, 1.43.5, 1.44.2.	N/A	More Details
CVE-2025-	Vulnerability in Wikimedia Foundation OATHAuth. This vulnerability is associated with program files src/Special/OATHManage.Php. This issue affects OATHAuth: from * before	N/A	More

11173	1.39.14, 1.43.4, 1.44.1.		Details
CVE-2025-61647	Vulnerability in Wikimedia Foundation CheckUser. This vulnerability is associated with program files src/Api/Rest/Handler/UserInfoHandler.Php. This issue affects CheckUser: from a3dc1bbcc33acbcca6831d6afaccbb1054c93a57, 0584eb2ad564648aa3ce9c555dd044dda02b55f4.	N/A	More Details
CVE-2025-61644	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files resources/src/mediawiki.Rcfilters/ui/WatchlistTopSectionWidget.Js. This issue affects MediaWiki: from * before > fb856ce9cf121e046305116852cca4899ecb48ca.	N/A	More Details
CVE-2025-61643	Vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/recentchanges/RecentChangeRCFeedNotifier.Php. This issue affects MediaWiki: from * before 1.39.14, 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-61642	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/htmlform/CodexHTMLForm.Php, includes/htmlform/fields/HTMLButtonField.Php. This issue affects MediaWiki: from * before 1.39.14, 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-61641	Vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/api/ApiQueryAllPages.Php. This issue affects MediaWiki: from * before 1.39.14, 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-61640	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files resources/src/mediawiki.Rcfilters/ui/RclToOrFromWidget.Js. This issue affects MediaWiki: from * before 1.39.14, 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-61639	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/logging/ManualLogEntry.Php, includes/recentchanges/RecentChangeFactory.Php, includes/recentchanges/RecentChangeStore.Php. This issue affects MediaWiki: from * before 1.39.14, 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-61657	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation Vector. This vulnerability is associated with program files resources/skins.Vector.Js/stickyHeader.Js. This issue affects Vector: from * before 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-67475	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/CommentFormatter/CommentParser.Php. This issue affects MediaWiki: from * before 1.39.16, 1.43.6, 1.44.3, 1.45.1.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Pass netdev to mlx5e_destroy_netdev instead of priv mlx5e_priv is an unstable structure that can be memset(0) if profile attaching fails. Pass netdev to mlx5e_destroy_netdev() to guarantee it will work on a valid netdev. On mlx5e_remove: Check validity of priv->profile, before attempting to cleanup any resources that might be not there. This fixes a kernel oops in mlx5e_remove when switchdev mode fails due to change profile failure. $ devlink dev eswitch set pci/0000:00:03.0 mode switchdev Error: mlx5_core: Failed setting eswitch to offloads. dmesg: workqueue: Failed to create a rescuer kthread for wq "mlx5e": -EINTR mlx5_core 0012:03:00.1: mlx5e_netdev_init_profile:6214:(pid 37199): mlx5e_priv_init failed, err=-12 mlx5_core 0012:03:00.1 gpu3rdma1: mlx5e_netdev_change_profile: new profile init failed, -12 workqueue: Failed to create a rescuer kthread for wq "mlx5e": -EINTR mlx5_core 0012:03:00.1: mlx5e_netdev_init_profile:6214:(pid 37199): mlx5e_priv_init failed, err=-12 mlx5_core 0012:03:00.1 gpu3rdma1:		

CVE-2026-23035	mlx5e_netdev_change_profile: failed to rollback to orig profile, -12 $ devlink dev reload pci/0000:00:03.0 ==> oops BUG: kernel NULL pointer dereference, address: 0000000000000370 PGD 0 P4D 0 Oops: Oops: 0000 [#1] SMP NOPTI CPU: 15 UID: 0 PID: 520 Comm: devlink Not tainted 6.18.0-rc5+ #115 PREEMPT(voluntary) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 RIP: 0010:mlx5e_dcbnl_dscp_app+0x23/0x100 RSP: 0018:ffffc9000083f8b8 EFLAGS: 00010286 RAX: ffff8881126fc380 RBX: ffff8881015ac400 RCX: ffffffff826ffc45 RDX: 0000000000000000 RSI: 0000000000000001 RDI: ffff8881035109c0 RBP: ffff8881035109c0 R08: ffff888101e3e838 R09: ffff888100264e10 R10: ffffc9000083f898 R11: ffffc9000083f8a0 R12: ffff888101b921a0 R13: ffff888101b921a0 R14: ffff8881015ac9a0 R15: ffff8881015ac400 FS: 00007f789a3c8740(0000) GS:ffff88856aa59000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000370 CR3: 000000010b6c0001 CR4: 0000000000370ef0 Call Trace: <TASK> mlx5e_remove+0x57/0x110 device_release_driver_internal+0x19c/0x200 bus_remove_device+0xc6/0x130 device_del+0x160/0x3d0 ? devl_param_driverinit_value_get+0x2d/0x90 mlx5_detach_device+0x89/0xe0 mlx5_unload_one_devl_locked+0x3a/0x70 mlx5_devlink_reload_down+0xc8/0x220 devlink_reload+0x7d/0x260 devlink_nl_reload_doit+0x45b/0x5a0 genl_family_rcv_msg_doit+0xe8/0x140	N/A	More Details
CVE-2026-1788	: Out-of-bounds Write vulnerability in Xquic Project Xquic Server xquic on Linux (QUIC protocol implementation, packet processing module modules) allows : Buffer Manipulation.This issue affects Xquic Server: through 1.8.3.	N/A	More Details
