SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 28 January 2026

Generated on 28 January 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-2025-4320	Authentication Bypass by Primary Weakness, Weak Password Recovery Mechanism for Forgotten Password vulnerability in Birebirsoft Software and Technology Solutions Sufirmam allows Authentication Bypass, Password Recovery Exploitation.This issue affects Sufirmam: through 23012026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	10.0	More Details
CVE-2025-69828	File Upload vulnerability in TMS Global Software TMS Management Console v.6.3.7.27386.20250818 allows a remote attacker to execute arbitrary code via the Logo upload in /Customer/AddEdit	10.0	More Details
CVE-2026-24304	Improper access control in Azure Resource Manager allows an authorized attacker to elevate privileges over a network.	9.9	More Details
CVE-2025-62050	Unrestricted Upload of File with Dangerous Type vulnerability in blazethemes Blogmatic blogmatic.This issue affects Blogmatic: from n/a through <= 1.0.3.	9.9	More Details
CVE-2025-62056	Unrestricted Upload of File with Dangerous Type vulnerability in blazethemes News Event news-event.This issue affects News Event: from n/a through <= 1.0.1.	9.9	More Details
CVE-2016-15057	** UNSUPPORTED WHEN ASSIGNED ** Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Apache Continuum. This issue affects Apache Continuum: all versions. Attackers with access to the installations REST API can use this to invoke arbitrary commands on the server. As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an	9.9	More Details

	alternative or restrict access to the instance to trusted users. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.		
CVE-2025-70982	Incorrect access control in the importUser function of SpringBlade v4.5.0 allows attackers with low-level privileges to arbitrarily import sensitive user data.	9.9	More Details
CVE-2026-1470	n8n contains a critical Remote Code Execution (RCE) vulnerability in its workflow Expression evaluation system. Expressions supplied by authenticated users during workflow configuration may be evaluated in an execution context that is not sufficiently isolated from the underlying runtime. An authenticated attacker could abuse this behavior to execute arbitrary code with the privileges of the n8n process. Successful exploitation may lead to full compromise of the affected instance, including unauthorized access to sensitive data, modification of workflows, and execution of system-level operations.	9.9	More Details
CVE-2025-70983	Incorrect access control in the authRoutes function of SpringBlade v4.5.0 allows attackers with low-level privileges to escalate privileges.	9.9	More Details
CVE-2026-22039	Kyverno is a policy engine designed for cloud native platform engineering teams. Versions prior to 1.16.3 and 1.15.3 have a critical authorization boundary bypass in namespaced Kyverno Policy apiCall. The resolved \`urlPath\` is executed using the Kyverno admission controller ServiceAccount, with no enforcement that the request is limited to the policy’s namespace. As a result, any authenticated user with permission to create a namespaced Policy can cause Kyverno to perform Kubernetes API requests using Kyverno’s admission controller identity, targeting any API path allowed by that ServiceAccount’s RBAC. This breaks namespace isolation by enabling cross-namespace reads (for example, ConfigMaps and, where permitted, Secrets) and allows cluster-scoped or cross-namespace writes (for example, creating ClusterPolicies) by controlling the urlPath through context variable substitution. Versions 1.16.3 and 1.15.3 contain a patch for the vulnerability.	9.9	More Details
CVE-2026-1363	IAQS and I6 developed by JNC has a Client-Side Enforcement of Server-Side Security vulnerability, allowing unauthenticated remote attackers to gain administrator privileges by manipulating the web front-end.	9.8	More Details
CVE-2026-1364	IAQS and I6 developed by JNC has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to directly operate system administrative functionalities.	9.8	More Details
CVE-2025-70457	A Remote Code Execution (RCE) vulnerability exists in Sourcecodester Modern Image Gallery App v1.0 within the gallery/upload.php component. The application fails to properly validate uploaded file contents. Additionally, the application preserves the user-supplied file extension during the save process. This allows an unauthenticated attacker to upload arbitrary PHP code by spoofing the MIME type as an image, leading to full system compromise.	9.8	More Details
CVE-2026-24306	Improper access control in Azure Front Door (AFD) allows an unauthorized attacker to elevate privileges over a network.	9.8	More Details
CVE-2026-24531	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Prowess prowess allows PHP Local File Inclusion.This issue affects Prowess: from n/a through <= 2.3.	9.8	More Details
CVE-2021-47891	Unified Remote 3.9.0.2463 contains a remote code execution vulnerability that allows attackers to send crafted network packets to execute arbitrary commands. Attackers can exploit the service by connecting to port 9512 and sending specially crafted packets to open a command prompt and download and execute malicious payloads.	9.8	More Details
CVE-	telnetd in GNU Inetutils through 2.7 allows remote authentication bypass via a "-f root"		More

2026-24061	value for the USER environment variable.	9.8	Details
CVE-2025-56590	An issue was discovered in the InsertFromURL() function of the Apryse HTML2PDF SDK thru 11.10. This vulnerability could allow an attacker to execute arbitrary operating system commands on the local server.	9.8	More Details
CVE-2022-25369	An issue was discovered in Dynamicweb before 9.12.8. An attacker can add a new administrator user without authentication. This flaw exists due to a logic issue when determining if the setup phases of the product can be run again. Once an attacker is authenticated as the new admin user they have added, it is possible to upload an executable file and achieve command execution. This is fixed in 9.5.9, 9.6.16, 9.7.8, 9.8.11, 9.9.8, 9.10.18, 9.12.8, and 9.13.0 (and later).	9.8	More Details
CVE-2025-67229	An improper certificate validation vulnerability exists in ToDesktop Builder v0.32.1 This vulnerability allows an unauthenticated, on-path attacker to spoof backend responses by exploiting insufficient certificate validation.	9.8	More Details
CVE-2026-24371	Missing Authorization vulnerability in bookingalgorithms BA Book Everything ba-book-everything allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects BA Book Everything: from n/a through <= 1.8.16.	9.8	More Details
CVE-2025-15521	The Academy LMS – WordPress LMS Plugin for Complete eLearning Solution plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.5.0. This is due to the plugin not properly validating a user's identity prior to updating their password and relying solely on a publicly-exposed nonce for authorization. This makes it possible for unauthenticated attackers to change arbitrary user's password, including administrators, and gain access to their account.	9.8	More Details
CVE-2026-22585	Use of a Broken or Risky Cryptographic Algorithm vulnerability in Salesforce Marketing Cloud Engagement (CloudPages, Forward to a Friend, Profile Center, Subscription Center, Unsub Center, View As Webpage modules) allows Web Services Protocol Manipulation. This issue affects Marketing Cloud Engagement: before January 21st, 2026.	9.8	More Details
CVE-2026-22582	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability in Salesforce Marketing Cloud Engagement (MicrositeUrl module) allows Web Services Protocol Manipulation. This issue affects Marketing Cloud Engagement: before January 21st, 2026.	9.8	More Details
CVE-2026-22583	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability in Salesforce Marketing Cloud Engagement (CloudPagesUrl module) allows Web Services Protocol Manipulation. This issue affects Marketing Cloud Engagement: before January 21st, 2026.	9.8	More Details
CVE-2025-21589	An Authentication Bypass Using an Alternate Path or Channel vulnerability in Juniper Networks Session Smart Router may allows a network-based attacker to bypass authentication and take administrative control of the device. This issue affects Session Smart Router: * from 5.6.7 before 5.6.17, * from 6.0 before 6.0.8 (affected from 6.0.8), * from 6.1 before 6.1.12-lts, * from 6.2 before 6.2.8-lts, * from 6.3 before 6.3.3-r2; This issue affects Session Smart Conductor: * from 5.6.7 before 5.6.17, * from 6.0 before 6.0.8 (affected from 6.0.8), * from 6.1 before 6.1.12-lts, * from 6.2 before 6.2.8-lts, * from 6.3 before 6.3.3-r2; This issue affects WAN Assurance Managed Routers: * from 5.6.7 before 5.6.17, * from 6.0 before 6.0.8 (affected from 6.0.8), * from 6.1 before 6.1.12-lts, * from 6.2 before 6.2.8-lts, * from 6.3 before 6.3.3-r2.	9.8	More Details
CVE-2026-24858	An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.5, FortiAnalyzer 7.4.0 through 7.4.9, FortiAnalyzer 7.2.0 through 7.2.11, FortiAnalyzer 7.0.0 through 7.0.15, FortiManager 7.6.0 through 7.6.5, FortiManager 7.4.0 through 7.4.9, FortiManager 7.2.0 through 7.2.11, FortiManager 7.0.0 through 7.0.15, FortiOS 7.6.0 through 7.6.5, FortiOS 7.4.0 through 7.4.10, FortiOS 7.2.0 through 7.2.12, FortiOS 7.0.0 through 7.0.18 may allow an attacker with a FortiCloud account and a registered device to log into other devices registered to other accounts, if FortiCloud SSO authentication is enabled on	9.8	More Details

	those devices.		
CVE-2026-24872	improper pointer arithmetic vulnerability in ProjectSkyfire SkyFire_548.This issue affects SkyFire_548: before 5.4.8-stable5.	9.8	More Details
CVE-2026-24832	Out-of-bounds Write vulnerability in ixray-team ixray-1.6-stcop.This issue affects ixray-1.6-stcop: before 1.3.	9.8	More Details
CVE-2021-47901	Dirsearch 0.4.1 contains a CSV injection vulnerability when using the --csv-report flag that allows attackers to inject formulas through redirected endpoints. Attackers can craft malicious server redirects with comma-separated paths containing Excel formulas to manipulate the generated CSV report.	9.8	More Details
CVE-2021-47900	Gila CMS versions prior to 2.0.0 contain a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary system commands through manipulated HTTP headers. Attackers can inject PHP code in the User-Agent header with shell_exec() to run system commands by sending crafted requests to the admin endpoint.	9.8	More Details
CVE-2020-36948	VestaCP 0.9.8-26 contains a session token vulnerability in the LoginAs module that allows remote attackers to manipulate authentication tokens. Attackers can exploit insufficient token validation to access user accounts and perform unauthorized login requests without proper administrative permissions.	9.8	More Details
CVE-2020-36941	Knockpy 4.1.1 contains a CSV injection vulnerability that allows attackers to inject malicious formulas into CSV reports through unfiltered server headers. Attackers can manipulate server response headers to include spreadsheet formulas that will execute when the CSV is opened in spreadsheet applications.	9.8	More Details
CVE-2020-36940	Easy CD & DVD Cover Creator 4.13 contains a buffer overflow vulnerability in the serial number input field that allows attackers to crash the application. Attackers can generate a 6000-byte payload and paste it into the serial number field to trigger an application crash.	9.8	More Details
CVE-2026-24830	Integer Overflow or Wraparound vulnerability in Ralim IronOS.This issue affects IronOS: before v2.23-rc2.	9.8	More Details
CVE-2026-22709	vm2 is an open source vm/sandbox for Node.js. In vm2 prior to version 3.10.2, `Promise.prototype.then` `Promise.prototype.catch` callback sanitization can be bypassed. This allows attackers to escape the sandbox and run arbitrary code. In lib/setup-sandbox.js, the callback function of `localPromise.prototype.then` is sanitized, but `globalPromise.prototype.then` is not sanitized. The return value of async functions is `globalPromise` object. Version 3.10.2 fixes the issue.	9.8	More Details
CVE-2025-13374	The Kalrav AI Agent plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the kalrav_upload_file AJAX action in all versions up to, and including, 2.3.3. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2025-13952	A web page that contains unusual GPU shader code is loaded from the Internet into the GPU compiler process triggers a write use-after-free crash in the GPU shader compiler library. On certain platforms, when the compiler process has system privileges this could enable further exploits on the device. The shader code contained in the web page executes a path in the compiler that held onto an out of date pointer, pointing to a freed memory object.	9.8	More Details
CVE-2026-22586	Hard-coded Cryptographic Key vulnerability in Salesforce Marketing Cloud Engagement (CloudPages, Forward to a Friend, Profile Center, Subscription Center, Unsub Center, View As Webpage modules) allows Web Services Protocol Manipulation. This issue affects Marketing Cloud Engagement: before January 21st, 2026.	9.8	More Details

CVE-2026-23975	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in uxper Golo golo allows PHP Local File Inclusion.This issue affects Golo: from n/a through < 1.7.5.	9.8	More Details
CVE-2026-23978	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Softwebmedia Gyan Elements gyan-elements allows PHP Local File Inclusion.This issue affects Gyan Elements: from n/a through <= 2.2.1.	9.8	More Details
CVE-2026-24770	RAGFlow is an open-source RAG (Retrieval-Augmented Generation) engine. In version 0.23.1 and possibly earlier versions, the MinerU parser contains a "Zip Slip" vulnerability, allowing an attacker to overwrite arbitrary files on the server (leading to Remote Code Execution) via a malicious ZIP archive. The MinerUParser class retrieves and extracts ZIP files from an external source (mineru_server_url). The extraction logic in `_extract_zip_no_root` fails to sanitize filenames within the ZIP archive. Commit 64c75d558e4a17a4a48953b4c201526431d8338f contains a patch for the issue.	9.8	More Details
CVE-2025-50003	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Amuli amuli allows PHP Local File Inclusion.This issue affects Amuli: from n/a through <= 2.3.0.	9.8	More Details
CVE-2021-47854	DD-WRT version 45723 contains a buffer overflow vulnerability in the UPNP network discovery service that allows remote attackers to potentially execute arbitrary code. Attackers can send crafted M-SEARCH packets with oversized UUID payloads to trigger buffer overflow conditions on the target device.	9.8	More Details
CVE-2025-69766	Tenda AX3 firmware v16.03.12.11 contains a stack-based buffer overflow in the formGetIptv function due to improper handling of the citytag stack buffer, which may result in memory corruption and remote code execution.	9.8	More Details
CVE-2026-0920	The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Administrative User Creation in all versions up to, and including, 1.5.6.3. This is due to the 'ajax_register_handle' function not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'lakit_bkrole' parameter during registration and gain administrator access to the site.	9.8	More Details
CVE-2026-1331	MeetingHub developed by HAMASTAR Technology has an Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	9.8	More Details
CVE-2026-23760	SmarterTools SmarterMail versions prior to build 9511 contain an authentication bypass vulnerability in the password reset API. The force-reset-password endpoint permits anonymous requests and fails to verify the existing password or a reset token when resetting system administrator accounts. An unauthenticated attacker can supply a target administrator username and a new password to reset the account, resulting in full administrative compromise of the SmarterMail instance. NOTE: SmarterMail system administrator privileges grant the ability to execute operating system commands via built-in management functionality, effectively providing administrative (SYSTEM or root) access on the underlying host.	9.8	More Details
CVE-2025-69764	Tenda AX3 firmware v16.03.12.11 contains a stack-based buffer overflow in the formGetIptv function due to improper handling of the stbpvid stack buffer, which may result in memory corruption and remote code execution.	9.8	More Details
CVE-2025-47474	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Ninetheme Anarkali anarkali allows PHP Local File Inclusion.This issue affects Anarkali: from n/a through <= 1.0.9.	9.8	More Details
CVE-2025-49055	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in kamleshyadav WP Lead Capturing Pages wp-lead-capture allows Blind SQL Injection.This issue affects WP Lead Capturing Pages: from n/a through <= 2.5.	9.8	More Details
CVE-2025-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ovatheme Athens athens allows PHP Local File	9.8	More

49994	Inclusion.This issue affects Athens: from n/a through <= 1.1.6.		Details
CVE-2025-50002	Unrestricted Upload of File with Dangerous Type vulnerability in Farost Energia energia allows Upload a Web Shell to a Web Server.This issue affects Energia: from n/a through <= 1.1.2.	9.8	More Details
CVE-2025-69763	Tenda AX3 firmware v16.03.12.11 contains a stack overflow in formSetIptv via the vlanId parameter, which can cause memory corruption and enable remote code execution.	9.8	More Details
CVE-2025-54003	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Depot depot allows PHP Local File Inclusion.This issue affects Depot: from n/a through <= 1.16.	9.8	More Details
CVE-2025-69762	Tenda AX3 firmware v16.03.12.11 contains a stack overflow in formSetIptv via the list parameter, which can cause memory corruption and enable remote code execution.	9.8	More Details
CVE-2025-63017	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in fuelthemes WerkStatt Plugin werkstatt-plugin allows PHP Local File Inclusion.This issue affects WerkStatt Plugin: from n/a through <= 1.6.6.	9.8	More Details
CVE-2021-47875	GeoGebra CAS Calculator 6.0.631.0 contains a denial of service vulnerability that allows attackers to crash the application by generating a large buffer overflow. Attackers can create a payload with 8000 repeated characters and paste it into the calculator's input field to trigger an application crash.	9.8	More Details
CVE-2026-23524	Laravel Reverb provides a real-time WebSocket communication backend for Laravel applications. In versions 1.6.3 and below, Reverb passes data from the Redis channel directly into PHP’s unserialize() function without restricting which classes can be instantiated, which leaves users vulnerable to Remote Code Execution. The exploitability of this vulnerability is increased because Redis servers are commonly deployed without authentication, but only affects Laravel Reverb when horizontal scaling is enabled (REVERB_SCALING_ENABLED=true). This issue has been fixed in version 1.7.0. As a workaround, require a strong password for Redis access and ensure the service is only accessible via a private network or local loopback, and/or set REVERB_SCALING_ENABLED=false to bypass the vulnerable logic entirely (if the environment uses only one Reverb node).	9.8	More Details
CVE-2021-47851	Mini Mouse 9.2.0 contains a remote code execution vulnerability that allows attackers to execute arbitrary commands through an unauthenticated HTTP endpoint. Attackers can leverage the /op=command endpoint to download and execute payloads by sending crafted JSON requests with malicious script commands.	9.8	More Details
CVE-2025-68909	Unrestricted Upload of File with Dangerous Type vulnerability in blazethemes Blogistic blogistic allows Using Malicious Files.This issue affects Blogistic: from n/a through <= 1.0.5.	9.8	More Details
CVE-2025-68910	Unrestricted Upload of File with Dangerous Type vulnerability in blazethemes Blogzee blogzee allows Using Malicious Files.This issue affects Blogzee: from n/a through <= 1.0.5.	9.8	More Details
CVE-2025-69052	Missing Authorization vulnerability in FmeAddons Registration & Login with Mobile Phone Number for WooCommerce registration-login-with-mobile-phone-number allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Registration & Login with Mobile Phone Number for WooCommerce: from n/a through <= 1.3.1.	9.8	More Details
CVE-2025-69101	Authentication Bypass Using an Alternate Path or Channel vulnerability in AmentoTech Workreap Core workreap_core allows Authentication Abuse.This issue affects Workreap Core: from n/a through <= 3.4.0.	9.8	More Details