CVE-2025-11598	In mObywatel iOS application an unauthorized user can use the App Switcher to view the account owner's personal information in the minimized app window, even after the login session has ended (reopening the app would require the user to log in). The data exposed depends on the last application view displayed before the application was minimized This issue was fixed in version 4.71.0	N/A	More Details
CVE-2025-59902	HTML injection vulnerability in NICE Chat. This vulnerability allows an attacker to inject and render arbitrary HTML content in email transcripts by modifying the 'firstName' and 'lastName' parameters during a chat session. The injected HTML is included in the body of the email sent by the system, which could enable phishing attacks, impersonation, or credential theft.	N/A	More Details
CVE-2025-41065	Stored Cross-Site Scripting (XSS) vulnerability type in LUNA software v7.5.5.6. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by inyecting a malicious payload through the 'Edit Batch Name' function. THe payload is stored by the application and subsequently displayed without proper sanitization when other users access it. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user.	N/A	More Details
CVE-2026-24465	Stack-based buffer overflow vulnerability exists in ELECOM wireless LAN access point devices. A crafted packet may lead to arbitrary code execution.	N/A	More Details
CVE-2026-24449	For WRC-X1500GS-B and WRC-X1500GSA-B, the initial passwords can be calculated easily from the system information.	N/A	More Details
CVE-2026-22550	OS command injection vulnerability exists in WRC-X1500GS-B and WRC-X1500GSA-B. A crafted request from a logged-in user may lead to an arbitrary OS command execution.	N/A	More Details
CVE-2026-20704	Cross-site request forgery vulnerability exists in WRC-X1500GS-B and WRC-X1500GSA-B. If a user accesses a malicious page while logged-in to the affected product, unintended operations may be performed.	N/A	More Details
CVE-2026-24694	The installer for Roland Cloud Manager ver.3.1.19 and prior insecurely loads Dynamic Link Libraries (DLLs), which could allow an attacker to execute arbitrary code with the privileges of the application.	N/A	More Details

CVE-2025-9711	A vulnerability in Brocade Fabric OS before 9.2.1c3 could allow elevating the privileges of the local authenticated user to “root” using the export option of seccertmgmt and seccryptocfg commands.	N/A	More Details
CVE-2025-58381	A vulnerability in Brocade Fabric OS before 9.2.1c2 could allow an authenticated attacker with admin privileges using the shell commands “source, ping6, sleep, disown, wait to modify the path variables and move upwards in the directory structure or to traverse to different directories.	N/A	More Details
CVE-2025-58380	A vulnerability in Brocade Fabric OS before 9.2.1 could allow an authenticated attacker with admin privileges using the shell command “grep” to modify the path variables and move upwards in the directory structure or to traverse to different directories.	N/A	More Details
CVE-2026-24936	When a specific function is enabled while joining a AD Domain from ADM, an improper input parameters validation vulnerability in a specific CGI program allowing an unauthenticated remote attacker to write arbitrary data to any file on the system. By exploiting this vulnerability, attackers can overwrite critical system files, leading to a complete system compromise. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.ROF1 as well as from ADM 5.0.0 through ADM 5.1.1.RCI1.	N/A	More Details
CVE-2026-0383	A vulnerability in Brocade Fabric OS could allow an authenticated, local attacker with privileges to access the Bash shell to access insecurely stored file contents including the history command.	N/A	More Details
CVE-2025-67476	Vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/Import/ImportableOldRevisionImporter.Php. This issue affects MediaWiki: from * before 1.44.3, 1.45.1.	N/A	More Details
CVE-2026-24935	A third-party NAT traversal module fails to validate SSL/TLS certificates when connecting to the signaling server. While subsequent access to device services requires additional authentication, a Man-in-the-Middle (MitM) attacker can intercept or redirect the NAT tunnel establishment. This could allow an attacker to disrupt service availability or facilitate further targeted attacks by acting as a proxy between the user and the device services. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.ROF1 as well as from ADM 5.0.0 through ADM 5.1.1.RCI1.	N/A	More Details
CVE-2026-24934	The DDNS function uses an insecure HTTP connection or fails to validate the SSL/TLS certificate when querying an external server for the device's WAN IP address. An unauthenticated remote attacker can perform a Man-in-the-Middle (MitM) attack to spoof the response, leading the device to update its DDNS record with an incorrect IP address. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.ROF1 as well as from ADM 5.0.0 through ADM 5.1.1.RCI1.	N/A	More Details
CVE-2026-24933	The API communication component fails to validate the SSL/TLS certificate when sending HTTPS requests to the server. An improper certificates validation vulnerability allows an unauthenticated remote attacker can perform a Man-in-the-Middle (MitM) attack to intercept the cleartext communication, potentially leading to the exposure of sensitive user information, including account emails, MD5 hashed passwords, and device serial numbers. Affected products and versions include: from ADM 4.1.0 through ADM 4.3.3.ROF1 as well as from ADM 5.0.0 through ADM 5.1.1.RCI1.	N/A	More Details
CVE-2026-24932	The DDNS update function in ADM fails to properly validate the hostname of the DDNS server's TLS/SSL certificate. Although the connection uses HTTPS, an improper validated TLS/SSL certificates allows a remote attacker can intercept the communication to perform a Man-in-the-Middle (MitM) attack, which may obtain the sensitive information of DDNS updating process, including the user's account email, MD5 hashed password, and device serial number.This issue affects ADM: from 4.1.0 through 4.3.3.ROF1, from 5.0.0 through 5.1.1.RCI1.	N/A	More Details
CVE-2025-67484	Vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/Api/ApiFormatXml.Php. This issue affects MediaWiki: from * before 1.39.16, 1.43.6, 1.44.3, 1.45.1.	N/A	More Details

CVE-2025-67483	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files resources/src/mediawiki.Page.Preview.Js. This issue affects MediaWiki: from * before 1.43.6, 1.44.3, 1.45.1.	N/A	More Details
CVE-2025-67482	Vulnerability in Wikimedia Foundation Scribunto, Wikimedia Foundation luasandbox. This vulnerability is associated with program files includes/Engines/LuaCommon/lualib/mwInit.Lua, library.C. This issue affects Scribunto: from * before 1.39.16, 1.43.6, 1.44.3, 1.45.1; luasandbox: from * before fea2304f8f6ab30314369a612f4f5b165e68e95a.	N/A	More Details
CVE-2025-67481	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files resources/src/mediawiki.JqueryMsg/mediawiki.JqueryMsg.Js. This issue affects MediaWiki: from * before 1.39.16, 1.43.6, 1.44.3, 1.45.1.	N/A	More Details
CVE-2025-67480	Vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/Api/ApiQueryRevisionsBase.Php. This issue affects MediaWiki: from * before 1.39.16, 1.43.6, 1.44.3, 1.45.1.	N/A	More Details
CVE-2025-67479	Vulnerability in Wikimedia Foundation MediaWiki, Wikimedia Foundation Cite. This vulnerability is associated with program files includes/Parser/CoreParserFunctions.Php, includes/Parser/Sanitizer.Php. This issue affects MediaWiki: from * before 1.39.14, 1.43.4, 1.44.1; Cite: from * before 1.39.14, 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-67478	Vulnerability in Wikimedia Foundation CheckUser. This vulnerability is associated with program files includes/Mail/UserMailer.Php. This issue affects CheckUser: from * before 1.39.14, 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-67477	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files resources/src/mediawiki.Special.Apisandbox/ApiSandboxLayout.Js. This issue affects MediaWiki: from * before 1.44.3, 1.45.1.	N/A	More Details
CVE-2025-61638	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki, Wikimedia Foundation Parsoid. This vulnerability is associated with program files includes/parser/Sanitizer.Php, src/Core/Sanitizer.Php. This issue affects MediaWiki: from * before 1.39.14, 1.43.4, 1.44.1; Parsoid: from * before 0.16.6, 0.20.4, 0.21.1.	N/A	More Details
CVE-2025-61637	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files resources/src/mediawiki.Action/mediawiki.Action.Edit.Preview.Js, resources/src/mediawiki.Page.Preview.Js. This issue affects MediaWiki: from * before 1.39.14, 1.43.4, 1.44.1.	N/A	More Details
CVE-2025-61636	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/htmlform/fields/HTMLButtonField.Php. This issue affects MediaWiki: from * before 1.39.14, 1.43.4, 1.44.1.	N/A	More Details
CVE-2024-4147	In lunary-ai/lunary version 1.2.13, an insufficient granularity of access control vulnerability allows users to delete prompts created in other organizations through ID manipulation. The vulnerability stems from the application's failure to validate the ownership of the prompt before deletion, only checking if the user has permissions to delete such resources without verifying if it belongs to the user's project or organization. As a result, users can remove prompts not owned by their organization or project, leading to legitimate users being unable to access the removed prompts and causing information inconsistencies.	N/A	More Details

CVE-2026-0630	An OS Command Injection vulnerability in TP-Link Archer BE230 v1.2(web modules) allows adjacent authenticated attacker to execute arbitrary code. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID.This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	N/A	More Details
CVE-2026-1770	Improper Control of Dynamically-Managed Code Resources vulnerability in Crafter Studio of Crafter CMS allows authenticated developers to execute OS commands via Groovy Sandbox Bypass. By inserting malicious Groovy elements, an attacker may bypass sandbox restrictions and obtain RCE (Remote Code Execution).	N/A	More Details