CVE-2025-69078	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Malta malta allows PHP Local File Inclusion.This issue affects Malta: from n/a through <= 1.3.3.	9.8	More Details
CVE-2021-47748	Hasura GraphQL 1.3.3 contains a remote code execution vulnerability that allows attackers to execute arbitrary shell commands through SQL query manipulation. Attackers can inject commands into the run_sql endpoint by crafting malicious GraphQL queries that execute system commands through PostgreSQL's COPY FROM PROGRAM functionality.	9.8	More Details
CVE-2025-69079	Deserialization of Untrusted Data vulnerability in ThemeREX Sound | Musical Instruments Online Store musicplace allows Object Injection.This issue affects Sound | Musical Instruments Online Store: from n/a through <= 1.6.9.	9.8	More Details
CVE-2026-22792	5ire is a cross-platform desktop artificial intelligence assistant and model context protocol client. Prior to version 0.15.3, an unsafe HTML rendering permits untrusted HTML (including on* event attributes) to execute in the renderer context. An attacker can inject an `<img onerror=...>` payload to run arbitrary JavaScript in the renderer, which can call exposed bridge APIs such as `window.bridge.mcpServersManager.createServer`. This enables unauthorized creation of MCP servers and lead to remote command execution. Version 0.15.3 fixes the issue.	9.6	More Details
CVE-2026-22793	5ire is a cross-platform desktop artificial intelligence assistant and model context protocol client. Prior to version 0.15.3, an unsafe option parsing vulnerability in the ECharts Markdown plugin allows any user able to submit ECharts code blocks to execute arbitrary JavaScript code in the renderer context. This can lead to Remote Code Execution (RCE) in environments where privileged APIs (such as Electron’s electron.mcp) are exposed, resulting in full compromise of the host system. Version 0.15.3 patches the issue.	9.6	More Details
CVE-2026-24042	Appsmith is a platform to build admin panels, internal tools, and dashboards. In versions 1.94 and below, publicly accessible apps allow unauthenticated users to execute unpublished (edit-mode) actions by sending viewMode=false (or omitting it) to POST /api/v1/actions/execute. This bypasses the expected publish boundary where public viewers should only execute published actions, not edit-mode versions. An attack can result in sensitive data exposure, execution of edit-mode queries and APIs, development data access, and the ability to trigger side effect behavior. This issue does not have a released fix at the time of publication.	9.4	More Details
CVE-2025-52024	A vulnerability exists in the Aptsys POS Platform Web Services module thru 2025-05-28, which exposes internal API testing tools to unauthenticated users. By accessing specific URLs, an attacker is presented with a directory-style index listing all available backend services and POS web services, each with an HTML form for submitting test input. These panels are intended for developer use, but are accessible in production environments with no authentication or session validation. This grants any external actor the ability to discover, test, and execute API endpoints that perform critical functions including but not limited to user transaction retrieval, credit adjustments, POS actions, and internal data queries.	9.4	More Details
CVE-2025-52025	An SQL Injection vulnerability exists in the GetServiceByRestaurantID endpoint of the Aptsys gemscms POS Platform backend thru 2025-05-28. The vulnerability arises because user input is directly inserted into a dynamic SQL query syntax without proper sanitization or parameterization. This allows an attacker to inject and execute arbitrary SQL code by submitting crafted input in the id parameter, leading to unauthorized data access or modification.	9.4	More Details
CVE-2025-4319	Improper Restriction of Excessive Authentication Attempts, Weak Password Recovery Mechanism for Forgotten Password vulnerability in Birebirsoft Software and Technology Solutions Sufirmam allows Brute Force, Password Recovery Exploitation.This issue affects Sufirmam: through 23012026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.4	More Details
	This vulnerability occurs when a WebSocket endpoint does not enforce proper		

CVE-2025-54816	authentication mechanisms, allowing unauthorized users to establish connections. As a result, attackers can exploit this weakness to gain unauthorized access to sensitive data or perform unauthorized actions. Given that no authentication is required, this can lead to privilege escalation and potentially compromise the security of the entire system.	9.4	More Details
CVE-2025-68857	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ichurakov Paid Downloads paid-downloads allows Blind SQL Injection.This issue affects Paid Downloads: from n/a through <= 3.15.	9.3	More Details
CVE-2026-24399	ChatterMate is a no-code AI chatbot agent framework. In versions 1.0.8 and below, the chatbot accepts and executes malicious HTML/JavaScript payloads when supplied as chat input. Specifically, an <iframe> payload containing a javascript: URI can be processed and executed in the browser context. This allows access to sensitive client-side data such as localStorage tokens and cookies, resulting in client-side injection. This issue has been fixed in version 1.0.9.	9.3	More Details
CVE-2026-21264	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Account allows an unauthorized attacker to perform spoofing over a network.	9.3	More Details
CVE-2026-24307	Improper validation of specified type of input in M365 Copilot allows an unauthorized attacker to disclose information over a network.	9.3	More Details
CVE-2026-24305	Azure Entra ID Elevation of Privilege Vulnerability	9.3	More Details
CVE-2025-68670	xrdp is an open source RDP server. xrdp before v0.10.5 contains an unauthenticated stack-based buffer overflow vulnerability. The issue stems from improper bounds checking when processing user domain information during the connection sequence. If exploited, the vulnerability could allow remote attackers to execute arbitrary code on the target system. The vulnerability allows an attacker to overwrite the stack buffer and the return address, which could theoretically be used to redirect the execution flow. The impact of this vulnerability is lessened if a compiler flag has been used to build the xrdp executable with stack canary protection. If this is the case, a second vulnerability would need to be used to leak the stack canary value. Upgrade to version 0.10.5 to receive a patch. Additionally, do not rely on stack canary protection on production systems.	9.1	More Details
CVE-2026-24736	Squidex is an open source headless content management system and content management hub. Versions of the application up to and including 7.21.0 allow users to define "Webhooks" as actions within the Rules engine. The url parameter in the webhook configuration does not appear to validate or restrict destination IP addresses. It accepts local addresses such as 127.0.0.1 or localhost. When a rule is triggered (Either manual trigger by manually calling the trigger endpoint or by a content update or any other triggers), the backend server executes an HTTP request to the user-supplied URL. Crucially, the server logs the full HTTP response in the rule execution log (lastDump field), which is accessible via the API. Which turns a "Blind" SSRF into a "Full Read" SSRF. As of time of publication, no patched versions are available.	9.1	More Details
CVE-2026-24874	Access of Resource Using Incompatible Type ('Type Confusion') vulnerability in themrdemonized xray-monolith.This issue affects xray-monolith: before 2025.12.30.	9.1	More Details
CVE-2026-22482	Server-Side Request Forgery (SSRF) vulnerability in wbolt.com IMGspider imgspider allows Server Side Request Forgery.This issue affects IMGspider: from n/a through <= 2.3.12.	9.1	More Details
CVE-2026-23966	sm-crypto provides JavaScript implementations of the Chinese cryptographic algorithms SM2, SM3, and SM4. A private key recovery vulnerability exists in the SM2 decryption logic of sm-crypto prior to version 0.3.14. By interacting with the SM2 decryption interface multiple times, an attacker can fully recover the private key within approximately several hundred interactions. Version 0.3.14 patches the issue.	9.1	More Details

CVE-2025-69312	Unrestricted Upload of File with Dangerous Type vulnerability in Xpro Xpro Elementor Addons xpro-elementor-addons allows Upload a Web Shell to a Web Server.This issue affects Xpro Elementor Addons: from n/a through <= 1.4.19.1.	9.1	More Details
CVE-2025-70985	Incorrect access control in the update function of RuoYi v4.8.2 allows unauthorized attackers to arbitrarily modify data outside of their scope.	9.1	More Details
CVE-2025-62741	Server-Side Request Forgery (SSRF) vulnerability in SmartDataSoft Pool Services pool-services allows Server Side Request Forgery.This issue affects Pool Services: from n/a through <= 3.3.	9.1	More Details
CVE-2025-62754	Missing Authorization vulnerability in Kapil Paul Payment Gateway bKash for WC woo-payment-bkash allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Payment Gateway bKash for WC: from n/a through <= 3.1.0.	9.1	More Details
CVE-2025-66719	An issue was discovered in Free5gc NRF 1.4.0. In the access-token generation logic of free5GC, the AccessTokenScopeCheck() function in file internal/sbi/processor/access_token.go bypasses all scope validation when the attacker uses a crafted targetNF value. This allows attackers to obtain an access token with any arbitrary scope.	9.1	More Details
CVE-2025-64252	Server-Side Request Forgery (SSRF) vulnerability in Marco Milesi ANAC XML Viewer anac-xml-viewer allows Server Side Request Forgery.This issue affects ANAC XML Viewer: from n/a through <= 1.8.2.	9.1	More Details
CVE-2026-20912	Gitea does not properly validate repository ownership when linking attachments to releases. An attachment uploaded to a private repository could potentially be linked to a release in a different public repository, making it accessible to unauthorized users.	9.1	More Details
CVE-2026-20750	Gitea does not properly validate project ownership in organization project operations. A user with project write access in one organization may be able to modify projects belonging to a different organization.	9.1	More Details
CVE-2026-24379	Authorization Bypass Through User-Controlled Key vulnerability in wpjobportal WP Job Portal wp-job-portal allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Job Portal: from n/a through <= 2.4.3.	9.1	More Details
CVE-2026-20897	Gitea does not properly validate repository ownership when deleting Git LFS locks. A user with write access to one repository may be able to delete LFS locks belonging to other repositories.	9.1	More Details
CVE-2026-24002	Grist is spreadsheet software using Python as its formula language. Grist offers several methods for running those formulas in a sandbox, for cases where the user may be working with untrusted spreadsheets. One such method runs them in pyodide, but pyodide on node does not have a useful sandbox barrier. If a user of Grist sets \`GRIST_SANDBOX_FLAVOR\` to \`pyodide\` and opens a malicious document, that document could run arbitrary processes on the server hosting Grist. The problem has been addressed in Grist version 1.7.9 and up, by running pyodide under deno. As a workaround, a user can use the gvisor-based sandbox by setting \`GRIST_SANDBOX_FLAVOR\` to \`gvisor\`.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-24406	iccDEV provides libraries and tools for interacting with, manipulating, and applying ICC color management profiles. Versions 2.3.1.1 and below have a Heap Buffer Overflow vulnerability in CIccTagNamedColor2::SetSize(). This occurs when user-controllable input is unsafely incorporated into ICC profile data or other structured binary blobs. Successful	8.8	More Details

	exploitation may allow an attacker to perform DoS, manipulate data, bypass application logic and Code Execution. This issue has been fixed in version 2.3.1.2.		
CVE-2021-47770	OpenPLC v3 contains an authenticated remote code execution vulnerability that allows attackers with valid credentials to inject malicious code through the hardware configuration interface. Attackers can upload a custom hardware layer with embedded reverse shell code that establishes a network connection to a specified IP and port, enabling remote command execution.	8.8	More Details
CVE-2026-24530	Missing Authorization vulnerability in sheepfish WebP Conversion webp-conversion allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WebP Conversion: from n/a through <= 2.1.	8.8	More Details
CVE-2026-24529	Missing Authorization vulnerability in Alejandro Quick Restaurant Reservations quick-restaurant-reservations allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Quick Restaurant Reservations: from n/a through <= 1.6.7.	8.8	More Details
CVE-2025-14866	The Melapress Role Editor plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.1.1. This is due to a misconfigured capability check on the 'save_secondary_roles_field' function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to assign themselves additional roles including Administrator.	8.8	More Details
CVE-2026-22273	Dell ECS, versions 3.8.1.0 through 3.8.1.7, and Dell ObjectScale versions prior to 4.2.0.0, contains an Use of Default Credentials vulnerability in the OS. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	8.8	More Details
CVE-2025-69182	Incorrect Privilege Assignment vulnerability in e-plugins Institutions Directory institutions-directory allows Privilege Escalation.This issue affects Institutions Directory: from n/a through <= 1.3.4.	8.8	More Details
CVE-2025-67847	A flaw was found in Moodle. An attacker with access to the restore interface could trigger server-side execution of arbitrary code. This is due to insufficient validation of restore input, which leads to unintended interpretation by core restore routines. Successful exploitation could result in a full compromise of the Moodle application.	8.8	More Details
CVE-2021-47852	Rockstar Games Launcher 1.0.37.349 contains a privilege escalation vulnerability that allows authenticated users to modify the service executable with weak permissions. Attackers can replace the RockstarService.exe with a malicious binary to create a new administrator user and gain elevated system access.	8.8	More Details
CVE-2021-47853	phpPgAdmin 7.13.0 contains a remote command execution vulnerability that allows authenticated attackers to execute arbitrary system commands through SQL query manipulation. Attackers can create a custom table, upload a malicious .txt file, and use the COPY FROM PROGRAM command to execute operating system commands with the application's privileges.	8.8	More Details
CVE-2025-69180	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in themepassion Ultra Portfolio ultra-portfolio allows Blind SQL Injection.This issue affects Ultra Portfolio: from n/a through <= 6.7.	8.8	More Details
CVE-2026-1420	A flaw has been found in Tenda AC23 16.03.07.52. This impacts an unknown function of the file /goform/WifiExtraSet. This manipulation of the argument wpapsk_crypto causes buffer overflow. Remote exploitation of the attack is possible. The exploit has been published and may be used.	8.8	More Details
CVE-2026-1427	Single Sign-On Portal System developed by WellChoose has a OS Command Injection vulnerability, allowing authenticated remote attackers to inject arbitrary OS commands and execute them on the server.	8.8	More Details
CVE-2026-1428	Single Sign-On Portal System developed by WellChoose has a OS Command Injection vulnerability, allowing authenticated remote attackers to inject arbitrary OS commands and execute them on the server.	8.8	More Details

CVE-2025-59106	The binary serving the web server and executing basically all actions launched from the Web UI is running with root privileges. This is against the least privilege principle. If an attacker is able to execute code on the system via other vulnerabilities it is possible to directly execute commands with highest privileges.	8.8	More Details
CVE-2025-68899	Deserialization of Untrusted Data vulnerability in designthemes Vivagh vivagh allows Object Injection.This issue affects Vivagh: from n/a through <= 2.4.	8.8	More Details
CVE-2025-68903	Deserialization of Untrusted Data vulnerability in AivahThemes Anona anona allows Object Injection.This issue affects Anona: from n/a through <= 8.0.	8.8	More Details
CVE-2021-47871	Hestia Control Panel 1.3.2 contains an arbitrary file write vulnerability that allows authenticated attackers to write files to arbitrary locations using the API index.php endpoint. Attackers can exploit the v-make-tmp-file command to write SSH keys or other content to specific file paths on the server.	8.8	More Details
CVE-2025-66428	An issue with WordPress directory names in WebPros WordPress Toolkit before 6.9.1 allows privilege escalation.	8.8	More Details
CVE-2026-24380	Missing Authorization vulnerability in Metagauss EventPrime eventprime-event-calendar-management allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects EventPrime: from n/a through <= 4.2.8.0.	8.8	More Details
CVE-2025-54002	Missing Authorization vulnerability in Jthemes xSmart xsmart allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects xSmart: from n/a through <= 1.2.9.4.	8.8	More Details
CVE-2026-24368	Missing Authorization vulnerability in Theme-one The Grid the-grid allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Grid: from n/a through < 2.8.0.	8.8	More Details
CVE-2026-24367	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in shinetheme Traveler traveler allows Blind SQL Injection.This issue affects Traveler: from n/a through < 3.2.8.	8.8	More Details
CVE-2026-24358	Missing Authorization vulnerability in ExpressTech Systems Quiz And Survey Master quiz-master-next allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Quiz And Survey Master: from n/a through <= 10.3.3.	8.8	More Details
CVE-2026-22472	Missing Authorization vulnerability in hassantafreshi Easy Form Builder easy-form-builder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Easy Form Builder: from n/a through <= 3.9.6.	8.8	More Details
CVE-2025-41726	A low privileged remote attacker can execute arbitrary code by sending specially crafted calls to the web service of the Device Manager or locally via an API and can cause integer overflows which then may lead to arbitrary code execution within privileged processes.	8.8	More Details
CVE-2026-22481	Missing Authorization vulnerability in Rasedul Haque Rumi BD Courier Order Ratio Checker bd-courier-order-ratio-checker allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects BD Courier Order Ratio Checker: from n/a through <= 2.0.1.	8.8	More Details
CVE-2020-36938	WinAVR version 20100110 contains an insecure permissions vulnerability that allows authenticated users to modify system files and executables. Attackers can leverage the overly permissive access controls to potentially modify critical DLLs and executable files in the WinAVR installation directory.	8.8	More Details
CVE-2020-36942	Victor CMS 1.0 contains a file upload vulnerability that allows authenticated users to upload malicious PHP files through the profile image upload feature. Attackers can upload a PHP shell to the /img directory and execute system commands by accessing the uploaded file via web browser.	8.8	More Details

CVE-2026-24356	Missing Authorization vulnerability in Roxnor GetGenie getgenie allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects GetGenie: from n/a through <= 4.3.0.	8.8	More Details
CVE-2026-23974	Missing Authorization vulnerability in uxper Golo golo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Golo: from n/a through < 1.7.5.	8.8	More Details
CVE-2025-69183	Incorrect Privilege Assignment vulnerability in e-plugins Hospital Doctor Directory hospital-doctor-directory allows Privilege Escalation.This issue affects Hospital Doctor Directory: from n/a through <= 1.3.9.	8.8	More Details
CVE-2026-22807	vLLM is an inference and serving engine for large language models (LLMs). Starting in version 0.10.1 and prior to version 0.14.0, vLLM loads Hugging Face `auto_map` dynamic modules during model resolution without gating on `trust_remote_code`, allowing attacker-controlled Python code in a model repo/path to execute at server startup. An attacker who can influence the model repo/path (local directory or remote Hugging Face repo) can achieve arbitrary code execution on the vLLM host during model load. This happens before any request handling and does not require API access. Version 0.14.0 fixes the issue.	8.8	More Details
CVE-2026-24532	Missing Authorization vulnerability in SiteLock SiteLock Security sitelock allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SiteLock Security: from n/a through <= 5.0.2.	8.8	More Details
CVE-2026-24778	Ghost is an open source content management system. In Ghost versions 5.43.0 through 5.12.04 and 6.0.0 through 6.14.0, an attacker was able to craft a malicious link that, when accessed by an authenticated staff user or member, would execute JavaScript with the victim's permissions, potentially leading to account takeover. Ghost Portal versions 2.29.1 through 2.51.4 and 2.52.0 through 2.57.0 were vulnerable to this issue. Ghost automatically loads the latest patch of the members Portal component via CDN. For Ghost 5.x users, upgrading to v5.121.0 or later fixes the vulnerability. v5.121.0 loads Portal v2.51.5, which contains the patch. For Ghost 6.x users, upgrading to v6.15.0 or later fixes the vulnerability. v6.15.0 loads Portal v2.57.1, which contains the patch. For Ghost installations using a customized or self-hosted version of Portal, it will be necessary to manually rebuild from or update to the latest patch version.	8.8	More Details
CVE-2025-66135	Missing Authorization vulnerability in merkulove Imager for Elementor imager-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Imager for Elementor: from n/a through <= 2.0.4.	8.8	More Details
CVE-2025-66136	Missing Authorization vulnerability in merkulove Carter for Elementor carter-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Carter for Elementor: from n/a through <= 1.0.2.	8.8	More Details
CVE-2025-49375	Missing Authorization vulnerability in cozythemes HomeLancer homelancer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects HomeLancer: from n/a through <= 1.0.1.	8.8	More Details
CVE-2025-49050	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in kamleshyadav WP Lead Capturing Pages wp-lead-capture allows Blind SQL Injection.This issue affects WP Lead Capturing Pages: from n/a through <= 2.5.	8.8	More Details
CVE-2026-24747	PyTorch is a Python package that provides tensor computation. Prior to version 2.10.0, a vulnerability in PyTorch's `weights_only` unpickler allows an attacker to craft a malicious checkpoint file (`.pth`) that, when loaded with `torch.load(..., weights_only=True)`, can corrupt memory and potentially lead to arbitrary code execution. Version 2.10.0 fixes the issue.	8.8	More Details
CVE-2025-63018	Missing Authorization vulnerability in wproyal Bard bard allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Bard: from n/a through <= 2.229.	8.8	More Details
CVE-	Missing Authorization vulnerability in uPress Booter booter-bots-crawlers-manager allows		