CVE-2026-1232	A medium-severity vulnerability has been identified in BeyondTrust Privilege Management for Windows versions <=25.7. Under certain conditions, a local authenticated user with elevated privileges may be able to bypass the product's anti-tamper protections, which could allow access to protected application components and the ability to modify product configuration.	N/A	More Details
CVE-2026-0921	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-1703	When pip is installing and extracting a maliciously crafted wheel archive, files may be extracted outside the installation directory. The path traversal is limited to prefixes of the installation directory, thus isn't able to inject or overwrite executable files in typical situations.	N/A	More Details
CVE-2026-1186	EAP Legislator is vulnerable to Path Traversal in file extraction functionality. Attacker can prepare zipx archive (default file type used by the Legislator application) and choose arbitrary path outside the intended directory (e.x. system startup) where files will be extracted by the victim upon opening the file. This issue was fixed in version 2.25a.	N/A	More Details
CVE-2026-0599	A vulnerability in huggingface/text-generation-inference version 3.3.6 allows unauthenticated remote attackers to exploit unbounded external image fetching during input validation in VLM mode. The issue arises when the router scans inputs for Markdown image links and performs a blocking HTTP GET request, reading the entire response body into memory and cloning it before decoding. This behavior can lead to resource exhaustion, including network bandwidth saturation, memory inflation, and CPU overutilization. The vulnerability is triggered even if the request is later rejected for exceeding token limits. The default deployment configuration, which lacks memory usage limits and authentication, exacerbates the impact, potentially crashing the host machine. The issue is resolved in version 3.3.7.	N/A	More Details
CVE-2025-7105	A vulnerability in danny-avila/librechat allows attackers to exploit the unrestricted Fork Function in `/api/convos/fork` to fork numerous contents rapidly. If the forked content includes a Mermaid graph with a large number of nodes, it can lead to a JavaScript heap out of memory error upon service restart, causing a denial of service. This issue affects the latest version of the product.	N/A	More Details
CVE-2025-6208	The `SimpleDirectoryReader` component in `llama_index.core` version 0.12.23 suffers from uncontrolled memory consumption due to a resource management flaw. The vulnerability arises because the user-specified file limit (`num_files_limit`) is applied after all files in a directory are loaded into memory. This can lead to memory exhaustion and degraded performance, particularly in environments with limited resources. The issue is resolved in version 0.12.41.	N/A	More Details
CVE-2025-10279	In mlflow version 2.20.3, the temporary directory used for creating Python virtual environments is assigned insecure world-writable permissions (0o777). This vulnerability allows an attacker with write access to the `/tmp` directory to exploit a race condition and overwrite `.py` files in the virtual environment, leading to arbitrary code execution.	N/A	More Details

	The issue is resolved in version 3.4.0.		
CVE-2024-5986	A vulnerability in h2oai/h2o-3 version 3.46.0.1 allows remote attackers to write arbitrary data to any file on the server. This is achieved by exploiting the `/3/Parse` endpoint to inject attacker-controlled data as the header of an empty file, which is then exported using the `/3/Frames/framename/export` endpoint. The impact of this vulnerability includes the potential for remote code execution and complete access to the system running h2o-3, as attackers can overwrite critical files such as private SSH keys or script files.	N/A	More Details
CVE-2024-5386	In lunary-ai/lunary version 1.2.2, an account hijacking vulnerability exists due to a password reset token leak. A user with a 'viewer' role can exploit this vulnerability to hijack another user's account by obtaining the password reset token. The vulnerability is triggered when the 'viewer' role user sends a specific request to the server, which responds with a password reset token in the 'recoveryToken' parameter. This token can then be used to reset the password of another user's account without authorization. The issue results from an excessive attack surface, allowing lower-privileged users to escalate their privileges and take over accounts.	N/A	More Details
CVE-2024-2356	A Local File Inclusion (LFI) vulnerability exists in the '/reinstall_extension' endpoint of the parisneo/lollms-webui application, specifically within the `name` parameter of the `@router.post("/reinstall_extension")` route. This vulnerability allows attackers to inject a malicious `name` parameter, leading to the server loading and executing arbitrary Python files from the upload directory for discussions. This issue arises due to the concatenation of `data.name` directly with `lollmsElfServer.lollms_paths.extensions_zoo_path` and its use as an argument for `ExtensionBuilder().build_extension()`. The server's handling of the `__init__.py` file in arbitrary locations, facilitated by `importlib.machinery.SourceFileLoader`, enables the execution of arbitrary code, such as command execution or creating a reverse-shell connection. This vulnerability affects the latest version of parisneo/lollms-webui and can lead to Remote Code Execution (RCE) when the application is exposed to an external endpoint or the UI, especially when bound to `0.0.0.0` or in `headless mode`. No user interaction is required for exploitation.	N/A	More Details
CVE-2025-61635	Vulnerability in Wikimedia Foundation ConfirmEdit. This vulnerability is associated with program files includes/FancyCaptcha/ApiFancyCaptchaReload.Php. This issue affects ConfirmEdit: *.	N/A	More Details
CVE-2026-1117	A vulnerability in the `lollms_generation_events.py` component of parisneo/lollms version 5.9.0 allows unauthenticated access to sensitive Socket.IO events. The `add_events` function registers event handlers such as `generate_text`, `cancel_generation`, `generate_msg`, and `generate_msg_from` without implementing authentication or authorization checks. This allows unauthenticated clients to execute resource-intensive or state-altering operations, leading to potential denial of service, state corruption, and race conditions. Additionally, the use of global flags (`lollmsElfServer.busy`, `lollmsElfServer.cancel_gen`) for state management in a multi-client environment introduces further vulnerabilities, enabling one client's actions to affect the server's state and other clients' operations. The lack of proper access control and reliance on insecure global state management significantly impacts the availability and integrity of the service.	N/A	More Details
CVE-2026-20401	In Modem, there is a possible system crash due to an uncaught exception. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01738310; Issue ID: MSV-5933.	N/A	More Details
CVE-2026-22888	Improper input verification issue exists in Cybozu Garoon 5.0.0 to 6.0.3, which may lead to unauthorized alteration of portal settings, potentially blocking access to the product.	N/A	More Details
CVE-	Cross-site scripting vulnerability exists in Message function of Cybozu Garoon 5.15.0 to		More

2026-22881	6.0.3, which may allow an attacker to reset arbitrary users’ passwords.	N/A	Details
CVE-2026-20711	Cross-site scripting vulnerability exists in E-mail function of Cybozu Garoon 5.0.0 to 6.0.3, which may allow an attacker to reset arbitrary users’ passwords.	N/A	More Details
CVE-2026-24788	RaspAP raspap-webgui versions prior to 3.3.6 contain an OS command injection vulnerability. If exploited, an arbitrary OS command may be executed by a user who can log in to the product.	N/A	More Details
CVE-2025-13348	An improper access control vulnerability exists in ASUS Secure Delete Driver of ASUS Business Manager. This vulnerability can be triggered by a local user sending a specially crafted request, potentially leading to the creation of arbitrary files in a specified path. Refer to the "Security Update for ASUS Business Manager" section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-25069	SunFounder Pironman Dashboard (pm_dashboard) version 1.3.13 and prior contain a path traversal vulnerability in the log file API endpoints. An unauthenticated remote attacker can supply traversal sequences via the filename parameter to read and delete arbitrary files. Successful exploitation can disclose sensitive information and delete critical system files, resulting in data loss and potential system compromise or denial of service.	N/A	More Details
CVE-2026-23039	In the Linux kernel, the following vulnerability has been resolved: drm/gud: fix NULL fb and crtc dereferences on USB disconnect On disconnect drm_atomic_helper_disable_all() is called which sets both the fb and crtc for a plane to NULL before invoking a commit. This causes a kernel oops on every display disconnect. Add guards for those dereferences.	N/A	More Details
CVE-2026-23038	In the Linux kernel, the following vulnerability has been resolved: pnfs/flexfiles: Fix memory leak in nfs4_ff_alloc_deviceid_node() In nfs4_ff_alloc_deviceid_node(), if the allocation for ds_versions fails, the function jumps to the out_scratch label without freeing the already allocated dsaddrs list, leading to a memory leak. Fix this by jumping to the out_err_drain_dsaddrs label, which properly frees the dsaddrs list before cleaning up other resources.	N/A	More Details