2026-24534	Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Booter: from n/a through <= 1.5.7.	8.8	More Details
CVE-2025-49049	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ZoomIt DZS Video Gallery dzs-videogallery allows SQL Injection.This issue affects DZS Video Gallery: from n/a through <= 12.37.	8.8	More Details
CVE-2025-66137	Missing Authorization vulnerability in merkulove Searcher for Elementor searcher-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Searcher for Elementor: from n/a through <= 1.0.3.	8.8	More Details
CVE-2025-66138	Missing Authorization vulnerability in merkulove Motionger for Elementor motionger-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Motionger for Elementor: from n/a through <= 2.0.4.	8.8	More Details
CVE-2026-24405	iccDEV provides libraries and tools for interacting with, manipulating, and applying ICC color management profiles. Versions 2.3.1.1 and below have a Heap Buffer Overflow vulnerability in CIccMpeCalculator::Read(). This occurs when user-controllable input is unsafely incorporated into ICC profile data or other structured binary blobs. Successful exploitation may allow an attacker to perform DoS, manipulate data, bypass application logic and Code Execution. This issue has been fixed in version 2.3.1.2.	8.8	More Details
CVE-2021-47904	PhreeBooks 5.2.3 contains an authenticated file upload vulnerability in the Image Manager that allows remote code execution. Attackers can upload a malicious PHP web shell by exploiting unrestricted file type uploads to gain command execution on the server.	8.8	More Details
CVE-2025-31413	Cross-Site Request Forgery (CSRF) vulnerability in bdthemes Element Pack Elementor Addons bdthemes-element-pack-lite allows Cross Site Request Forgery.This issue affects Element Pack Elementor Addons: from n/a through <= 8.3.13.	8.8	More Details
CVE-2025-69293	Incorrect Privilege Assignment vulnerability in e-plugins Final User final-user allows Privilege Escalation.This issue affects Final User: from n/a through <= 1.2.5.	8.8	More Details
CVE-2026-1328	A vulnerability was detected in Totolink NR1800X 9.1.0u.6279_B20210910. Impacted is the function setWizardCfg of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. Performing a manipulation of the argument ssid results in buffer overflow. The attack may be initiated remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-1324	A vulnerability was identified in Sangfor Operation and Maintenance Management System up to 3.0.12. Affected by this issue is the function SessionController of the file /isomp-protocol/protocol/session of the component SSH Protocol Handler. The manipulation of the argument keypassword leads to os command injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-69292	Incorrect Privilege Assignment vulnerability in e-plugins WP Membership wp-membership allows Privilege Escalation.This issue affects WP Membership: from n/a through <= 1.6.4.	8.8	More Details
CVE-2025-50007	Incorrect Privilege Assignment vulnerability in Jthemes xSmart xsmart allows Privilege Escalation.This issue affects xSmart: from n/a through <= 1.2.9.4.	8.8	More Details
CVE-2026-24412	iccDEV provides libraries and tools for interacting with, manipulating, and applying ICC color management profiles. Versions 2.3.1.1 and below have aHeap Buffer Overflow vulnerability in the CIccTagXmlSegmentedCurve::ToXml() function. This occurs when user-controllable input is unsafely incorporated into ICC profile data or other structured binary blobs. Successful exploitation may allow an attacker to perform DoS, manipulate data, bypass application logic and Code Execution. This issue has been fixed in version 2.3.1.2.	8.8	More Details
CVE-2025-	Dell Unisphere for PowerMax, version(s) 10.2.0.x, contain(s) an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged	8.8	More

36588	attacker with remote access could potentially exploit this vulnerability, leading to Command execution.		Details
CVE-2026-24572	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Nelio Software Nelio Content nelio-content allows Blind SQL Injection.This issue affects Nelio Content: from n/a through <= 4.1.0.	8.8	More Details
CVE-2026-1329	A flaw has been found in Tenda AX1803 1.0.0.1. The affected element is the function fromGetWifiGuestBasic of the file /goform/WifiGuestSet. Executing a manipulation of the argument guestWrlPwd/guestEn/guestSsid/hideSsid/guestSecurity can lead to stack-based buffer overflow. The attack may be launched remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2021-47903	LiteSpeed Web Server Enterprise 5.4.11 contains an authenticated command injection vulnerability in the external app configuration interface. Authenticated administrators can inject shell commands through the 'Command' parameter in the server configuration, allowing remote code execution via path traversal and bash command injection.	8.8	More Details
CVE-2021-47888	Textpattern versions prior to 4.8.3 contain an authenticated remote code execution vulnerability that allows logged-in users to upload malicious PHP files. Attackers can upload a PHP file with a shell command execution payload and execute arbitrary commands by accessing the uploaded file through a specific URL parameter.	8.8	More Details
CVE-2025-62106	Missing Authorization vulnerability in Mario Peshev WP-CRM System wp-crm-system allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP-CRM System: from n/a through <= 3.4.5.	8.8	More Details
CVE-2025-5805	Missing Authorization vulnerability in Ninetheme Electron electron allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Electron: from n/a through <= 1.8.2.	8.8	More Details
CVE-2026-23954	Incus is a system container and virtual machine manager. Versions 6.21.0 and below allow a user with the ability to launch a container with a custom image (e.g a member of the ‘incus’ group) to use directory traversal or symbolic links in the templating functionality to achieve host arbitrary file read, and host arbitrary file write. This ultimately results in arbitrary command execution on the host. When using an image with a metadata.yaml containing templates, both the source and target paths are not checked for symbolic links or directory traversal. This can also be exploited in IncusOS. A fix is planned for versions 6.0.6 and 6.21.0, but they have not been released at the time of publication.	8.7	More Details
CVE-2026-23953	Incus is a system container and virtual machine manager. In versions 6.20.0 and below, a user with the ability to launch a container with a custom YAML configuration (e.g a member of the ‘incus’ group) can create an environment variable containing newlines, which can be used to add additional configuration items in the container’s lxc.conf due to newline injection. This can allow adding arbitrary lifecycle hooks, ultimately resulting in arbitrary command execution on the host. Exploiting this issue on IncusOS requires a slight modification of the payload to change to a different writable directory for the validation step (e.g /tmp). This can be confirmed with a second container with /tmp mounted from the host (A privileged action for validation only). A fix is planned for versions 6.0.6 and 6.21.0, but they have not been released at the time of publication.	8.7	More Details
CVE-2025-27378	AES contains a SQL injection vulnerability due to an inactive configuration that prevents the latest SQL parsing logic from being applied. When this configuration is not enabled, crafted input may be improperly handled, allowing attackers to inject and execute arbitrary SQL queries.	8.6	More Details
CVE-2025-69045	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in FooEvents FooEvents for WooCommerce fooevents allows SQL Injection.This issue affects FooEvents for WooCommerce: from n/a through <= 1.20.4.	8.6	More Details
CVE-2026-	Python-Multipart is a streaming multipart parser for Python. Prior to version 0.0.22, a Path Traversal vulnerability exists when using non-default configuration options `UPLOAD_DIR` and `UPLOAD_KEEP_FILENAME=True`. An attacker can write uploaded files to arbitrary locations on the filesystem by crafting a malicious filename. Users should upgrade to	8.6	More Details

24486	version 0.0.22 to receive a patch or, as a workaround, avoid using `UPLOAD_KEEP_FILENAME=True` in project configurations.		
CVE-2025-69097	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in VibeThemes WPLMS wplms_plugin allows Path Traversal.This issue affects WPLMS: from n/a through <= 1.9.9.5.4.	8.6	More Details
CVE-2025-68901	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in AivahThemes Anona anona allows Path Traversal.This issue affects Anona: from n/a through <= 8.0.	8.6	More Details
CVE-2025-69099	Deserialization of Untrusted Data vulnerability in fuelthemes North north-wp allows Object Injection.This issue affects North: from n/a through <= 5.7.5.	8.6	More Details
CVE-2025-50004	Deserialization of Untrusted Data vulnerability in artbees JupiterX Core jupiterx-core allows Object Injection.This issue affects JupiterX Core: from n/a through <= 4.10.1.	8.5	More Details
CVE-2025-14459	A flaw was found in KubeVirt Containerized Data Importer (CDI). This vulnerability allows a user to clone PersistentVolumeClaims (PVCs) from unauthorized namespaces, resulting in unauthorized access to data via the DataImportCron PVC source mechanism.	8.5	More Details
CVE-2025-68881	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Saad Iqbal AppExperts appexperts allows SQL Injection.This issue affects AppExperts: from n/a through <= 1.4.5.	8.5	More Details
CVE-2026-24882	In GnuPG before 2.5.17, a stack-based buffer overflow exists in tpm2daemon during handling of the PKDECRYPT command for TPM-backed RSA and ECC keys.	8.4	More Details
CVE-2026-0710	A flaw was found in SIPp. A remote attacker could exploit this by sending specially crafted Session Initiation Protocol (SIP) messages during an active call. This vulnerability, a NULL pointer dereference, can cause the application to crash, leading to a denial of service. Under specific conditions, it may also allow an attacker to execute unauthorized code, compromising the system's integrity and availability.	8.4	More Details
CVE-2021-47881	dataSIMS Avionics ARINC 664-1 version 4.5.3 contains a local buffer overflow vulnerability that allows attackers to overwrite memory by manipulating the milstd1553result.txt file. Attackers can craft a malicious file with carefully constructed payload and alignment sections to potentially execute arbitrary code on the Windows system.	8.4	More Details
CVE-2026-0603	A flaw was found in Hibernate. A remote attacker with low privileges could exploit a second-order SQL injection vulnerability by providing specially crafted, unsanitized non-alphanumeric characters in the ID column when the InlineIdsOrClauseBuilder is used. This could lead to sensitive information disclosure, such as reading system files, and allow for data manipulation or deletion within the application's database, resulting in an application level denial of service.	8.3	More Details
CVE-2025-68137	EVerest is an EV charging software stack. Prior to version 2025.10.0, an integer overflow occurring in `SdpPacket::parse_header()` allows the current buffer length to be set to 7 after a complete header of size 8 has been read. The remaining length to read is computed using the current length subtracted by the header length which results in a negative value. This value is then interpreted as `SIZE_MAX` (or slightly less) because the expected type of the argument is `size_t`. Depending on whether the server is plain TCP or TLS, this leads to either an infinite loop or a stack buffer overflow. Version 2025.10.0 fixes the issue.	8.3	More Details
CVE-2025-69050	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Edge-Themes Overworld overworld allows PHP Local File Inclusion.This issue affects Overworld: from n/a through <= 1.3.	8.2	More Details
CVE-2025-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in goalthemes Dekoro dekoro allows PHP Local File	8.2	More Details

69041	Inclusion.This issue affects Dekoro: from n/a through <= 1.0.7.		
CVE-2020-36951	Phpscript-sgh 0.1.0 contains a time-based blind SQL injection vulnerability in the admin interface that allows attackers to manipulate database queries through the 'id' parameter. Attackers can exploit this vulnerability by crafting malicious payloads that trigger time delays, enabling them to extract sensitive database information through conditional sleep techniques.	8.2	More Details
CVE-2021-47902	Testa Online Test Management System 3.4.7 contains a SQL injection vulnerability that allows attackers to manipulate database queries through the 'q' search parameter. Attackers can inject malicious SQL code in the search field to extract database information, potentially accessing sensitive user or system data.	8.2	More Details
CVE-2026-21227	Improper limitation of a pathname to a restricted directory ('path traversal') in Azure Logic Apps allows an unauthorized attacker to elevate privileges over a network.	8.2	More Details
CVE-2025-69042	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in goalthemes Lindo lindo allows PHP Local File Inclusion.This issue affects Lindo: from n/a through <= 1.2.5.	8.2	More Details
CVE-2025-69049	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Töbel tobel allows PHP Local File Inclusion.This issue affects Töbel: from n/a through <= 1.6.	8.2	More Details
CVE-2025-69043	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in goalthemes Rashy rashy allows PHP Local File Inclusion.This issue affects Rashy: from n/a through <= 1.1.3.	8.2	More Details
CVE-2025-69065	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Snow Mountain snowmountain allows PHP Local File Inclusion.This issue affects Snow Mountain: from n/a through <= 1.4.3.	8.2	More Details
CVE-2025-69064	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Pets Land petsland allows PHP Local File Inclusion.This issue affects Pets Land: from n/a through <= 1.2.8.	8.2	More Details
CVE-2025-69062	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Weedles weedles allows PHP Local File Inclusion.This issue affects Weedles: from n/a through <= 1.1.12.	8.2	More Details
CVE-2025-69061	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes MoveMe moveme allows PHP Local File Inclusion.This issue affects MoveMe: from n/a through <= 1.2.15.	8.2	More Details
CVE-2025-69046	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in WebGeniusLab iRecco Core irecco-core allows PHP Local File Inclusion.This issue affects iRecco Core: from n/a through <= 1.3.6.	8.2	More Details
CVE-2025-69040	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in goalthemes Bfres bfres allows PHP Local File Inclusion.This issue affects Bfres: from n/a through <= 1.2.1.	8.2	More Details
CVE-2025-69047	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in magentech MaxShop sw_maxshop allows PHP Local File Inclusion.This issue affects MaxShop: from n/a through <= 3.6.20.	8.2	More Details
CVE-2026-	A vulnerability in Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P), Cisco Unity Connection, and Cisco Webex Calling Dedicated Instance could allow an unauthenticated, remote attacker&nbsp;to execute arbitrary commands on the underlying operating system of an affected device.&nbsp; This vulnerability is due to improper validation of user-supplied input in HTTP requests. An attacker could exploit this vulnerability by sending a	8.2	More Details

20045	sequence of crafted HTTP requests to the web-based management interface of an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root. Note: Cisco has assigned this security advisory a Security Impact Rating (SIR) of Critical rather than High as the score indicates. The reason is that exploitation of this vulnerability could result in an attacker elevating privileges to root.		
CVE-2025-69100	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in fuelthemes North north-wp allows PHP Local File Inclusion.This issue affects North: from n/a through <= 5.7.5.	8.2	More Details
CVE-2021-47848	Blitar Tourism 1.0 contains an authentication bypass vulnerability that allows attackers to bypass login by injecting SQL code through the username parameter. Attackers can manipulate the login request by sending a crafted username with SQL injection techniques to gain unauthorized administrative access.	8.2	More Details
CVE-2021-47846	Digital Crime Report Management System 1.0 contains a critical SQL injection vulnerability affecting multiple login pages that allows unauthenticated attackers to bypass authentication. Attackers can exploit the vulnerability by sending crafted SQL injection payloads in email and password parameters across police, incharge, user, and HQ login endpoints.	8.2	More Details
CVE-2026-22022	Deployments of Apache Solr 5.3.0 through 9.10.0 that rely on Solr's "Rule Based Authorization Plugin" are vulnerable to allowing unauthorized access to certain Solr APIs, due to insufficiently strict input validation in those components. Only deployments that meet all of the following criteria are impacted by this vulnerability: * Use of Solr's "RuleBasedAuthorizationPlugin" * A RuleBasedAuthorizationPlugin config (see security.json) that specifies multiple "roles" * A RuleBasedAuthorizationPlugin permission list (see security.json) that uses one or more of the following pre-defined permission rules: "config-read", "config-edit", "schema-read", "metrics-read", or "security-read". * A RuleBasedAuthorizationPlugin permission list that doesn't define the "all" pre-defined permission * A networking setup that allows clients to make unfiltered network requests to Solr. (i.e. user-submitted HTTP/HTTPS requests reach Solr as-is, unmodified or restricted by any intervening proxy or gateway) Users can mitigate this vulnerability by ensuring that their RuleBasedAuthorizationPlugin configuration specifies the "all" pre-defined permission and associates the permission with an "admin" or other privileged role. Users can also upgrade to a Solr version outside of the impacted range, such as the recently released Solr 9.10.1.	8.2	More Details
CVE-2025-69077	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Hobo hobo allows PHP Local File Inclusion.This issue affects Hobo: from n/a through <= 1.0.10.	8.2	More Details
CVE-2026-24524	Missing Authorization vulnerability in Essekia Tablesome tablesome allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tablesome: from n/a through <= 1.1.35.2.	8.1	More Details
CVE-2026-24470	Skipper is an HTTP router and reverse proxy for service composition. Prior to version 0.24.0, when running Skipper as an Ingress controller, users with permissions to create an Ingress and a Service of type ExternalName can create routes that enable them to use Skipper's network access to reach internal services. Version 0.24.0 disables Kubernetes ExternalName by default. As a workaround, developers can allow list targets of an ExternalName and allow list via regular expressions.	8.1	More Details
CVE-2025-68510	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeGoods Photography photography allows PHP Local File Inclusion.This issue affects Photography: from n/a through < 7.7.5.	8.1	More Details
CVE-2025-69039	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in goalthemes Bailly bailly allows PHP Local File Inclusion.This issue affects Bailly: from n/a through <= 1.3.4.	8.1	More Details
CVE-	Missing Authorization vulnerability in CloudPanel CLP Varnish Cache clp-varnish-cache		