CVE-2026-23037	In the Linux kernel, the following vulnerability has been resolved: can: etas_es58x: allow partial RX URB allocation to succeed When es58x_alloc_rx_urbs() fails to allocate the requested number of URBs but succeeds in allocating some, it returns an error code. This causes es58x_open() to return early, skipping the cleanup label 'free_urbs', which leads to the anchored URBs being leaked. As pointed out by maintainer Vincent Mailhol, the driver is designed to handle partial URB allocation gracefully. Therefore, partial allocation should not be treated as a fatal error. Modify es58x_alloc_rx_urbs() to return 0 if at least one URB has been allocated, restoring the intended behavior and preventing the leak in es58x_open().	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: btrfs: release path before iget_failed() in btrfs_read_locked_inode() In btrfs_read_locked_inode() if we fail to lookup the inode, we jump to the 'out' label with a path that has a read locked leaf and then we call iget_failed(). This can result in a ABBA deadlock, since iget_failed() triggers inode eviction and that causes the release of the delayed inode, which must lock the delayed inode's mutex, and a task updating a delayed inode starts by taking the node's mutex and then modifying the inode's subvolume btree. Syzbot reported the following lockdep splat for this: == WARNING: possible circular locking dependency detected syzkaller #0 Not tainted -- btrfs-cleaner/8725 is trying to acquire lock: ffff0000d6826a48 (&delayed_node->mutex){+.+.}-{4:4}, at: __btrfs_release_delayed_node+0xa0/0x9b0 fs/btrfs/delayed-inode.c:290 but task is already holding lock: ffff0000dbeba878 (btrfs-tree-00){++++}-{4:4}, at: btrfs_tree_read_lock_nested+0x44/0x2ec fs/btrfs/locking.c:145 which lock already depends on the new lock. the existing dependency chain (in reverse order) is: -> #1		

CVE-2026-23036	(btrfs-tree-00){++++}-{4:4}: __lock_release kernel/locking/lockdep.c:5574 [inline] lock_release+0x198/0x39c kernel/locking/lockdep.c:5889 up_read+0x24/0x3c kernel/locking/rwsem.c:1632 btrfs_tree_read_unlock+0xdc/0x298 fs/btrfs/locking.c:169 btrfs_tree_unlock_rw fs/btrfs/locking.h:218 [inline] btrfs_search_slot+0xa6c/0x223c fs/btrfs/ctree.c:2133 btrfs_lookup_inode+0xd8/0x38c fs/btrfs/inode-item.c:395 __btrfs_update_delayed_inode+0x124/0xed0 fs/btrfs/delayed-inode.c:1032 btrfs_update_delayed_inode fs/btrfs/delayed-inode.c:1118 [inline] __btrfs_commit_inode_delayed_items+0x15f8/0x1748 fs/btrfs/delayed-inode.c:1141 __btrfs_run_delayed_items+0x1ac/0x514 fs/btrfs/delayed-inode.c:1176 btrfs_run_delayed_items_nr+0x28/0x38 fs/btrfs/delayed-inode.c:1219 flush_space+0x26c/0xb68 fs/btrfs/space-info.c:828 do_async_reclaim_metadata_space+0x110/0x364 fs/btrfs/space-info.c:1158 btrfs_async_reclaim_metadata_space+0x90/0xd8 fs/btrfs/space-info.c:1226 process_one_work+0x7e8/0x155c kernel/workqueue.c:3263 process_scheduled_works kernel/workqueue.c:3346 [inline] worker_thread+0x958/0xed8 kernel/workqueue.c:3427 kthread+0x5fc/0x75c kernel/kthread.c:463 ret_from_fork+0x10/0x20 arch/arm64/kernel/entry.S:844 -> #0 (&delayed_node->mutex){+.+.}-{4:4}: check_prev_add kernel/locking/lockdep.c:3165 [inline] check_prevs_add kernel/locking/lockdep.c:3284 [inline] validate_chain kernel/locking/lockdep.c:3908 [inline] __lock_acquire+0x1774/0x30a4 kernel/locking/lockdep.c:5237 lock_acquire+0x14c/0x2e0 kernel/locking/lockdep.c:5868 __mutex_lock_common+0x1d0/0x2678 kernel/locking/mutex.c:598 __mutex_lock kernel/locking/mutex.c:760 [inline] mutex_lock_nested+0x2c/0x38 kernel/locking/mutex.c:812 __btrfs_release_delayed_node+0xa0/0x9b0 fs/btrfs/delayed-inode.c:290 btrfs_release_delayed_node fs/btrfs/delayed-inode.c:315 [inline] btrfs_remove_delayed_node+0x68/0x84 fs/btrfs/delayed-inode.c:1326 btrfs_evict_inode+0x578/0xe28 fs/btrfs/inode.c:5587 evict+0x414/0x928 fs/inode.c:810 iput_final fs/inode.c:1914 [inline] iput+0x95c/0xad4 fs/inode.c:1966 iget_failed+0xec/0x134 fs/bad_inode.c:248 btrfs_read_locked_inode+0xe1c/0x1234 fs/btrfs/inode.c:4101 btrfs_iget+0x1b0/0x264 fs/btrfs/inode.c:5837 btrfs_run_defrag_inode fs/btrfs/defrag.c:237 [inline] btrfs_run_defrag_inodes+0x520/0xdc4 fs/btrf ---truncated---	N/A	More Details
CVE-2026-0631	An OS Command Injection vulnerability in TP-Link Archer BE230 v1.2(vpn modules) allows an adjacent authenticated attacker to execute arbitrary code. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID.This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	N/A	More Details
CVE-2026-22221	An OS Command Injection vulnerability in TP-Link Archer BE230 v1.2(vpn modules) allows adjacent authenticated attacker execute arbitrary code. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID.This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	N/A	More Details
CVE-2026-22222	An OS Command Injection vulnerability in TP-Link Archer BE230 v1.2(web modules) allows adjacent authenticated attacker to execute arbitrary code. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID.This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	N/A	More Details
CVE-	An OS Command Injection vulnerability in TP-Link Archer BE230 v1.2(vpn modules) allows adjacent authenticated attacker execute arbitrary code. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe		More

2026-22223	compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID.This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	N/A	Details