2026-24525	allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects CLP Varnish Cache: from n/a through <= 1.0.2.	8.1	More Details
CVE-2025-10856	Unrestricted Upload of File with Dangerous Type vulnerability in Solvera Software Services Trade Inc. Teknoera allows File Content Injection.This issue affects Teknoera: through 01102025.	8.1	More Details
CVE-2026-24490	MobSF is a mobile application security testing tool used. Prior to version 4.4.5, a Stored Cross-site Scripting (XSS) vulnerability in MobSF's Android manifest analysis allows an attacker to execute arbitrary JavaScript in the context of a victim's browser session by uploading a malicious APK. The `android:host` attribute from `<data android:scheme="android_secret_code">` elements is rendered in HTML reports without sanitization, enabling session hijacking and account takeover. Version 4.4.5 fixes the issue.	8.1	More Details
CVE-2026-24038	Horilla is a free and open source Human Resource Management System (HRMS). In version 1.4.0, the OTP handling logic has a flawed equality check that can be bypassed. When an OTP expires, the server returns None, and if an attacker omits the otp field from their POST request, the user-supplied OTP is also None, causing the comparison user_otp == otp to pass. This allows an attacker to bypass two-factor authentication entirely without ever providing a valid OTP. If administrative accounts are targeted, it could lead to compromise of sensitive HR data, manipulation of employee records, and further system-wide abuse. This issue has been fixed in version 1.5.0.	8.1	More Details
CVE-2026-21721	The dashboard permissions API does not verify the target dashboard scope and only checks the dashboards.permissions:* action. As a result, a user who has permission management rights on one dashboard can read and modify permissions on other dashboards. This is an organization-internal privilege escalation.	8.1	More Details
CVE-2026-24357	Missing Authorization vulnerability in Brecht WP Recipe Maker wp-recipe-maker allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Recipe Maker: from n/a through <= 10.2.4.	8.1	More Details
CVE-2025-69076	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Modern Housewife modernhousewife allows PHP Local File Inclusion.This issue affects Modern Housewife: from n/a through <= 1.0.12.	8.1	More Details
CVE-2026-24881	In GnuPG before 2.5.17, a crafted CMS (S/MIME) EnvelopedData message carrying an oversized wrapped session key can cause a stack-based buffer overflow in gpg-agent during PKDECRYPT--kem=CMS handling. This can easily be leveraged for denial of service; however, there is also memory corruption that could lead to remote code execution.	8.1	More Details
CVE-2026-24741	ConvertXis a self-hosted online file converter. In versions prior to 0.17.0, the `POST /delete` endpoint uses a user-controlled `filename` value to construct a filesystem path and deletes it via `unlink` without sufficient validation. By supplying path traversal sequences (e.g., `../`), an attacker can delete arbitrary files outside the intended uploads directory, limited only by the permissions of the server process. Version 0.17.0 fixes the issue.	8.1	More Details
CVE-2025-68908	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in temash Barberry barberry allows PHP Local File Inclusion.This issue affects Barberry: from n/a through <= 2.9.9.87.	8.1	More Details
CVE-2026-24009	Docling Core (or docling-core) is a library that defines core data types and transformations in the document processing application Docling. A PyYAML-related Remote Code Execution (RCE) vulnerability, namely CVE-2020-14343, is exposed in docling-core starting in version 2.21.0 and prior to version 2.48.4, specifically only if the application uses pyyaml prior to version 5.4 and invokes `docling_core.types.doc.DoclingDocument.load_from_yaml()` passing it untrusted YAML data. The vulnerability has been patched in docling-core version 2.48.4. The fix mitigates the issue by switching `PyYAML` deserialization from `yaml.FullLoader` to `yaml.SafeLoader`, ensuring that untrusted data cannot trigger code execution. Users who cannot immediately upgrade docling-core can alternatively ensure that the installed version of PyYAML is 5.4 or greater.	8.1	More Details

CVE-2026-24869	Use-after-free in the Layout: Scrolling and Overflow component. This vulnerability affects Firefox < 147.0.2.	8.1	More Details
CVE-2025-47555	Authorization Bypass Through User-Controlled Key vulnerability in Themeum Tutor LMS tutor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tutor LMS: from n/a through <= 3.9.4.	8.1	More Details
CVE-2026-22278	Dell PowerScale OneFS versions prior to 9.13.0.0 contains an improper restriction of excessive authentication attempts vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	8.1	More Details
CVE-2026-24353	Missing Authorization vulnerability in wpeverest User Registration user-registration allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects User Registration: from n/a through <= 4.4.9.	8.1	More Details
CVE-2025-69314	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in fuelthemes Werkstatt werkstatt allows PHP Local File Inclusion.This issue affects Werkstatt: from n/a through < 4.8.3.	8.1	More Details
CVE-2026-24129	Runtipi is a Docker-based, personal homeserver orchestrator that facilitates multiple services on a single server. Versions 3.7.0 and above allow an authenticated user to execute arbitrary system commands on the host server by injecting shell metacharacters into backup filenames. The BackupManager fails to sanitize the filenames of uploaded backups. The system persists user-uploaded files directly to the host filesystem using the raw originalname provided in the request. This allows an attacker to stage a file containing shell metacharacters (e.g., $(id).tar.gz) at a predictable path, which is later referenced during the restore process. The successful storage of the file is what allows the subsequent restore command to reference and execute it. This issue has been fixed in version 4.7.0.	8.0	More Details
CVE-2025-4764	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Aida Computer Information Technology Inc. Hotel Guest Hotspot allows SQL Injection.This issue affects Hotel Guest Hotspot: through 22012026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.0	More Details
CVE-2025-3839	A flaw was found in Epiphany, a tool that allows websites to open external URL handler applications with minimal user interaction. This design can be misused to exploit vulnerabilities within those handlers, making them appear remotely exploitable. The browser fails to properly warn or gate this action, resulting in potential code execution on the client device via trusted UI behavior.	8.0	More Details
CVE-2020-36975	EPSON Status Monitor 3 version 8.0 contains an unquoted service path vulnerability that allows local attackers to potentially execute arbitrary code by exploiting the service binary path. Attackers can leverage the unquoted path in 'C:\Program Files\Common Files\EPSON\EPW!3SSRP\E_S60RPB.EXE' to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2021-47861	Event Log Explorer 4.9.3 contains an unquoted service path vulnerability that allows local users to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted service path by placing malicious executables in specific file system locations that will be executed with LocalSystem account privileges during service startup.	7.8	More Details
CVE-2020-36957	PDF Complete 3.5.310.2002 contains an unquoted service path vulnerability in its pdfsvc.exe service configuration. Attackers can exploit the unquoted path to inject and execute malicious code with elevated LocalSystem privileges.	7.8	More Details
CVE-2026-1284	An Out-Of-Bounds Write vulnerability affecting the EPRT file reading procedure in SOLIDWORKS eDrawings from Release SOLIDWORKS 2025 through Release SOLIDWORKS 2026 could allow an attacker to execute arbitrary code while opening a specially crafted EPRT file.	7.8	More Details
CVE-2021-	Hi-Rez Studios 5.1.6.3 contains an unquoted service path vulnerability in the HiPatchService 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	7.8	More Details

47862	malicious executables with LocalSystem permissions.		
CVE-2026-1283	A Heap-based Buffer Overflow vulnerability affecting the EPRT file reading procedure in SOLIDWORKS eDrawings from Release SOLIDWORKS 2025 through Release SOLIDWORKS 2026 could allow an attacker to execute arbitrary code while opening a specially crafted EPRT file.	7.8	More Details
CVE-2021-47863	MacPaw Encrypto 1.0.1 contains an unquoted service path vulnerability in its Encrypto Service configuration that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in C:\Program Files\Encrypto\ to inject malicious executables and escalate privileges on Windows systems.	7.8	More Details
CVE-2021-47864	OSAS Traverse Extension 11 contains an unquoted service path vulnerability in the TravExtensionHostSvc service running with LocalSystem privileges. Attackers can exploit the unquoted path to inject and execute malicious code by placing executable files in the service's path, potentially gaining elevated system access.	7.8	More Details
CVE-2021-47867	WIN-PACK PRO4.8 contains an unquoted service path vulnerability in the ScheduleService that allows local users to potentially execute code with elevated system privileges. Attackers can exploit the unquoted path in 'C:\Program Files <x86>\WINPAKPRO\ScheduleService Service.exe' to inject malicious code that would execute during service startup.	7.8	More Details
CVE-2021-47866	WIN-PACK PRO 4.8 contains an unquoted service path vulnerability in the GuardTourService that allows local users to potentially execute code with elevated system privileges. Attackers can exploit the unquoted path in C:\Program Files <x86>\WINPAKPRO\WP GuardTour Service.exe to inject malicious code that would execute during service startup.	7.8	More Details
CVE-2020-36937	Microvirt MEMU Play 3.7.0 contains an unquoted service path vulnerability in the MEmusvc Windows service 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 elevated LocalSystem privileges.	7.8	More Details
CVE-2020-36953	MiniTool ShadowMaker 3.2 contains an unquoted service path vulnerability in the MTAgentService that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in 'C:\Program Files\MiniTool ShadowMaker\AgentService.exe' to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2020-36952	IObit Uninstaller 10 Pro contains an unquoted service path vulnerability that allows local users to potentially execute code with elevated system privileges. Attackers can exploit the unquoted service path in the IObit Uninstaller Service to insert malicious code that would execute with SYSTEM-level permissions during service startup.	7.8	More Details
CVE-2026-20613	The ArchiveReader.extractContents() function used by cctl image load and container image load performs no pathname validation before extracting an archive member. This means that a carelessly or maliciously constructed archive can extract a file into any user-writable location on the system using relative pathnames. This issue is addressed in container 0.8.0 and containerization 0.21.0.	7.8	More Details
CVE-2026-0648	The vulnerability stems from an incorrect error-checking logic in the CreateCounter() function (in threadx/utility/rtos_compatibility_layers/OSEK/tx_osek.c) when handling the return value of osek_get_counter(). Specifically, the current code checks if cntr_id equals 0u to determine failure, but @osek_get_counter() actually returns E_OS_SYS_STACK (defined as 12U) when it fails. This mismatch causes the error branch to never execute even when the counter pool is exhausted. As a result, when the counter pool is depleted, the code proceeds to cast the error code (12U) to a pointer (OSEK_COUNTER *), creating a wild pointer. Subsequent writes to members of this pointer lead to writes to illegal memory addresses (e.g., 0x0000000C), which can trigger immediate HardFaults or silent memory corruption. This vulnerability poses significant risks, including potential denial-of-service attacks (via repeated calls to exhaust the counter pool) and unauthorized memory access.	7.8	More Details
	Magic Mouse 2 Utilities 2.20 contains an unquoted service path vulnerability in its Windows		

CVE-2020-36936	service configuration. Attackers can exploit the unquoted path to inject malicious executables and gain elevated system privileges by placing a malicious file in the service path.	7.8	More Details
CVE-2020-36982	Motorola Device Manager 2.5.4 contains an unquoted service path vulnerability in the MotoHelperService.exe service that allows local users to potentially inject malicious code. Attackers can exploit the unquoted path in the service configuration to execute arbitrary code with elevated system privileges during service startup.	7.8	More Details
CVE-2026-24765	PHPUnit is a testing framework for PHP. A vulnerability has been discovered in versions prior to 12.5.8, 11.5.50, 10.5.62, 9.6.33, and 8.5.52 involving unsafe deserialization of code coverage data in PHPT test execution. The vulnerability exists in the `cleanupForCoverage()` method, which deserializes code coverage files without validation, potentially allowing remote code execution if malicious `.coverage` files are present prior to the execution of the PHPT test. The vulnerability occurs when a `.coverage` file, which should not exist before test execution, is deserialized without the `allowed_classes` parameter restriction. An attacker with local file write access can place a malicious serialized object with a `__wakeup()` method into the file system, leading to arbitrary code execution during test runs with code coverage instrumentation enabled. This vulnerability requires local file write access to the location where PHPUnit stores or expects code coverage files for PHPT tests. This can occur through CI/CD pipeline attacks, the local development environment, and/or compromised dependencies. Rather than just silently sanitizing the input via `['allowed_classes' => false]`, the maintainer has chosen to make the anomalous state explicit by treating pre-existing `.coverage` files for PHPT tests as an error condition. Starting in versions in versions 12.5.8, 11.5.50, 10.5.62, 9.6.33, when a `.coverage` file is detected for a PHPT test prior to execution, PHPUnit will emit a clear error message identifying the anomalous state. Organizations can reduce the effective risk of this vulnerability through proper CI/CD configuration, including ephemeral runners, code review enforcement, branch protection, artifact isolation, and access control.	7.8	More Details
CVE-2025-67264	An OS command injection vulnerability in the com.sprd.engineermode component in Doogee Note59, Note59 Pro, and Note59 Pro+ allows a local attacker to execute arbitrary code and escalate privileges via the EngineerMode ADB shell, due to incomplete patching of CVE-2025-31710	7.8	More Details
CVE-2021-47898	Epson USB Display 1.6.0.0 contains an unquoted service path vulnerability in the EMP_UDSA service running with LocalSystem privileges. Attackers can exploit the unquoted path by placing malicious executables in intermediate directories to gain elevated system access.	7.8	More Details
CVE-2021-47896	PDF Complete Corporate Edition 4.1.45 contains an unquoted service path vulnerability in the pdfcDispatcher service that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in the service binary location to inject malicious executables that will be run with elevated LocalSystem privileges.	7.8	More Details
CVE-2020-36983	Quick 'n Easy FTP Service 3.2 contains an unquoted service path vulnerability that allows local attackers to execute arbitrary code during service startup. Attackers can exploit the misconfigured service binary path to inject malicious executables with elevated LocalSystem privileges during system boot or service restart.	7.8	More Details
CVE-2021-47890	LogonExpert 8.1 contains an unquoted service path vulnerability in the LogonExpertSvc service running with LocalSystem privileges. Attackers can exploit the unquoted path to place malicious executables in intermediate directories, potentially gaining elevated system access during service startup.	7.8	More Details
CVE-2021-47889	Softros LAN Messenger 9.6.4 contains an unquoted service path vulnerability in the SoftrosSpellChecker service that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in 'C:\Program Files (x86)\Softros Systems\Softros Messenger\Spell Checker\' to inject malicious executables and escalate privileges.	7.8	More Details
CVE-	Motorola Device Manager 2.4.5 contains an unquoted service path vulnerability in the PST		

2020-36981	Service that allows local users to potentially execute arbitrary code. Attackers can exploit the unquoted path in ForwardDaemon.exe to inject malicious code that will execute with elevated system privileges during service startup.	7.8	More Details
CVE-2020-36935	KMSpico 17.1.0.0 contains an unquoted service path vulnerability in the Service KMSELDI configuration that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted binary path in C:\Program Files\KMSpico\Service_KMS.exe to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2020-36980	SAntivirus IC 10.0.21.61 contains an unquoted service path vulnerability in its Windows service configuration that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted executable path to inject malicious files in the service binary path, enabling privilege escalation to system-level permissions.	7.8	More Details
CVE-2020-36979	Atheros Coex Service Application 8.0.0.255 contains an unquoted service path vulnerability in its Windows service configuration. Attackers can exploit the unquoted path by placing malicious executables in the service path to gain elevated system privileges during service startup.	7.8	More Details
CVE-2020-36977	Wondershare Driver Install Service contains an unquoted service path vulnerability in the ElevationService executable that allows local attackers to potentially inject malicious code. Attackers can exploit the unquoted path to replace the service binary with a malicious executable, enabling privilege escalation to LocalSystem account.	7.8	More Details
CVE-2020-36959	IDT PC Audio 1.0.6499.0 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 STacSV service to inject malicious code that would execute with LocalSystem account permissions during service startup.	7.8	More Details
CVE-2020-36976	Acer Global Registration Service 1.0.0.3 contains an unquoted service path vulnerability in its service configuration that allows local users to potentially execute arbitrary code. Attackers can exploit the unquoted path in C:\Program Files (x86)\Acer\Registration\ to inject malicious executables that would run with elevated LocalSystem privileges during service startup.	7.8	More Details
CVE-2020-36933	HTC IPTInstaller 4.0.9 contains an unquoted service path vulnerability in the PassThru Service configuration. Attackers can exploit the unquoted binary path to inject and execute malicious code with elevated LocalSystem privileges.	7.8	More Details
CVE-2020-36934	Deep Instinct Windows Agent 1.2.24.0 contains an unquoted service path vulnerability in the DeepNetworkService that allows local users to potentially execute code with elevated privileges. Attackers can exploit the unquoted path in C:\Program Files\HP Sure Sense\DeepNetworkService.exe to inject malicious code that would execute with LocalSystem permissions during service startup.	7.8	More Details
CVE-2020-36958	Kite 1.2020.1119.0 contains an unquoted service path vulnerability in the KiteService Windows service that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in 'C:\Program Files\Kite\KiteService.exe' to inject malicious executables and escalate privileges on the system.	7.8	More Details
CVE-2021-47859	ActivIdentity 8.2 contains an unquoted service path vulnerability in the ac.sharedstore service that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted binary path in C:\Program Files\Common Files\ActivIdentity\ to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2021-47882	FreeLAN 2.2 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-2021-47884	OKI Configuration Tool 1.6.53 contains an unquoted service path vulnerability in the OKI Local Port Manager service that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in 'C:\Program Files\Okidata\Common\extend3\portmgrsrv.exe' to inject malicious executables and	7.8	More Details

	escalate privileges.		
CVE-2021-47878	eBeam Education Suite 2.5.0.9 contains an unquoted service path vulnerability in the eBeam Device Service that allows local users to potentially execute code with elevated privileges. Attackers can exploit the unquoted path in the service configuration to inject malicious code that would execute with LocalSystem privileges during service startup.	7.8	More Details
CVE-2021-47887	OKI Print Job Accounting 4.4.10 contains an unquoted service path vulnerability in the OkiJaSvc service that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in 'C:\Program Files\Okidata\Print Job Accounting\' to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2021-47879	eBeam Interactive Suite 3.6 contains an unquoted service path vulnerability in the eBeam Stylus Driver service that allows local users to potentially execute code with elevated privileges. Attackers can exploit the unquoted path in C:\Program Files (x86)\Luidia\eBeam Stylus Driver\ to inject malicious executables that would run with LocalSystem permissions.	7.8	More Details
CVE-2021-47874	VFS for Git 1.0.21014.1 contains an unquoted service path vulnerability in the GVFS.Service Windows service that allows local attackers to execute code with elevated privileges. Attackers can exploit the unquoted binary path to inject malicious executables that will be launched with LocalSystem privileges during service startup or system reboot.	7.8	More Details
CVE-2021-47880	Realtek Wireless LAN Utility 700.1631 contains an unquoted service path vulnerability that allows local users to potentially execute code with elevated system privileges. Attackers can exploit the unquoted service path by inserting malicious code in the system root path that would execute during application startup or system reboot.	7.8	More Details
CVE-2026-24875	Integer Overflow or Wraparound vulnerability in yoyofr modizer.This issue affects modizer: before 4.1.1.	7.8	More Details
CVE-2025-41727	A local low privileged attacker can bypass the authentication of the Device Manager user interface, allowing them to perform privileged operations and gain administrator access.	7.8	More Details
CVE-2026-1361	ASDA-Soft Stack-based Buffer Overflow Vulnerability	7.8	More Details
CVE-2020-36974	Realtek Andrea RT Filters 1.0.64.7 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 'C:\Program Files\IDT\WDM\AESTSr64.exe' to inject malicious code that would execute during service startup or system reboot.	7.8	More Details
CVE-2021-47869	Brother BRAdmin Professional 3.75 contains an unquoted service path vulnerability in the BRA_Scheduler service that allows local users to potentially execute arbitrary code. Attackers can place a malicious executable named 'BRAdmin' in the C:\Program Files (x86)\Brother\ directory to gain local system privileges.	7.8	More Details
CVE-2021-47886	Pingzapper 2.3.1 contains an unquoted service path vulnerability in the PingzapperSvc service that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in 'C:\Program Files (x86)\Pingzapper\PZService.exe' to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2021-47868	WIN-PACK PRO 4.8 contains an unquoted service path vulnerability in the WPCommandFileService that allows local users to potentially execute code with elevated privileges. Attackers can exploit the unquoted path in C:\Program Files <x86>\WINPAKPRO\WPCommandFileService Service.exe to inject malicious code that would execute with LocalSystem permissions.	7.8	More Details
CVE-2021-47883	Sandboxie Plus 0.7.2 contains an unquoted service path vulnerability in the SbieSvc service that allows local attackers to execute code with elevated privileges. Attackers can exploit the unquoted binary path to inject malicious executables that will be launched with LocalSystem permissions during service startup.	7.8	More Details

CVE-2026-21509	Reliance on untrusted inputs in a security decision in Microsoft Office allows an unauthorized attacker to bypass a security feature locally.	7.8	More Details
CVE-2026-24873	Out-of-bounds Read vulnerability in Rinnegatamante lpp-vita.This issue affects lpp-vita: before lpp-vita r6.	7.8	More Details
CVE-2025-33234	NVIDIA runx contains a vulnerability where an attacker could cause a code injection. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-23881	Kyverno is a policy engine designed for cloud native platform engineering teams. Versions prior to 1.16.3 and 1.15.3 have unbounded memory consumption in Kyverno's policy engine that allows users with policy creation privileges to cause denial of service by crafting policies that exponentially amplify string data through context variables. Versions 1.16.3 and 1.15.3 contain a patch for the vulnerability.	7.7	More Details
CVE-2025-69311	Missing Authorization vulnerability in Broadstreet Broadstreet Ads broadstreet allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Broadstreet Ads: from n/a through <= 1.52.1.	7.6	More Details
CVE-2026-24538	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in omnipressteam Omnipress omnipress allows PHP Local File Inclusion.This issue affects Omnipress: from n/a through <= 1.6.6.	7.6	More Details
CVE-2026-22470	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in FireStorm Plugins FireStorm Professional Real Estate fs-real-estate-plugin allows Blind SQL Injection.This issue affects FireStorm Professional Real Estate: from n/a through <= 2.7.11.	7.6	More Details
CVE-2025-27380	HTML injection in Project Release in Altium Enterprise Server (AES) 7.0.3 on all platforms allows an authenticated attacker to execute arbitrary JavaScript in the victim’s browser via crafted HTML content.	7.6	More Details
CVE-2026-23737	seroval facilitates JS value stringification, including complex structures beyond JSON.stringify capabilities. In versions 1.4.0 and below, improper input handling in the JSON deserialization component can lead to arbitrary JavaScript code execution. Exploitation is possible via overriding constant value and error deserialization, allowing indirect access to unsafe JS evaluation. At minimum, attackers need the ability to perform 4 separate requests on the same function, and partial knowledge of how the serialized data is used during later runtime processing. This vulnerability affects the fromJSON and fromCrossJSON functions in a client-to-server transmission scenario. This issue has been fixed in version 1.4.0.	7.5	More Details
CVE-2021-47895	Nsauditor 3.2.2.0 contains a denial of service vulnerability that allows attackers to crash the application by overwriting the Event Description field with a large buffer. Attackers can generate a 10,000-character 'U' buffer and paste it into the Event Description field to trigger an application crash.	7.5	More Details
CVE-2025-66720	Null pointer dereference in free5gc pcf 1.4.0 in file internal/sbi/processor/ampolicy.go in function HandleDeletePoliciesPolAssoId.	7.5	More Details
CVE-2026-22260	Suricata is a network IDS, IPS and NSM engine. Starting in version 8.0.0 and prior to version 8.0.3, Suricata can crash with a stack overflow. Version 8.0.3 patches the issue. As a workaround, use default values for \`request-body-limit\` and \`response-body-limit\`.	7.5	More Details
CVE-2026-24827	Out-of-bounds Write vulnerability in gerstrong Commander-Genius.This issue affects Commander-Genius: before Release refs/pull/358/merge.	7.5	More Details
CVE-2026-	Missing Release of Memory after Effective Lifetime vulnerability in Is-Daouda is-Engine.This	7.5	More

24828	issue affects is-Engine: before 3.3.4.		Details
CVE-2025-70648	Tenda AX1803 v1.0.0.1 was discovered to contain a stack overflow in the security_5g parameter of the sub_727F4 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2021-47894	Managed Switch Port Mapping Tool 2.85.2 contains a denial of service vulnerability that allows attackers to crash the application by creating an oversized buffer. Attackers can generate a 10,000-character buffer and paste it into the IP Address and SNMP Community Name fields to trigger the application crash.	7.5	More Details
CVE-2025-70646	Tenda AX1803 v1.0.0.1 was discovered to contain a stack overflow in the security parameter of the sub_72290 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2021-47893	AgataSoft PingMaster Pro 2.1 contains a denial of service vulnerability in the Trace Route feature that allows attackers to crash the application by overflowing the host name input field. Attackers can generate a 10,000-character buffer and paste it into the host name field to trigger an application crash and potential system instability.	7.5	More Details
CVE-2025-70644	Tenda AX-1806 v1.0.0.1 was discovered to contain a stack overflow in the time parameter of the sub_60CFC function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2026-22464	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in wphocus My auctions allegro my-auctions-allegro-free-edition allows PHP Local File Inclusion.This issue affects My auctions allegro: from n/a through <= 3.6.33.	7.5	More Details
CVE-2025-69908	An unauthenticated information disclosure vulnerability in Newgen OmniApp allows attackers to enumerate valid privileged usernames via a publicly accessible client-side JavaScript resource.	7.5	More Details
CVE-2025-68905	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in jegtheme JNews - Pay Writer jnews-pay-writer allows PHP Local File Inclusion.This issue affects JNews - Pay Writer: from n/a through <= 11.0.0.	7.5	More Details
CVE-2025-70651	Tenda AX-1803 v1.0.0.1 was discovered to contain a stack overflow in the ssid parameter of the form_fast_setting_wifi_set function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-69313	Missing Authorization vulnerability in WPXPO PostX ultimate-post allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PostX: from n/a through <= 5.0.3.	7.5	More Details
CVE-2026-24783	soroban-fixed-point-math is a fixed-point math library for Soroban smart contacts. In versions 1.3.0 and 1.4.0, the `mulDiv(x, y, z)` function incorrectly handled cases where both the intermediate product $x * y$ and the divisor z were negative. The logic assumed that if the intermediate product was negative, the final result must also be negative, neglecting the sign of z. This resulted in rounding being applied in the wrong direction for cases where both $x * y$ and z were negative. The functions most at risk are `fixed_div_floor` and `fixed_div_ceil`, as they often use non-constant numbers as the divisor z in `mulDiv`. This error is present in all signed `FixedPoint` and `SorobanFixedPoint` implementations, including `i64`, `i128`, and `I256`. Versions 1.3.1 and 1.4.1 contain a patch. No known workarounds for this issue are available.	7.5	More Details
CVE-2026-22401	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in pavothemes Freshio freshio allows PHP Local File Inclusion.This issue affects Freshio: from n/a through <= 2.4.2.	7.5	More Details
CVE-2020-36949	TapinRadio 2.13.7 contains a denial of service vulnerability in the application proxy settings that allows attackers to crash the program by overflowing input fields. Attackers can paste a large buffer of 20,000 characters into the username and address fields to cause the	7.5	More Details

	application to become unresponsive and require reinstallation.		
CVE-2025-63019	Insertion of Sensitive Information Into Sent Data vulnerability in Johan Jonk Stenström Cookies and Content Security Policy cookies-and-content-security-policy allows Retrieve Embedded Sensitive Data.This issue affects Cookies and Content Security Policy: from n/a through <= 2.34.	7.5	More Details
CVE-2025-69319	Improper Control of Generation of Code ('Code Injection') vulnerability in Beaver Builder Beaver Builder beaver-builder-lite-version allows Code Injection.This issue affects Beaver Builder: from n/a through <= 2.9.4.1.	7.5	More Details
CVE-2025-63051	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in sizam REHub Framework rehub-framework allows Retrieve Embedded Sensitive Data.This issue affects REHub Framework: from n/a through < 19.9.9.4.	7.5	More Details
CVE-2020-36946	SyncBreeze 10.0.28 contains a denial of service vulnerability in the login endpoint that allows remote attackers to crash the service. Attackers can send an oversized payload in the login request to overwhelm the application and potentially disrupt service availability.	7.5	More Details
CVE-2026-22258	Suricata is a network IDS, IPS and NSM engine. Prior to versions 8.0.3 and 7.0.14, crafted DCERPC traffic can cause Suricata to expand a buffer w/o limits, leading to memory exhaustion and the process getting killed. While reported for DCERPC over UDP, it is believed that DCERPC over TCP and SMB are also vulnerable. DCERPC/TCP in the default configuration should not be vulnerable as the default stream depth is limited to 1MiB. Versions 8.0.3 and 7.0.14 contain a patch. Some workarounds are available. For DCERPC/UDP, disable the parser. For DCERPC/TCP, the \`stream.reassembly.depth\` setting will limit the amount of data that can be buffered. For DCERPC/SMB, the \`stream.reassembly.depth\` can be used as well, but is set to unlimited by default. Imposing a limit here may lead to loss of visibility in SMB.	7.5	More Details
CVE-2020-36939	Cassandra Web 0.5.0 contains a directory traversal vulnerability that allows unauthenticated attackers to read arbitrary files by manipulating path traversal parameters. Attackers can exploit the disabled Rack::Protection module to read sensitive system files like /etc/passwd and retrieve Apache Cassandra database credentials.	7.5	More Details
CVE-2025-70650	Tenda AX-1806 v1.0.0.1 was discovered to contain a stack overflow in the deviceList parameter of the formSetMacFilterCfg function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2026-22402	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in pavothemes Triply triply allows PHP Local File Inclusion.This issue affects Triply: from n/a through <= 2.4.7.	7.5	More Details
CVE-2025-52026	An information disclosure vulnerability exists in the /srvs/membersrv/getCashiers endpoint of the Aptsys gemscms backend platform thru 2025-05-28. This unauthenticated endpoint returns a list of cashier accounts, including names, email addresses, usernames, and passwords hashed using MD5. As MD5 is a broken cryptographic function, the hashes can be easily reversed using public tools, exposing user credentials in plaintext. This allows remote attackers to perform unauthorized logins and potentially gain access to sensitive POS operations or backend functions.	7.5	More Details
CVE-2026-22259	Suricata is a network IDS, IPS and NSM engine. Prior to versions 8.0.3 and 7.0.14, specially crafted traffic can cause Suricata to consume large amounts of memory while parsing DNP3 traffic. This can lead to the process slowing down and running out of memory, potentially leading to it getting killed by the OOM killer. Versions 8.0.3 or 7.0.14 contain a patch. As a workaround, disable the DNP3 parser in the suricata yaml (disabled by default).	7.5	More Details
CVE-2025-70986	Incorrect access control in the selectDept function of RuoYi v4.8.2 allows unauthorized attackers to arbitrarily access sensitive department data.	7.5	More Details
CVE-2025-67221	The orjson.dumps function in orjson thru 3.11.4 does not limit recursion for deeply nested JSON documents.	7.5	More Details

CVE-2026-24609	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Laurent laurent allows PHP Local File Inclusion.This issue affects Laurent: from n/a through <= 3.1.	7.5	More Details
CVE-2025-13878	Malformed BRID/HHIT records can cause `named` to terminate unexpectedly. This issue affects BIND 9 versions 9.18.40 through 9.18.43, 9.20.13 through 9.20.17, 9.21.12 through 9.21.16, 9.18.40-S1 through 9.18.43-S1, and 9.20.13-S1 through 9.20.17-S1.	7.5	More Details
CVE-2025-70645	Tenda AX-1806 v1.0.0.1 was discovered to contain a stack overflow in the deviceList parameter of the formSetWifiMacFilterCfg function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2026-24635	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in DevsBlink EduBlink Core edublink-core allows PHP Local File Inclusion.This issue affects EduBlink Core: from n/a through <= 2.0.7.	7.5	More Details
CVE-2026-24536	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in webpushr Webpushr webpushr-web-push-notifications allows Retrieve Embedded Sensitive Data.This issue affects Webpushr: from n/a through <= 4.38.0.	7.5	More Details
CVE-2026-24608	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Laurent Core laurent-core allows PHP Local File Inclusion.This issue affects Laurent Core: from n/a through <= 2.4.1.	7.5	More Details
CVE-2026-0911	The Hustle – Email Marketing, Lead Generation, Optins, Popups plugin for WordPress is vulnerable to arbitrary file uploads due to incorrect file type validation in the action_import_module() function in all versions up to, and including, 7.8.9.2. This makes it possible for authenticated attackers, with a lower-privileged role (e.g., Subscriber-level access and above), to upload arbitrary files on the affected site's server which may make remote code execution possible. Successful exploitation requires an admin to grant Hustle module permissions (or module edit access) to the low-privileged user so they can access the Hustle admin page and obtain the required nonce.	7.5	More Details
CVE-2026-23962	Mastodon is a free, open-source social network server based on ActivityPub. Mastodon versions before v4.3.18, v4.4.12, and v4.5.5 do not have a limit on the maximum number of poll options for remote posts, allowing attackers to create polls with a very large amount of options, greatly increasing resource consumption. Depending on the number of poll options, an attacker can cause disproportionate resource usage in both Mastodon servers and clients, potentially causing Denial of Service either server-side or client-side. Mastodon versions v4.5.5, v4.4.12, v4.3.18 are patched.	7.5	More Details
CVE-2026-23965	sm-crypto provides JavaScript implementations of the Chinese cryptographic algorithms SM2, SM3, and SM4. A signature forgery vulnerability exists in the SM2 signature verification logic of sm-crypto prior to version 0.4.0. Under default configurations, an attacker can forge valid signatures for arbitrary public keys. If the message space contains sufficient redundancy, the attacker can fix the prefix of the message associated with the forged signature to satisfy specific formatting requirements. Version 0.4.0 patches the issue.	7.5	More Details
CVE-2026-23967	sm-crypto provides JavaScript implementations of the Chinese cryptographic algorithms SM2, SM3, and SM4. A signature malleability vulnerability exists in the SM2 signature verification logic of the sm-crypto library prior to version 0.3.14. An attacker can derive a new valid signature for a previously signed message from an existing signature. Version 0.3.14 patches the issue.	7.5	More Details
CVE-2026-24138	FOG is a free open-source cloning/imaging/rescue suite/inventory management system. Versions 1.5.10.1754 and below contain an unauthenticated SSRF vulnerability in getversion.php which can be triggered by providing a user-controlled url parameter. It can be used to fetch both internal websites and files on the machine running FOG. This appears to be reachable without an authenticated web session when the request includes newService=1. The issue does not have a fixed release version at the time of publication.	7.5	More Details
	GeoGebra Graphing Calculator 6.0.631.0 contains a denial of service vulnerability that		

CVE-2021-47877	allows attackers to crash the application by inputting an oversized buffer. Attackers can generate a payload of 8000 repeated characters to overwhelm the input field and cause the application to become unresponsive.	7.5	More Details
CVE-2026-24831	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in ixray-team ixray-1.6-stcop.This issue affects ixray-1.6-stcop: before 1.3.	7.5	More Details
CVE-2026-21520	Exposure of Sensitive Information to an Unauthorized Actor in Copilot Studio allows a unauthenticated attacker to view sensitive information through network attack vector	7.5	More Details
CVE-2021-47876	GeoGebra Classic 5.0.631.0-d contains a denial of service vulnerability in the input field that allows attackers to crash the application by sending oversized buffer content. Attackers can generate a large buffer of 800,000 repeated characters and paste it into the 'Entrada:' input field to trigger an application crash.	7.5	More Details
CVE-2026-24006	Seroval facilitates JS value stringification, including complex structures beyond JSON.stringify capabilities. In versions 1.4.0 and below, serialization of objects with extreme depth can exceed the maximum call stack limit. In version 1.4.1, Seroval introduces a `depthLimit` parameter in serialization/deserialization methods. An error will be thrown if the depth limit is reached.	7.5	More Details
CVE-2025-68882	Missing Authorization vulnerability in Scalenut Scalenut scalenut allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Scalenut: from n/a through <= 1.1.3.	7.5	More Details
CVE-2026-23864	Multiple denial of service vulnerabilities exist in React Server Components, affecting the following packages: react-server-dom-parcel, react-server-dom-turbopack, react-server-dom-webpack. The vulnerabilities are triggered by sending specially crafted HTTP requests to Server Function endpoints, and could lead to server crashes, out-of-memory exceptions or excessive CPU usage; depending on the vulnerable code path being exercised, the application configuration and application code. Strongly consider upgrading to the latest package versions to reduce risk and prevent availability issues in applications using React Server Components.	7.5	More Details
CVE-2025-53968	This vulnerability arises because there are no limitations on the number of authentication attempts a user can make. An attacker can exploit this weakness by continuously sending authentication requests, leading to a denial-of-service (DoS) condition. This can overwhelm the authentication system, rendering it unavailable to legitimate users and potentially causing service disruption. This can also allow attackers to conduct brute-force attacks to gain unauthorized access.	7.5	More Details
CVE-2026-24390	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in QantumThemes Kentha Elementor Widgets kentha-elementor allows PHP Local File Inclusion.This issue affects Kentha Elementor Widgets: from n/a through < 3.1.	7.5	More Details
CVE-2026-20736	Gitea does not properly verify repository context when deleting attachments. A user who previously uploaded an attachment to a repository may be able to delete it after losing access to that repository by making the request through a different repository they can access.	7.5	More Details
CVE-2025-67274	An issue in continuous.software aangine v.2025.2 allows a remote attacker to obtain sensitive information via the excel-integration-service template download module, integration-persistence-service job listing module, portfolio-item-service data retrieval module endpoints	7.5	More Details
CVE-2021-47865	ProFTPD 1.3.7a contains a denial of service vulnerability that allows attackers to overwhelm the server by creating multiple simultaneous FTP connections. Attackers can repeatedly establish connections using threading to exhaust server connection limits and block legitimate user access.	7.5	More Details

CVE-2026-1330	MeetingHub developed by HAMASTAR Technology has an Arbitrary File Read vulnerability, allowing unauthenticated remote attackers to exploit Absolute Path Traversal to download arbitrary system files.	7.5	More Details
CVE-2026-21720	Every uncached /avatar/:hash request spawns a goroutine that refreshes the Gravatar image. If the refresh sits in the 10-slot worker queue longer than three seconds, the handler times out and stops listening for the result, so that goroutine blocks forever trying to send on an unbuffered channel. Sustained traffic with random hashes keeps tripping this timeout, so goroutine count grows linearly, eventually exhausting memory and causing Grafana to crash on some systems.	7.5	More Details
CVE-2026-23957	seroval facilitates JS value stringification, including complex structures beyond JSON.stringify capabilities. In versions 1.4.0 and below, overriding encoded array lengths by replacing them with an excessively large value causes the deserialization process to significantly increase processing time. This issue has been fixed in version 1.4.1.	7.5	More Details
CVE-2021-47850	Mini Mouse 9.2.0 contains a path traversal vulnerability that allows remote attackers to access arbitrary system files and directories through crafted HTTP requests. Attackers can retrieve sensitive files like win.ini and list contents of system directories such as C:\Users\Public by manipulating file and path parameters.	7.5	More Details
CVE-2021-47746	NodeBB Plugin Emoji 3.2.1 contains an arbitrary file write vulnerability that allows administrative users to write files to arbitrary system locations through the emoji upload API. Attackers with admin access can craft file upload requests with directory traversal to overwrite system files by manipulating the file path parameter.	7.5	More Details
CVE-2025-13928	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.7 before 18.6.4, 18.7 before 18.7.2, and 18.8 before 18.8.2 that could have allowed an unauthenticated user to cause a denial of service condition by exploiting incorrect authorization validation in API endpoints.	7.5	More Details
CVE-2025-13927	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 11.9 before 18.6.4, 18.7 before 18.7.2, and 18.8 before 18.8.2 that could have allowed an unauthenticated user to create a denial of service condition by sending crafted requests with malformed authentication data.	7.5	More Details
CVE-2026-23593	A vulnerability in the web-based management interface of HPE Aruba Networking Fabric Composer could allow an unauthenticated remote attacker to view some system files. Successful exploitation could allow an attacker to read files within the affected directory.	7.5	More Details
CVE-2025-10855	Authorization Bypass Through User-Controlled Key vulnerability in Solvera Software Services Trade Inc. Teknoera allows Exploitation of Trusted Identifiers.This issue affects Teknoera: through 01102025.	7.5	More Details
CVE-2025-68907	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in AivahThemes Hostme v2 hostmev2 allows Path Traversal.This issue affects Hostme v2: from n/a through <= 7.0.	7.5	More Details
CVE-2026-24469	C++ HTTP Server is an HTTP/1.1 server built to handle client connections and serve HTTP requests. Versions 1.0 and below are vulnerable to Path Traversal via the RequestHandler::handleRequest method. This flaw allows an unauthenticated, remote attacker to read arbitrary files from the server's filesystem by crafting a malicious HTTP GET request containing ../ sequences. The application fails to sanitize the filename variable derived from the user-controlled URL path, directly concatenating it to the files_directory base path and enabling traversal outside the intended root. No patch was available at the time of publication.	7.5	More Details
CVE-2025-10024	Authorization Bypass Through User-Controlled Key vulnerability in EXERT Computer Technologies Software Ltd. Co. Education Management System allows Parameter Injection.This issue affects Education Management System: through 23.09.2025.	7.5	More Details
CVE-2025-	An issue in ollama v.0.12.10 allows a remote attacker to cause a denial of service via the fs/ggml/gguf.go, function readGGUFV1String reads a string length from untrusted GGUF	7.5	More