CVE-2025-61634	Vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/Rest/Handler/PageHTMLHandler.Php. This issue affects MediaWiki: from * before 1.39.14, 1.43.4, 1.44.1.	N/A	More Details
CVE-2026-25222	PolarLearn is a free and open-source learning program. In 0-PRERELEASE-15 and earlier, a timing attack vulnerability in the sign-in process allows unauthenticated attackers to determine if a specific email address is registered on the platform. By measuring the response time of the login endpoint, an attacker can distinguish between valid and invalid email addresses. This occurs because the server only performs the computationally expensive Argon2 password hashing if the user exists in the database. Requests for existing users take significantly longer (~650ms) than requests for non-existent users (~160ms).	N/A	More Details
CVE-2026-25221	PolarLearn is a free and open-source learning program. In 0-PRERELEASE-15 and earlier, the OAuth 2.0 implementation for GitHub and Google login providers is vulnerable to Login Cross-Site Request Forgery (CSRF). The application fails to implement and verify the state parameter during the authentication flow. This allows an attacker to pre-authenticate a session and trick a victim into logging into the attacker's account. Any data the victim then enters or academic progress they make is stored on the attacker's account, leading to data loss for the victim and information disclosure to the attacker.	N/A	More Details
CVE-2026-25134	Group-Office is an enterprise customer relationship management and groupware tool. Prior to 6.8.150, 25.0.82, and 26.0.5, the MaintenanceController exposes an action zipLanguage which takes a lang parameter and passes it directly to a system zip command via exec(). This can be combined with uploading a crafted zip file to achieve remote code execution. This vulnerability is fixed in 6.8.150, 25.0.82, and 26.0.5.	N/A	More Details
CVE-2026-24471	continuwuity is a Matrix homeserver written in Rust. This vulnerability allows an attacker with a malicious remote server to cause the local server to sign an arbitrary event upon user interaction. Upon a user account leaving a room (rejecting an invite), joining a room or knocking on a room, the victim server may ask a remote server for assistance. If the victim asks the attacker server for assistance the attacker is able to provide an arbitrary event, which the victim will sign and return to the attacker. For the /leave endpoint, this works for any event with a supported room version, where the origin and origin_server_ts is set by the victim. For the /join endpoint, an additionally victim-set content field in the format of a join membership is needed. For the /knock endpoint, an additional victim-set content field in the format of a knock membership and a room version not between 1 and 6 is needed. This was exploited as a part of a larger chain against the continuwuity.org homeserver. This vulnerability affects all Conduit-derived servers. This vulnerability is fixed in Continuwuity 0.5.1, Conduit 0.10.11, Grapevine 0aae932b, and Tuwunel 1.4.9.	N/A	More Details
CVE-2026-24133	jsPDF is a library to generate PDFs in JavaScript. Prior to 4.1.0, user control of the first argument of the addImage method results in denial of service. If given the possibility to pass unsanitized image data or URLs to the addImage method, a user can provide a harmful BMP file that results in out of memory errors and denial of service. Harmful BMP files have large width and/or height entries in their headers, which lead to excessive memory allocation. The html method is also affected. The vulnerability has been fixed in jsPDF@4.1.0.	N/A	More Details
CVE-2026-24043	jsPDF is a library to generate PDFs in JavaScript. Prior to 4.1.0, user control of the first argument of the addMetadata function allows users to inject arbitrary XML. If given the possibility to pass unsanitized input to the addMetadata method, a user can inject arbitrary XMP metadata into the generated PDF. If the generated PDF is signed, stored or otherwise processed after, the integrity of the PDF can no longer be guaranteed. The vulnerability has been fixed in jsPDF@4.1.0.	N/A	More Details

CVE-2026-24040	jsPDF is a library to generate PDFs in JavaScript. Prior to 4.1.0, the addJS method in the jspdf Node.js build utilizes a shared module-scoped variable (text) to store JavaScript content. When used in a concurrent environment (e.g., a Node.js web server), this variable is shared across all requests. If multiple requests generate PDFs simultaneously, the JavaScript content intended for one user may be overwritten by a subsequent request before the document is generated. This results in Cross-User Data Leakage, where the PDF generated for User A contains the JavaScript payload (and any embedded sensitive data) intended for User B. Typically, this only affects server-side environments, although the same race conditions might occur if jsPDF runs client-side. The vulnerability has been fixed in jsPDF@4.1.0.	N/A	More Details