66960	metadata		Details
CVE-2025-66959	An issue in ollama v.0.12.10 allows a remote attacker to cause a denial of service via the GGUF decoder	7.5	More Details
CVE-2026-23956	seroval facilitates JS value stringification, including complex structures beyond JSON.stringify capabilities. In versions 1.4.0 and below, overriding RegExp serialization with extremely large patterns can exhaust JavaScript runtime memory during deserialization. Additionally, overriding RegExp serialization with patterns that trigger catastrophic backtracking can lead to ReDoS (Regular Expression Denial of Service). This issue has been fixed in version 1.4.1.	7.5	More Details
CVE-2021-47802	Tenda D151 and D301 routers contain an unauthenticated configuration download vulnerability that allows remote attackers to retrieve router configuration files. Attackers can send a request to /goform/getimage endpoint to download configuration data including admin credentials without authentication.	7.5	More Details
CVE-2026-24377	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in POSIMYTH Nexter Blocks the-plus-addons-for-block-editor allows Retrieve Embedded Sensitive Data.This issue affects Nexter Blocks: from n/a through <= 4.6.3.	7.5	More Details
CVE-2026-24523	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Marcus (aka @msykes) WP FullCalendar wp-fullcalendar allows Retrieve Embedded Sensitive Data.This issue affects WP FullCalendar: from n/a through <= 1.6.	7.5	More Details
CVE-2025-69907	An unauthenticated information disclosure vulnerability exists in Newgen OmniDocs due to missing authentication and access control on the /omnidocs/GetListofCabinet API endpoint. A remote attacker can access this endpoint without valid credentials to retrieve sensitive internal configuration information, including cabinet names and database-related metadata. This allows unauthorized enumeration of backend deployment details and may facilitate further targeted attacks.	7.5	More Details
CVE-2026-1257	The Administrative Shortcodes plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 0.3.4 via the 'slug' attribute of the 'get_template' shortcode. This is due to insufficient path validation on user-supplied input passed to the get_template_part() function. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.	7.5	More Details
CVE-2026-22271	Dell ECS, versions 3.8.1.0 through 3.8.1.7, and Dell ObjectScale versions prior to 4.2.0.0, contains a Cleartext Transmission of Sensitive Information vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to information exposure.	7.5	More Details
CVE-2025-56589	A Local File Inclusion (LFI) and a Server-Side Request Forgery (SSRF) vulnerability was found in the InsertFromHtmlString() function of the Apryse HTML2PDF SDK thru 11.6.0. These vulnerabilities could allow an attacker to read local files on the server or make arbitrary HTTP requests to internal or external services. Both vulnerabilities could lead to the disclosure of sensitive data or potential system takeover.	7.5	More Details
CVE-2026-21521	Improper neutralization of escape, meta, or control sequences in Copilot allows an unauthorized attacker to disclose information over a network.	7.4	More Details
CVE-2026-21524	Exposure of sensitive information to an unauthorized actor in Azure Data Explorer allows an unauthorized attacker to disclose information over a network.	7.4	More Details
	EVerest is an EV charging software stack. In versions 2025.9.0 and below, an attacker can exhaust the operating system's memory and cause the module to terminate by initiating		

CVE-2025-68133	an unlimited number of TCP connections that never proceed to ISO 15118-2 communication. This is possible because a new thread is started for each incoming plain TCP or TLS socket connection before any verification occurs, and the verification performed is too permissive. The EVerest processes and all its modules shut down, affecting all EVSE functionality. This issue is fixed in version 2025.10.0.	7.4	More Details
CVE-2025-69822	An issue in Atomberg Atomberg Erica Smart Fan Firmware Version: V1.0.36 allows an attacker to obtain sensitive information and escalate privileges via a crafted deauth frame	7.4	More Details
CVE-2025-68141	EVerest is an EV charging software stack. Prior to version 2025.10.0, during the deserialization of a `DC_ChargeLoopRes` message that includes Receipt as well as TaxCosts, the vector `<DetailedTax>tax_costs` in the target `Receipt` structure is accessed out of bounds. This occurs in the method `template <> void convert(const struct iso20_dc_DetailedTaxType& in, datatypes::DetailedTax& out)` which leads to a null pointer dereference and causes the module to terminate. The EVerest processes and all its modules shut down, affecting all EVSE. Version 2025.10.0 fixes the issue.	7.4	More Details
CVE-2025-65098	Typebot is an open-source chatbot builder. In versions prior to 3.13.2, client-side script execution in Typebot allows stealing all stored credentials from any user. When a victim previews a malicious typebot by clicking "Run", JavaScript executes in their browser and exfiltrates their OpenAI keys, Google Sheets tokens, and SMTP passwords. The `/api/trpc/credentials.getCredentials` endpoint returns plaintext API keys without verifying credential ownership. Version 3.13.2 fixes the issue.	7.4	More Details
CVE-2025-68136	EVerest is an EV charging software stack. Prior to version 2025.10.0, once the module receives a SDP request, it creates a whole new set of objects like `Session`, `IConnection` which open new TCP socket for the ISO15118-20 communications and registers callbacks for the created file descriptor, without closing and destroying the previous ones. Previous `Session` is not saved and the usage of an `unique_ptr` is lost, destroying connection data. Latter, if the used socket and therefore file descriptor is not the last one, it will lead to a null pointer dereference. Version 2025.10.0 fixes the issue.	7.4	More Details
CVE-2025-69821	An issue in Beat XP VEGA Smartwatch (Firmware Version - RB303ATV006229) allows an attacker to cause a denial of service via the BLE connection	7.4	More Details
CVE-2026-24123	BentoML is a Python library for building online serving systems optimized for AI apps and model inference. Prior to version 1.4.34, BentoML's `bentofile.yaml` configuration allows path traversal attacks through multiple file path fields (`description`, `docker.setup_script`, `docker.dockerfile_template`, `conda.environment_yml`). An attacker can craft a malicious bentofile that, when built by a victim, exfiltrates arbitrary files from the filesystem into the bento archive. This enables supply chain attacks where sensitive files (SSH keys, credentials, environment variables) are silently embedded in bentos and exposed when pushed to registries or deployed. Version 1.4.34 contains a patch for the issue.	7.4	More Details
CVE-2025-68134	EVerest is an EV charging software stack. Prior to version 2025.10.0, the use of the `assert` function to handle errors frequently causes the module to crash. This is particularly critical because the manager shuts down all other modules and exits when any one of them terminates, leading to a denial of service. In a context where a manager handles multiple EVSE, this would also impact other users. Version 2025.10.0 fixes the issue.	7.4	More Details
CVE-2026-0723	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.6 before 18.6.4, 18.7 before 18.7.2, and 18.8 before 18.8.2 that could have allowed an individual with existing knowledge of a victim's credential ID to bypass two-factor authentication by submitting forged device responses.	7.4	More Details
CVE-2026-22264	Suricata is a network IDS, IPS and NSM engine. Prior to version 8.0.3 and 7.0.14, an unsigned integer overflow can lead to a heap use-after-free condition when generating excessive amounts of alerts for a single packet. Versions 8.0.3 and 7.0.14 contain a patch. As a workaround, do not run untrusted rulesets or run with less than 65536 signatures that can match on the same packet.	7.4	More Details

CVE-2025-68902	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in AivahThemes Anona anona allows Path Traversal.This issue affects Anona: from n/a through <= 8.0.	7.3	More Details
CVE-2024-11976	The The BuddyPress plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 14.3.3. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2025-69187	Missing Authorization vulnerability in e-plugins Final User final-user allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Final User: from n/a through <= 1.2.5.	7.3	More Details
CVE-2025-69185	Missing Authorization vulnerability in e-plugins Hotel Listing hotel-listing allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Hotel Listing: from n/a through <= 1.4.2.	7.3	More Details
CVE-2026-1449	A flaw has been found in Hisense TransTech Smart Bus Management System up to 20260113. Affected is the function Page_Load of the file YZSoft/Forms/XForm/BM/BusComManagement/TireMng.aspx. Executing a manipulation of the argument key can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-69184	Missing Authorization vulnerability in e-plugins Institutions Directory institutions-directory allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Institutions Directory: from n/a through <= 1.3.4.	7.3	More Details
CVE-2025-69181	Missing Authorization vulnerability in e-plugins Lawyer Directory lawyer-directory allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Lawyer Directory: from n/a through <= 1.3.4.	7.3	More Details
CVE-2025-69190	Missing Authorization vulnerability in e-plugins Listihub listihub allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Listihub: from n/a through <= 1.0.6.	7.3	More Details
CVE-2025-69048	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Universal Video Player universal-video-player allows Reflected XSS.This issue affects Universal Video Player: from n/a through <= 3.8.4.	7.3	More Details
CVE-2025-69051	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CridioStudio ListingPro Reviews listingpro-reviews allows Reflected XSS.This issue affects ListingPro Reviews: from n/a through <= 1.7.	7.3	More Details
CVE-2025-69053	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Universal Video Player universal-video-player allows Reflected XSS.This issue affects Universal Video Player: from n/a through <= 3.8.4.	7.3	More Details
CVE-2025-68904	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jegtheme JNews - Frontend Submit jnews-frontend-submit allows Reflected XSS.This issue affects JNews - Frontend Submit: from n/a through <= 11.0.0.	7.3	More Details
CVE-2025-69188	Missing Authorization vulnerability in e-plugins fitness-trainer fitness-trainer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects fitness-trainer: from n/a through <= 1.7.1.	7.3	More Details
CVE-2025-69186	Missing Authorization vulnerability in e-plugins Hospital Doctor Directory hospital-doctor-directory allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Hospital Doctor Directory: from n/a through <= 1.3.9.	7.3	More Details
CVE-2025-69191	Missing Authorization vulnerability in e-plugins ListingHub listinghub allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ListingHub: from n/a through <= 1.2.7.	7.3	More Details
	A vulnerability has been found in Sangfor Operation and Maintenance Security		

CVE-2026-1412	Management System up to 3.0.12. The impacted element is an unknown function of the file /fort/audit/get_clip_img of the component HTTP POST Request Handler. Such manipulation of the argument frame/dirno leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-68906	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jegtheme JNews - Video jnews-video allows Reflected XSS.This issue affects JNews - Video: from n/a through <= 11.0.2.	7.3	More Details
CVE-2025-27821	Out-of-bounds Write vulnerability in Apache Hadoop HDFS native client. This issue affects Apache Hadoop: from 3.2.0 before 3.4.2. Users are recommended to upgrade to version 3.4.2, which fixes the issue.	7.3	More Details
CVE-2026-23988	Rufus is a utility that helps format and create bootable USB flash drives. Versions 4.11 and below contain a race condition (TOCTOU) in src/net.c during the creation, validation, and execution of the Fido PowerShell script. Since Rufus runs with elevated privileges (Administrator) but writes the script to the %TEMP% directory (writeable by standard users) without locking the file, a local attacker can replace the legitimate script with a malicious one between the file write operation and the execution step. This allows arbitrary code execution with Administrator privileges. This issue has been fixed in version 4.12_BETA.	7.3	More Details
CVE-2026-1422	A vulnerability was found in code-projects Online Examination System 1.0. Affected by this vulnerability is an unknown functionality of the file /index.php of the component Login Page. Performing a manipulation of the argument User results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-55705	This vulnerability occurs when the system permits multiple simultaneous connections to the backend using the same charging station ID. This can result in unauthorized access, data inconsistency, or potential manipulation of charging sessions. The lack of proper session management and expiration control allows attackers to exploit this weakness by reusing valid charging station IDs to establish multiple sessions concurrently.	7.3	More Details
CVE-2026-23736	seroval facilitates JS value stringification, including complex structures beyond JSON.stringify capabilities. In versions 1.4.0 and below, due to improper input validation, a malicious object key can lead to prototype pollution during JSON deserialization. This vulnerability affects only JSON deserialization functionality. This issue is fixed in version 1.4.1.	7.3	More Details
CVE-2025-69192	Missing Authorization vulnerability in e-plugins Real Estate Pro real-estate-pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Real Estate Pro: from n/a through <= 2.1.5.	7.3	More Details
CVE-2025-69193	Missing Authorization vulnerability in e-plugins WP Membership wp-membership allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Membership: from n/a through <= 1.6.4.	7.3	More Details
CVE-2026-1443	A flaw has been found in code-projects Online Music Site 1.0. Affected by this issue is some unknown functionality of the file /Administrator/PHP/AdminDeleteUser.php. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-24624	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in saeros1984 Neoforum neoforum allows Blind SQL Injection.This issue affects Neoforum: from n/a through <= 1.0.	7.2	More Details
CVE-2021-47897	PEEL Shopping 9.3.0 contains a stored cross-site scripting vulnerability in the address parameter of the change_params.php script. Attackers can inject malicious JavaScript payloads that execute when users interact with the address text box, potentially enabling client-side script execution.	7.2	More Details
CVE-2026-	The Frontis Blocks plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.1.6. This is due to insufficient restriction on the 'url' parameter in the 'template_proxy' function. This makes it possible for unauthenticated	7.2	More Details

0807	attackers to make web requests to arbitrary locations originating from the web application via the '/template-proxy/' and '/proxy-image/' endpoint.		
CVE-2026-23592	Insecure file operations in HPE Aruba Networking Fabric Composerâ€™s backup functionality could allow authenticated attackers to achieve remote code execution. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system.	7.2	More Details
CVE-2021-47873	VestaCP versions prior to 0.9.8-25 contain a cross-site scripting vulnerability in the IP interface configuration that allows attackers to inject malicious scripts. Attackers can exploit the 'v_interface' parameter by sending a crafted POST request to the add/ip/ endpoint with a stored XSS payload.	7.2	More Details
CVE-2026-24478	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. Prior to version 1.10.0, a critical Path Traversal vulnerability in the DrupalWiki integration allows a malicious admin (or an attacker who can convince an admin to configure a malicious DrupalWiki URL) to write arbitrary files to the server. This can lead to Remote Code Execution (RCE) by overwriting configuration files or writing executable scripts. Version 1.10.0 fixes the issue.	7.2	More Details
CVE-2021-47858	Genexis Platinum-4410 P4410-V2-1.31A contains a stored cross-site scripting vulnerability in the 'start_addr' parameter of the Security Management interface. Attackers can inject malicious scripts through the start source address field that will persist and trigger for privileged users when they access the security management page.	7.2	More Details
CVE-2021-47892	PEEL Shopping 9.3.0 contains a stored cross-site scripting vulnerability in the 'Comments / Special Instructions' parameter of the purchase page. Attackers can inject malicious JavaScript payloads that will execute when the page is refreshed, potentially allowing client-side script execution.	7.2	More Details
CVE-2026-0800	The User Submitted Posts – Enable Users to Submit Posts from the Front End plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom fields in all versions up to, and including, 20251210 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2021-47857	Moodle 3.10.3 contains a persistent cross-site scripting vulnerability in the calendar event subtitle field that allows attackers to inject malicious scripts. Attackers can craft a calendar event with malicious JavaScript in the subtitle track label to execute arbitrary code when users view the event.	7.2	More Details
CVE-2026-1448	A vulnerability was detected in D-Link DIR-615 up to 4.10. This impacts an unknown function of the file /wiz_policy_3_machine.php of the component Web Management Interface. Performing a manipulation of the argument ipaddr results in os command injection. It is possible to initiate the attack remotely. The exploit is now public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	7.2	More Details
CVE-2021-47855	Openlitespeed 1.7.9 contains a stored cross-site scripting vulnerability in the dashboard's Notes parameter that allows administrators to inject malicious scripts. Attackers can craft a payload in the Notes field during listener configuration that will execute when an administrator clicks on the Default Icon.	7.2	More Details
CVE-2020-36947	LibreNMS 1.46 contains an authenticated SQL injection vulnerability in the MAC accounting graph endpoint that allows remote attackers to extract database information. Attackers can exploit the vulnerability by manipulating the 'sort' parameter with crafted SQL injection techniques to retrieve sensitive database contents through time-based blind SQL injection.	7.1	More Details
CVE-2025-68839	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Remi Corson Easy Theme Options easy-theme-options allows Reflected XSS.This issue affects Easy Theme Options: from n/a through <= 1.0.	7.1	More Details
CVE-	The AhaChat Messenger Marketing WordPress plugin through 1.1 does not sanitise and		