CVE-2026-0924	BuhoCleaner contains an insecure XPC service that allows local, unprivileged users to escalate their privileges to root via insecure functions.This issue affects BuhoCleaner: 1.15.2.	N/A	More Details
CVE-2025-6927	Vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/specials/pagers/BlockListPager.Php, includes/api/ApiQueryBlocks.Php. This issue affects MediaWiki: from >= 1.42.0 before 1.39.13, 1.42.7 1.43.2, 1.44.0.	N/A	More Details
CVE-2025-6597	Vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/auth/AuthManager.Php. This issue affects MediaWiki: from * before 1.39.13, 1.42.7, 1.43.2, 1.44.0.	N/A	More Details
CVE-2025-6596	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation Vector. This vulnerability is associated with program files resources/skins.Vector.Js/portlets.Js, resources/skins.Vector.Legacy.Js/portlets.Js. This issue affects Vector: from >= 1.40.0 before 1.42.7, 1.43.2, 1.44.0.	N/A	More Details
CVE-2025-6593	Vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/user/User.Php. This issue affects MediaWiki: from 1.27.0 before 1.39.13, 1.42.7 1.43.2, 1.44.0.	N/A	More Details
CVE-2025-6592	Vulnerability in Wikimedia Foundation AbuseFilter. This vulnerability is associated with program files includes/auth/AuthManager.Php. This issue affects AbuseFilter: from fe0b1cb9e9691faf4d8d9bd80646589f6ec37615 before 1.43.2, 1.44.0.	N/A	More Details
CVE-2025-6591	Vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/api/ApiFeedContributions.Php. This issue affects MediaWiki: from * before 1.39.13, 1.42.7 1.43.2, 1.44.0.	N/A	More Details
CVE-2025-6590	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/htmlform/fields/HTMLUserTextField.Php. This issue affects MediaWiki: from * through 1.39.12, 1.42.76 1.43.1, 1.44.0.	N/A	More Details
CVE-2025-6589	Vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/specials/pagers/BlockListPager.Php. This issue affects MediaWiki: >= 1.42.0.	N/A	More Details
CVE-2025-12772	Brocade SANnav before 2.4.0b logs the Brocade Fabric OS Switch admin password on the SANnav support save logs. When OOM occurs on a Brocade SANnav server, the call stack trace for the Brocade switch is also collected in the heap dump file which contains this switch password in clear text. The vulnerability could allow a remote authenticated attacker with admin privilege able to access the SANnav logs or the supportsave to read the switch admin password.	N/A	More Details
CVE-2025-12680	Brocade SANnav before Brocade SANnav 2.4.0b logs database passwords in clear text in the standby SANnav server, after disaster recovery failover. The vulnerability could allow a remote authenticated attacker with admin privilege able to access the SANnav logs or the supportsave to read the database password.	N/A	More Details

CVE-2025-12679	A vulnerability in Brocade SANnav before 2.4.0b prints the Password-Based Encryption (PBE) key in plaintext in the system audit log file. The vulnerability could allow a remote authenticated attacker with access to the audit logs to access the pbe key. Note: The vulnerability is only triggered during a migration and not in a new installation. The system audit logs are accessible only to a privileged user on the server. These audit logs are the local server VM’s audit logs and are not controlled by SANnav. These logs are only visible to the server admin of the host server and are not visible to the SANnav admin or any SANnav user.	N/A	More Details
CVE-2026-22229	A command injection vulnerability may be exploited after the admin's authentication via the import of a crafted VPN client configuration file on the TP-Link Archer BE230 v1.2. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID. This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	N/A	More Details
CVE-2026-22227	A command injection vulnerability may be exploited after the admin's authentication via the configuration backup restoration function of the TP-Link Archer BE230 v1.2. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID. This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	N/A	More Details
CVE-2026-22226	A command injection vulnerability may be exploited after the admin's authentication in the VPN server configuration module on the TP-Link Archer BE230 v1.2. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID. This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	N/A	More Details
CVE-2026-22225	A command injection vulnerability may be exploited after the admin's authentication in the VPN Connection Service on the Archer BE230 v1.2. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID. This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	N/A	More Details
CVE-2026-22224	A command injection vulnerability may be exploited after the admin's authentication in the cloud communication interface on the TP-Link Archer BE230 v1.2. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID. This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	N/A	More Details
CVE-2021-47916	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details