2025-14316	escape a parameter before outputting it 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-2026-24049	wheel is a command line tool for manipulating Python wheel files, as defined in PEP 427. In versions 0.40.0 through 0.46.1, the unpack function is vulnerable to file permission modification through mishandling of file permissions after extraction. The logic blindly trusts the filename from the archive header for the chmod operation, even though the extraction process itself might have sanitized the path. Attackers can craft a malicious wheel file that, when unpacked, changes the permissions of critical system files (e.g., /etc/passwd, SSH keys, config files), allowing for Privilege Escalation or arbitrary code execution by modifying now-writable scripts. This issue has been fixed in version 0.46.2.	7.1	More Details
CVE-2025-68883	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in extremeidea bidorbuy Store Integrator bidorbuystoreintegrator allows Reflected XSS.This issue affects bidorbuy Store Integrator: from n/a through <= 2.12.0.	7.1	More Details
CVE-2025-68884	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Arevico WP Simple Redirect wp-simple-redirect allows Reflected XSS.This issue affects WP Simple Redirect: from n/a through <= 1.1.	7.1	More Details
CVE-2025-68894	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in shoutoutglobal ShoutOut shoutout allows Reflected XSS.This issue affects ShoutOut: from n/a through <= 4.0.2.	7.1	More Details
CVE-2025-69054	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in highwarden Super Logos Showcase superlogoshowcase-wp allows Reflected XSS.This issue affects Super Logos Showcase: from n/a through <= 2.8.	7.1	More Details
CVE-2025-68858	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Casey Bisson wpCAS wpcas allows Reflected XSS.This issue affects wpCAS: from n/a through <= 1.07.	7.1	More Details
CVE-2026-24046	Backstage is an open framework for building developer portals. Multiple Scaffolder actions and archive extraction utilities were vulnerable to symlink-based path traversal attacks. An attacker with access to create and execute Scaffolder templates could exploit symlinks to read arbitrary files via the \`debug:log\` action by creating a symlink pointing to sensitive files (e.g., \`/etc/passwd\`, configuration files, secrets); delete arbitrary files via the \`fs:delete\` action by creating symlinks pointing outside the workspace, and write files outside the workspace via archive extraction (tar/zip) containing malicious symlinks. This affects any Backstage deployment where users can create or execute Scaffolder templates. This vulnerability is fixed in \`@backstage/backend-defaults\` versions 0.12.2, 0.13.2, 0.14.1, and 0.15.0; \`@backstage/plugin-scaffolder-backend\` versions 2.2.2, 3.0.2, and 3.1.1; and \`@backstage/plugin-scaffolder-node\` versions 0.11.2 and 0.12.3. Users should upgrade to these versions or later. Some workarounds are available. Follow the recommendation in the Backstage Threat Model to limit access to creating and updating templates, restrict who can create and execute Scaffolder templates using the permissions framework, audit existing templates for symlink usage, and/or run Backstage in a containerized environment with limited filesystem access.	7.1	More Details
CVE-2025-68835	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in matiskiba Ravpage ravpage allows Reflected XSS.This issue affects Ravpage: from n/a through <= 2.33.	7.1	More Details
CVE-2026-22355	Cross-Site Request Forgery (CSRF) vulnerability in gregmolnar Simple XML Sitemap simple-xml-sitemap allows Stored XSS.This issue affects Simple XML Sitemap: from n/a through <= 1.3.	7.1	More Details
CVE-2026-24411	iccDEV provides libraries and tools for interacting with, manipulating, and applying ICC color management profiles. Versions 2.3.1.1 and below have Undefined Behavior in CIccTagXmlSegmentedCurve::ToXml(). This occurs when user-controllable input is unsafely incorporated into ICC profile data or other structured binary blobs. Successful exploitation may allow an attacker to perform DoS, manipulate data, bypass application logic and Code Execution. This issue has been fixed in version 2.3.1.2.	7.1	More Details

CVE-2026-0535	A maliciously crafted HTML payload, stored in a component’s description and clicked by a user, can trigger a Stored Cross-site Scripting (XSS) vulnerability in the Autodesk Fusion desktop application. A malicious actor may leverage this vulnerability to read local files or execute arbitrary code in the context of the current process.	7.1	More Details
CVE-2025-69320	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand Magazine grandmagazine allows Reflected XSS.This issue affects Grand Magazine: from n/a through <= 3.5.7.	7.1	More Details
CVE-2026-22444	The "create core" API of Apache Solr 8.6 through 9.10.0 lacks sufficient input validation on some API parameters, which can cause Solr to check the existence of and attempt to read file-system paths that should be disallowed by Solr's "allowPaths" security setting https://https://solr.apache.org/guide/solr/latest/configuration-guide/configuring-solr-xml.html#the-solr-element . These read-only accesses can allow users to create cores using unexpected configsets if any are accessible via the filesystem. On Windows systems configured to allow UNC paths this can additionally cause disclosure of NTLM "user" hashes. Solr deployments are subject to this vulnerability if they meet the following criteria: * Solr is running in its "standalone" mode. * Solr's "allowPath" setting is being used to restrict file access to certain directories. * Solr's "create core" API is exposed and accessible to untrusted users. This can happen if Solr's RuleBasedAuthorizationPlugin https://solr.apache.org/guide/solr/latest/deployment-guide/rule-based-authorization-plugin.html is disabled, or if it is enabled but the "core-admin-edit" predefined permission (or an equivalent custom permission) is given to low-trust (i.e. non-admin) user roles. Users can mitigate this by enabling Solr's RuleBasedAuthorizationPlugin (if disabled) and configuring a permission-list that prevents untrusted users from creating new Solr cores. Users should also upgrade to Apache Solr 9.10.1 or greater, which contain fixes for this issue.	7.1	More Details
CVE-2025-69321	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand Spa grandspa allows Reflected XSS.This issue affects Grand Spa: from n/a through <= 3.5.5.	7.1	More Details
CVE-2026-0533	A maliciously crafted HTML payload in a design name, when displayed during the delete confirmation dialog and clicked by a user, can trigger a Stored Cross-site Scripting (XSS) vulnerability in the Autodesk Fusion desktop application. A malicious actor may leverage this vulnerability to read local files or execute arbitrary code in the context of the current process.	7.1	More Details
CVE-2026-24404	iccDEV provides libraries and tools for interacting with, manipulating, and applying ICC color management profiles. In versions 2.3.1.1 and below, CIccXmlArrayType() contains a Null Pointer Dereference and Undefined Behavior vulnerability. This occurs when user-controllable input is unsafely incorporated into ICC profile data or other structured binary blobs. Successful exploitation may allow an attacker to perform DoS, manipulate data, bypass application logic and Code Execution. This issue has been fixed in version 2.3.1.2.	7.1	More Details
CVE-2025-67230	Improper permissions in the handler for the Custom URL Scheme in ToDesktop Builder v0.33.0 allows attackers with renderer-context access to invoke external protocol handlers without sufficient validation.	7.1	More Details
CVE-2026-24407	iccDEV provides libraries and tools for interacting with, manipulating, and applying ICC color management profiles. Versions 2.3.1.1 and below have Undefined Behavior in icSigCalcOp(). This occurs when user-controllable input is unsafely incorporated into ICC profile data or other structured binary blobs. Successful exploitation may allow an attacker to perform DoS, manipulate data, bypass application logic and Code Execution. This issue has been fixed in version 2.3.1.2.	7.1	More Details
CVE-2026-0534	A maliciously crafted HTML payload, stored in a part’s attribute and clicked by a user, can trigger a Stored Cross-site Scripting (XSS) vulnerability in the Autodesk Fusion desktop application. A malicious actor may leverage this vulnerability to read local files or execute arbitrary code in the context of the current process.	7.1	More Details

CVE-2026-24409	iccDEV provides libraries and tools for interacting with, manipulating, and applying ICC color management profiles. Versions 2.3.1.1 and below have Undefined Behavior and Null Pointer Deference in CIccTagXmlFloatNum<>::ParseXml(). This occurs when user-controllable input is unsafely incorporated into ICC profile data or other structured binary blobs. Successful exploitation may allow an attacker to perform DoS, manipulate data, bypass application logic and Code Execution. This issue has been fixed in version 2.3.1.2.	7.1	More Details
CVE-2021-47872	SEO Panel versions prior to 4.9.0 contain a blind SQL injection vulnerability in the archive.php page that allows authenticated attackers to manipulate database queries through the 'order_col' parameter. Attackers can use sqlmap to exploit the vulnerability and extract database information by injecting malicious SQL code into the order column parameter.	7.1	More Details
CVE-2025-69318	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hossni Mubarak JobWP jobwp allows Stored XSS.This issue affects JobWP: from n/a through <= 2.4.5.	7.1	More Details
CVE-2026-24779	vLLM is an inference and serving engine for large language models (LLMs). Prior to version 0.14.1, a Server-Side Request Forgery (SSRF) vulnerability exists in the `MediaConnector` class within the vLLM project's multimodal feature set. The load_from_url and load_from_url_async methods obtain and process media from URLs provided by users, using different Python parsing libraries when restricting the target host. These two parsing libraries have different interpretations of backslashes, which allows the host name restriction to be bypassed. This allows an attacker to coerce the vLLM server into making arbitrary requests to internal network resources. This vulnerability is particularly critical in containerized environments like `llm-d`, where a compromised vLLM pod could be used to scan the internal network, interact with other pods, and potentially cause denial of service or access sensitive data. For example, an attacker could make the vLLM pod send malicious requests to an internal `llm-d` management endpoint, leading to system instability by falsely reporting metrics like the KV cache state. Version 0.14.1 contains a patch for the issue.	7.1	More Details
CVE-2026-24410	iccDEV provides libraries and tools for interacting with, manipulating, and applying ICC color management profiles. Versions 2.3.1.1 and below have Undefined Behavior and Null Pointer Deference in CIccProfileXml::ParseBasic(). This occurs when user-controllable input is unsafely incorporated into ICC profile data or other structured binary blobs. Successful exploitation may allow an attacker to perform DoS, manipulate data, bypass application logic and Code Execution. This issue has been fixed in version 2.3.1.2.	7.1	More Details
CVE-2026-23976	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Chill Modula Image Gallery modula-best-grid-gallery allows Stored XSS.This issue affects Modula Image Gallery: from n/a through <= 2.13.4.	7.1	More Details
CVE-2026-24403	iccDEV provides libraries and tools for interacting with, manipulating, and applying ICC color management profiles. In versions 2.3.1.1 and below, an integer overflow vulnerability exists in icValidateStatus CIccProfile::CheckHeader() when user-controllable input is incorporated into profile data unsafely. Tampering with tag tables, offsets, or size fields can trigger parsing errors, memory corruption, or DoS, potentially enabling arbitrary Code Execution or bypassing application logic. This issue has been fixed in version 2.3.1.2.	7.1	More Details
CVE-2026-21417	Dell CloudBoost Virtual Appliance, versions prior to 19.14.0.0, contains a Plaintext Storage of Password vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.0	More Details
CVE-2025-27379	A stored cross-site scripting (XSS) vulnerability in the BOM Viewer in Altium AES 7.0.3 allows an authenticated attacker to inject arbitrary JavaScript into the Description field of a schematic, which is executed when the BOM Viewer renders the affected content.	6.8	More Details
CVE-2026-0810	A flaw was found in gix-date. The `gix_date::parse::TimeBuf::as_str` function can generate strings containing invalid non-UTF8 characters. This issue violates the internal safety invariants of the `TimeBuf` component, leading to undefined behavior when these malformed strings are subsequently processed. This could potentially result in application instability or other unforeseen consequences.	6.8	More Details

CVE-2025-14973	The Recipe Card Blocks Lite WordPress plugin before 3.4.13 does not sanitize and escape a parameter before using it in a SQL statement, allowing contributors and above to perform SQL injection attacks.	6.8	More Details
CVE-2025-71176	pytest through 9.0.2 on UNIX relies on directories with the /tmp/pytest-of-{user} name pattern, which allows local users to cause a denial of service or possibly gain privileges.	6.8	More Details
CVE-2025-67124	A TOCTOU and symlink race in svenstaro/miniserve 0.32.0 upload finalization (when uploads are enabled) can allow an attacker to overwrite arbitrary files outside the intended upload/document root in deployments where the attacker can create/replace filesystem entries in the upload destination directory (e.g., shared writable directory/volume).	6.8	More Details
CVE-2026-23893	openCryptoki is a PKCS#11 library and provides tooling for Linux and AIX. Versions 2.3.2 and above are vulnerable to symlink-following when running in privileged contexts. A token-group user can redirect file operations to arbitrary filesystem targets by planting symlinks in group-writable token directories, resulting in privilege escalation or data exposure. Token and lock directories are 0770 (group-writable for token users), so any token-group member can plant files and symlinks inside them. When run as root, the base code handling token directory file access, as well as several openCryptoki tools used for administrative purposes, may reset ownership or permissions on existing files inside the token directories. An attacker with token-group membership can exploit the system when an administrator runs a PKCS#11 application or administrative tool that performs chown on files inside the token directory during normal maintenance. This issue is fixed in commit 5e6e4b4, but has not been included in a released version at the time of publication.	6.8	More Details
CVE-2026-23946	Tendenci is an open source content management system built for non-profits, associations and cause-based sites. Versions 15.3.11 and below include a critical deserialization vulnerability in the Helpdesk module (which is not enabled by default). This vulnerability allows Remote Code Execution (RCE) by an authenticated user with staff security level due to using Python's pickle module in helpdesk /reports/. The original CVE-2020-14942 was incompletely patched. While ticket_list() was fixed to use safe JSON deserialization, the run_report() function still uses unsafe pickle.loads(). The impact is limited to the permissions of the user running the application, typically www-data, which generally lacks write (except for upload directories) and execute permissions. This issue has been fixed in version 15.3.12.	6.8	More Details
CVE-2025-68609	A vulnerability in Palantir's Aries service allowed unauthenticated access to log viewing and management functionality on Apollo instances using default configuration. The defect resulted in both authentication and authorization checks being bypassed, potentially allowing any network-accessible client to view system logs and perform operations without valid credentials. No evidence of exploitation was identified during the vulnerability window.	6.6	More Details
CVE-2025-70899	PHPgurukul Online Course Registration v3.1 lacks Cross-Site Request Forgery (CSRF) protection on all administrative forms. An attacker can perform unauthorized actions on behalf of authenticated administrators by tricking them into visiting a malicious webpage.	6.5	More Details
CVE-2025-68911	Missing Authorization vulnerability in solacewp Solace solace allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Solace: from n/a through <= 2.1.16.	6.5	More Details
CVE-2026-20883	Gitea's stopwatch API does not re-validate repository access permissions. After a user's access to a private repository is revoked, they may still view issue titles and repository names through previously started stopwatches.	6.5	More Details
CVE-2026-22347	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in subhansanjaya Carousel Horizontal Posts Content Slider carousel-horizontal-posts-content-slider allows DOM-Based XSS.This issue affects Carousel Horizontal Posts Content Slider: from n/a through <= 3.3.2.	6.5	More Details
CVE-	Gitea does not properly validate ownership when toggling OpenID URI visibility. An		More

2026-20904	authenticated user may be able to change the visibility settings of other users' OpenID identities.	6.5	Details
CVE-2025-14559	A flaw was found in the keycloak-services component of Keycloak. This vulnerability allows the issuance of access and refresh tokens for disabled users, leading to unauthorized use of previously revoked privileges, via a business logic vulnerability in the Token Exchange implementation when a privileged client invokes the token exchange flow.	6.5	More Details
CVE-2025-57785	A Double Free in XSLT `show_index` has been identified in Hiawatha webserver version 11.7 which allows an unauthenticated attacker to corrupt data which may lead to arbitrary code execution.	6.5	More Details
CVE-2026-24354	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Shortcodes & Performance penci-shortcodes allows DOM-Based XSS.This issue affects Penci Shortcodes & Performance: from n/a through <= 6.1.	6.5	More Details
CVE-2025-69315	Missing Authorization vulnerability in NSquared Simply Schedule Appointments simply-schedule-appointments allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Simply Schedule Appointments: from n/a through <= 1.6.9.15.	6.5	More Details
CVE-2026-22463	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Micro.company Form to Chat App form-to-chat allows Stored XSS.This issue affects Form to Chat App: from n/a through <= 1.2.5.	6.5	More Details
CVE-2020-36950	Laravel Nova 3.7.0 contains a denial of service vulnerability that allows authenticated users to crash the application by manipulating the 'range' parameter. Attackers can send simultaneous requests with an extremely high range value to overwhelm and crash the server.	6.5	More Details
CVE-2026-24361	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThimPress LearnPress &#8211; Course Review learnpress-course-review allows Stored XSS.This issue affects LearnPress &#8211; Course Review: from n/a through <= 4.1.9.	6.5	More Details
CVE-2026-23952	ImageMagick is free and open-source software used for editing and manipulating digital images. Versions 14.10.1 and below have a NULL pointer dereference vulnerability in the MSL (Magick Scripting Language) parser when processing <comment> tags before images are loaded. This can lead to DoS attack due to assertion failure (debug builds) or NULL pointer dereference (release builds). This issue is fixed in version 14.10.2.	6.5	More Details
CVE-2025-14911	User-controlled chunkSize metadata from MongoDB lacks appropriate validation allowing malformed GridFS metadata to overflow the bounding container.	6.5	More Details
CVE-2025-68135	EVerest is an EV charging software stack. Prior to version 2025.10.0, C++ exceptions are not properly handled for and by the `TbdController` loop, leading to its caller and itself to silently terminates. Thus, this leads to a denial of service as it is responsible of SDP and ISO15118-20 servers. Version 2025.10.0 fixes the issue.	6.5	More Details
CVE-2025-69095	Missing Authorization vulnerability in designthemes Reservation Plugin dt-reservation-plugin allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Reservation Plugin: from n/a through <= 1.7.	6.5	More Details
CVE-2026-23964	Mastodon is a free, open-source social network server based on ActivityPub. Prior to versions 4.5.5, 4.4.12, and 4.3.18, an insecure direct object reference in the web push subscription update endpoint lets any authenticated user update another user's push subscription by guessing or obtaining the numeric subscription id. This can be used to disrupt push notifications for other users and also leaks the web push subscription endpoint. Any user with a web push subscription is impacted, because another authenticated user can tamper with their push subscription settings if they can guess or obtain the subscription id. This allows an attacker to disrupt push notifications by changing the policy (whether to filter notifications from non-followers or non-followed users) and subscribed notification types of their victims. Additionally, the endpoint returns the subscription object, which includes the push notification endpoint for this subscription, but	6.5	More Details

	not its keypair. Mastodon versions v4.5.5, v4.4.12, v4.3.18 are patched.		
CVE-2026-1504	Inappropriate implementation in Background Fetch API in Google Chrome prior to 144.0.7559.110 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-23890	pnpm is a package manager. Prior to version 10.28.1, a path traversal vulnerability in pnpm's bin linking allows malicious npm packages to create executable shims or symlinks outside of `node_modules/.bin`. Bin names starting with `@` bypass validation, and after scope normalization, path traversal sequences like `../../` remain intact. This issue affects all pnpm users who install npm packages and CI/CD pipelines using pnpm. It can lead to overwriting config files, scripts, or other sensitive files. Version 10.28.1 contains a patch.	6.5	More Details
CVE-2026-23889	pnpm is a package manager. Prior to version 10.28.1, a path traversal vulnerability in pnpm's tarball extraction allows malicious packages to write files outside the package directory on Windows. The path normalization only checks for `./` but not `.\`. On Windows, backslashes are directory separators, enabling path traversal. This vulnerability is Windows-only. This issue impacts Windows pnpm users and Windows CI/CD pipelines (GitHub Actions Windows runners, Azure DevOps). It can lead to overwriting `.npmrc`, build configs, or other files. Version 10.28.1 contains a patch.	6.5	More Details
CVE-2026-23888	pnpm is a package manager. Prior to version 10.28.1, a path traversal vulnerability in pnpm's binary fetcher allows malicious packages to write files outside the intended extraction directory. The vulnerability has two attack vectors: (1) Malicious ZIP entries containing `../` or absolute paths that escape the extraction root via AdmZip's `extractAllTo`, and (2) The `BinaryResolution.prefix` field is concatenated into the extraction path without validation, allowing a crafted prefix like `../../evil` to redirect extracted files outside `targetDir`. The issue impacts all pnpm users who install packages with binary assets, users who configure custom Node.js binary locations and CI/CD pipelines that auto-install binary dependencies. It can lead to overwriting config files, scripts, or other sensitive files leading to RCE. Version 10.28.1 contains a patch.	6.5	More Details
CVE-2026-24383	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins B Slider b-slider allows DOM-Based XSS.This issue affects B Slider: from n/a through <= 2.0.6.	6.5	More Details
CVE-2026-24829	Out-of-bounds Write, Heap-based Buffer Overflow vulnerability in Is-Daouda is-Engine.This issue affects is-Engine: before 3.3.4.	6.5	More Details
CVE-2026-20800	Gitea's notification API does not re-validate repository access permissions when returning notification details. After a user's access to a private repository is revoked, they may still view issue and pull request titles through previously received notifications.	6.5	More Details
CVE-2026-24389	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Chill Gallery PhotoBlocks photoblocks-grid-gallery allows DOM-Based XSS.This issue affects Gallery PhotoBlocks: from n/a through <= 1.3.2.	6.5	More Details
CVE-2025-68896	Missing Authorization vulnerability in vrpr WDV One Page Docs wdv-one-page-docs allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WDV One Page Docs: from n/a through <= 1.2.4.	6.5	More Details
CVE-2026-24585	Missing Authorization vulnerability in Hyyan Abo Fakher Hyyan WooCommerce Polylang Integration woo-poly-integration allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Hyyan WooCommerce Polylang Integration: from n/a through <= 1.5.0.	6.5	More Details
CVE-2026-24623	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in saeros1984 Neoforum neoforum allows Reflected XSS.This issue affects Neoforum: from n/a through <= 1.0.	6.5	More Details
CVE-2026-	Dell ECS, versions 3.8.1.0 through 3.8.1.7, and Dell ObjectScale versions prior to 4.2.0.0, contains a Cleartext Transmission of Sensitive Information vulnerability in the Fabric Syslog. An unauthenticated attacker with remote access could potentially exploit this	6.5	More Details

22274	vulnerability to intercept and modify information in transit.		
CVE-2026-24526	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Steve Truman Email Inquiry &amp; Cart Options for WooCommerce woocommerce-email-inquiry-cart-options allows DOM-Based XSS.This issue affects Email Inquiry &amp; Cart Options for WooCommerce: from n/a through <= 3.4.3.	6.5	More Details
CVE-2026-24528	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pixelgrade Nova Blocks nova-blocks allows DOM-Based XSS.This issue affects Nova Blocks: from n/a through <= 2.1.9.	6.5	More Details
CVE-2025-13335	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.1 before 18.6.4, 18.7 before 18.7.2, and 18.8 before 18.8.2 that under certain circumstances could have allowed an authenticated user to create a denial of service condition by configuring malformed Wiki documents that bypass cycle detection.	6.5	More Details
CVE-2025-68073	Missing Authorization vulnerability in Ninja Team GDPR CCPA Compliance Support ninja-gdpr-compliance allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects GDPR CCPA Compliance Support: from n/a through <= 2.7.4.	6.5	More Details
CVE-2026-24420	phpMyFAQ is an open source FAQ web application. Versions 4.0.16 and below allow an authenticated user without the dlattachment permission to download FAQ attachments due to a incomprehensive permissions check. The presence of a right key is improperly validated as proof of authorization in attachment.php. Additionally, the group and user permission logic contains a flawed conditional expression that may allow unauthorized access. This issue has been fixed in version	6.5	More Details
CVE-2026-24421	phpMyFAQ is an open source FAQ web application. Versions 4.0.16 and below have flawed authorization logic which exposes the /api/setup/backup endpoint to any authenticated user despite their permissions. SetupController.php uses userIsAuthenticated() but does not verify that the requester has configuration/admin permissions. Non-admin users can trigger a configuration backup and retrieve its path. The endpoint only checks authentication, not authorization, and returns a link to the generated ZIP. This issue is fixed in version 4.0.17.	6.5	More Details
CVE-2026-24565	Insertion of Sensitive Information Into Sent Data vulnerability in bPlugins B Accordion b-accordion allows Retrieve Embedded Sensitive Data.This issue affects B Accordion: from n/a through <= 2.0.0.	6.5	More Details
CVE-2026-24566	Missing Authorization vulnerability in iNET iNET Webkit inet-webkit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects iNET Webkit: from n/a through <= 1.2.4.	6.5	More Details
CVE-2026-24617	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Daniel Iser Easy Modal easy-modal allows Stored XSS.This issue affects Easy Modal: from n/a through <= 2.1.0.	6.5	More Details
CVE-2026-24616	Missing Authorization vulnerability in Damian WP Popups wp-popups-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Popups: from n/a through <= 2.2.0.3.	6.5	More Details
CVE-2025-68558	Missing Authorization vulnerability in averta Depicter Slider depicter allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Depicter Slider: from n/a through <= 4.0.4.	6.5	More Details
CVE-2025-32057	The Infotainment ECU manufactured by Bosch which is installed in Nissan Leaf ZE1 – 2020 uses a Redbend service for over-the-air provisioning and updates. HTTPS is used for communication with the back-end server. Due to usage of the default configuration for the underlying SSL engine, the server root certificate is not verified. As a result, an attacker may be able to impersonate a Redbend backend server using a self-signed certificate. First identified on Nissan Leaf ZE1 manufactured in 2020.	6.5	More Details
	The All-in-One Video Gallery plugin for WordPress is vulnerable to unauthorized		

CVE-2025-14947	modification of data due to a missing capability check on the `ajax_callback_create_bunny_stream_video`, `ajax_callback_get_bunny_stream_video`, and `ajax_callback_delete_bunny_stream_video` functions in all versions up to, and including, 4.6.4. This makes it possible for unauthenticated attackers to create and delete videos on the Bunny Stream CDN associated with the victim's account, provided they can obtain a valid nonce which is exposed in public player templates.	6.5	More Details
CVE-2025-68900	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kriesi Enfold enfold allows DOM-Based XSS.This issue affects Enfold: from n/a through <= 7.1.3.	6.5	More Details
CVE-2026-24630	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Design Stylish Cost Calculator stylish-cost-calculator allows Stored XSS.This issue affects Stylish Cost Calculator: from n/a through <= 8.1.8.	6.5	More Details
CVE-2025-69612	A path traversal vulnerability exists in TMS Management Console (version 6.3.7.27386.20250818) from TMS Global Software. The "Download Template" function in the profile dashboard does not neutralize directory traversal sequences (../) in the filePath parameter, allowing authenticated users to read arbitrary files, such as the server's Web.config.	6.5	More Details
CVE-2026-22353	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in winkm89 teachPress teachpress allows Stored XSS.This issue affects teachPress: from n/a through <= 9.0.12.	6.5	More Details
CVE-2026-24401	Avahi is a system which facilitates service discovery on a local network via the mDNS/DNS-SD protocol suite. In versions 0.9rc2 and below, avahi-daemon can be crashed via a segmentation fault by sending an unsolicited mDNS response containing a recursive CNAME record, where the alias and canonical name point to the same domain (e.g., "h.local" as a CNAME for "h.local"). This causes unbounded recursion in the lookup_handle_cname function, leading to stack exhaustion. The vulnerability affects record browsers where AVAHI_LOOKUP_USE_MULTICAST is set explicitly, which includes record browsers created by resolvers used by nss-mdns. This issue is patched in commit 78eab31128479f06e30beb8c1cbf99dd921e2524.	6.5	More Details
CVE-2020-36978	Froxlor Server Management Panel 0.10.16 contains a persistent cross-site scripting vulnerability in customer registration input fields. Attackers can inject malicious scripts through username, name, and firstname parameters to execute code when administrators view customer traffic modules.	6.4	More Details
CVE-2025-12836	The VK Google Job Posting Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Job Description field in versions up to, and including, 1.2.20 due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers with author-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14941	The GZSEO plugin for WordPress is vulnerable to authorization bypass leading to Stored Cross-Site Scripting in all versions up to, and including, 2.0.11. This is due to missing capability checks on multiple AJAX handlers combined with insufficient input sanitization and output escaping on the embed_code parameter. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary content into any post on the site that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2021-47906	BloofoxCMS 0.5.2.1 contains a stored cross-site scripting vulnerability in the articles text parameter that allows authenticated attackers to inject malicious scripts. Attackers can insert malicious javascript payloads in the text field to execute scripts and potentially steal authenticated users' cookies.	6.4	More Details
CVE-2026-0746	The AI Engine plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 3.3.2 via the 'get_audio' function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services, if "Public API" is enabled in the plugin settings,	6.4	More Details

	and 'allow_url_fopen' is set to 'On' on the server.		
CVE-2020-36960	Forma LMS 2.3 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious scripts into user profile first and last name fields. Attackers can craft scripts like '<script>alert(document.cookie)</script>' to execute arbitrary JavaScript when the profile is viewed by other users.	6.4	More Details
CVE-2025-14985	The Alpha Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘alpha_block_css’ parameter in all versions up to, and including, 1.5.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1097	The ThemeRuby Multi Authors – Assign Multiple Writers to Posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'before' and 'after' shortcode attributes in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1095	The Canto Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'fx' shortcode attribute in all versions up to, and including, 1.0 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-2020-36956	Openfire 4.6.0 contains a stored cross-site scripting vulnerability in the nodejs plugin that allows attackers to inject malicious scripts through the 'path' parameter. Attackers can craft a payload with script tags to execute arbitrary JavaScript in the context of administrative users viewing the nodejs configuration page.	6.4	More Details
CVE-2026-0914	The WP DSGVO Tools (GDPR) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'lw_content_block' shortcode in all versions up to, and including, 3.1.36 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-2020-36954	Xeroneit Library Management System 3.1 contains a stored cross-site scripting vulnerability in the Book Category feature that allows administrators to inject malicious scripts. Attackers can insert a payload in the Category Name field to execute arbitrary JavaScript code when the page is loaded.	6.4	More Details
CVE-2020-36932	SeaCMS 11.1 contains a stored cross-site scripting vulnerability in the checkuser parameter of the admin settings page. Attackers can inject malicious JavaScript payloads that will execute in users' browsers when the page is loaded.	6.4	More Details
CVE-2020-36931	Click2Magic 1.1.5 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious scripts in the chat name input. Attackers can craft a malicious payload in the chat name to capture administrator cookies when the admin processes user requests.	6.4	More Details
CVE-2025-15522	The Uncanny Automator – Easy Automation, Integration, Webhooks & Workflow Builder Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the automator_discord_user_mapping shortcode in all versions up to, and including, 6.10.0.2 due to insufficient input sanitization and output escaping on the verified_message parameter. 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 with a verified Discord account accesses the injected page.	6.4	More Details
CVE-2026-1099	The Administrative Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'login' and 'logout' shortcode attributes in all versions up to, and including, 0.3.4 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	6.4	More Details

	scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2026-1410	A vulnerability was detected in Beetel 777VR1 up to 01.00.09/01.00.09_55. Impacted is an unknown function of the component UART Interface. The manipulation results in missing authentication. An attack on the physical device is feasible. This attack is characterized by high complexity. The exploitability is considered difficult. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.4	More Details
CVE-2025-14525	A flaw was found in kubevirt. A user within a virtual machine (VM), if the guest agent is active, can exploit this by causing the agent to report an excessive number of network interfaces. This action can overwhelm the system's ability to store VM configuration updates, effectively blocking changes to the Virtual Machine Instance (VMI). This allows the VM user to restrict the VM administrator's ability to manage the VM, leading to a denial of service for administrative operations.	6.4	More Details
CVE-2026-1189	The LeadBI Plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'form_id' parameter of the 'leadbi_form' shortcode in all versions up to, and including, 1.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14069	The Schema & Structured Data for WP & AMP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'saswp_custom_schema_field' profile field in all versions up to, and including, 1.54 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-2025-14745	The RSS Aggregator – RSS Import, News Feeds, Feed to Post, and Autoblogging plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wp-rss-aggregator' shortcode in all versions up to, and including, 5.0.10 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2020-36955	Grav CMS 1.6.30 with Admin Plugin 1.9.18 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through the page title field. Attackers can create a new page with a malicious script in the title, which will be executed when the page is viewed in the admin panel or on the site.	6.4	More Details
CVE-2026-1098	The CM CSS Columns plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tag' shortcode attribute in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-24047	Backstage is an open framework for building developer portals, and @backstage/cli-common provides config loading functionality used by the backend and command line interface of Backstage. Prior to version 0.1.17, the `resolveSafeChildPath` utility function in `@backstage/backend-plugin-api`, which is used to prevent path traversal attacks, failed to properly validate symlink chains and dangling symlinks. An attacker could bypass the path validation via symlink chains (creating `link1 → link2 → /outside` where intermediate symlinks eventually resolve outside the allowed directory) and dangling symlinks (creating symlinks pointing to non-existent paths outside the base directory, which would later be created during file operations). This function is used by Scaffolder actions and other backend components to ensure file operations stay within designated directories. This vulnerability is fixed in `@backstage/backend-plugin-api` version 0.1.17. Users should upgrade to this version or later. Some workarounds are available. Run Backstage in a containerized environment with limited filesystem access and/or restrict template creation to trusted users.	6.3	More Details
	A security vulnerability has been detected in Totolink NR1800X 9.1.0u.6279_B20210910.		

CVE-2026-1327	This issue affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. Such manipulation of the argument command 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-2026-1326	A weakness has been identified in Totolink NR1800X 9.1.0u.6279_B20210910. This vulnerability affects the function setWanCfg of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. This manipulation of the argument Hostname 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-2026-1414	A vulnerability was determined in Sangfor Operation and Maintenance Security Management System up to 3.0.12. This impacts the function getInformation of the file /equipment/get_Information of the component HTTP POST Request Handler. Executing a manipulation of the argument fortEquipmentIp can lead to command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-1413	A vulnerability was found in Sangfor Operation and Maintenance Security Management System up to 3.0.12. This affects the function portValidate of the file /fort/ip_and_port/port_validate of the component HTTP POST Request Handler. Performing a manipulation of the argument port results in command injection. The attack can be initiated remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-1423	A vulnerability was determined in code-projects Online Examination System 1.0. Affected by this issue is some unknown functionality of the file /admin_pic.php. Executing a manipulation can lead to unrestricted upload. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2021-47849	Mini Mouse 9.3.0 contains a path traversal vulnerability that allows attackers to access sensitive system directories through the device information endpoint. Attackers can retrieve file lists from system directories like /usr, /etc, and /var by manipulating file path parameters in API requests.	6.2	More Details
CVE-2026-1411	A flaw has been found in Beetel 777VR1 up to 01.00.09/01.00.09_55. The affected element is an unknown function of the component UART Interface. This manipulation causes improper access controls. It is feasible to perform the attack on the physical device. The complexity of an attack is rather high. The exploitability is described as difficult. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.1	More Details
CVE-2025-48094	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Magic Slider magic_slider allows Reflected XSS.This issue affects Magic Slider: from n/a through <= 2.2.	6.1	More Details
CVE-2021-47905	MyBB Delete Account Plugin 1.4 contains a cross-site scripting vulnerability in the account deletion reason input field. Attackers can inject malicious scripts that will execute in the admin interface when viewing delete account reasons.	6.1	More Details
CVE-2025-11687	A flaw was found in the gi-docgen. This vulnerability allows arbitrary JavaScript execution in the context of the page — enabling DOM access, session cookie theft and other client-side attacks — via a crafted URL that supplies a malicious value to the q GET parameter (reflected DOM XSS).	6.1	More Details
CVE-2025-47600	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in xtemos WoodMart woodmart allows Code Injection.This issue affects WoodMart: from n/a through <= 8.3.7.	6.1	More Details
CVE-2026-1127	The Timeline Event History plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `id` parameter in all versions up to, and including, 3.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE-2025-47666	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Image&Video FullScreen Background lbg_fullscreen_fullwidth_slider allows Reflected XSS.This issue affects Image&Video FullScreen Background: from n/a through <= 1.6.7.	6.1	More Details
CVE-2025-69316	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 TableOn posts-table-filterable allows Reflected XSS.This issue affects TableOn: from n/a through <= 1.0.4.2.	6.1	More Details
CVE-2025-69317	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in scriptsbundle CarSpot carspot allows Reflected XSS.This issue affects CarSpot: from n/a through < 2.4.6.	6.1	More Details
CVE-2025-49043	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Magic Responsive Slider and Carousel WordPress magic_carousel allows Reflected XSS.This issue affects Magic Responsive Slider and Carousel WordPress: from n/a through <= 1.6.	6.1	More Details
CVE-2025-27005	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup HTML5 Video Player lbg-vp2-html5-bottom allows Reflected XSS.This issue affects HTML5 Video Player: from n/a through <= 5.3.5.	6.1	More Details
CVE-2025-49045	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in highwarden Super Interactive Maps super-interactive-maps allows Reflected XSS.This issue affects Super Interactive Maps: from n/a through <= 2.3.	6.1	More Details
CVE-2025-49046	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup xPromoter top_bar_promoter allows Reflected XSS.This issue affects xPromoter: from n/a through <= 1.3.4.	6.1	More Details
CVE-2025-49066	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Accordion Slider PRO accordion_slider_pro allows Reflected XSS.This issue affects Accordion Slider PRO: from n/a through <= 1.2.	6.1	More Details
CVE-2025-49249	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ApusTheme Drone drone allows Reflected XSS.This issue affects Drone: from n/a through <= 1.40.	6.1	More Details
CVE-2025-50005	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Composer td-composer allows DOM-Based XSS.This issue affects tagDiv Composer: from n/a through <= 5.4.2.	6.1	More Details
CVE-2025-50006	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jthemes xSmart xsmart allows Reflected XSS.This issue affects xSmart: from n/a through <= 1.2.9.4.	6.1	More Details
CVE-2025-52746	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ayecode Restaurante restaurante allows Reflected XSS.This issue affects Restaurante: from n/a through <= 3.0.7.	6.1	More Details
CVE-2025-32123	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup HTML5 Video Player with Playlist & Multiple Skins lbg-vp2-html5-rightside allows Reflected XSS.This issue affects HTML5 Video Player with Playlist & Multiple Skins: from n/a through <= 5.3.5.	6.1	More Details
CVE-2026-1467	A flaw was found in libsoup, an HTTP client library. This vulnerability, known as CRLF (Carriage Return Line Feed) Injection, occurs when an HTTP proxy is configured and the library improperly handles URL-decoded input used to create the Host header. A remote attacker can exploit this by providing a specially crafted URL containing CRLF sequences, allowing them to inject additional HTTP headers or complete HTTP request bodies. This can lead to unintended or unauthorized HTTP requests being forwarded by the proxy, potentially impacting downstream services.	6.1	More Details
CVE-	An attacker could decrypt sensitive data, impersonate legitimate users or devices, and		More

2025-25051	potentially gain access to network resources for lateral attacks.	6.1	Details
CVE-2026-0862	The Save as PDF Plugin by PDFCrowd plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘options’ parameter in all versions up to, and including, 4.5.5 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. NOTE: Successful exploitation of this vulnerability requires that the PDFCrowd API key is blank (also known as "demo mode", which is the default configuration when the plugin is installed) or known.	6.1	More Details
CVE-2025-69098	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpWave Hide My WP hide_my_wp allows Reflected XSS.This issue affects Hide My WP: from n/a through <= 6.2.12.	6.1	More Details
CVE-2026-24555	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in artplacer ArtPlacer Widget artplacer-widget allows Stored XSS.This issue affects ArtPlacer Widget: from n/a through <= 2.23.1.	6.1	More Details
CVE-2018-25116	MyBB Thread Redirect Plugin 0.2.1 contains a cross-site scripting vulnerability in the custom text input field for thread redirects. Attackers can inject malicious SVG scripts that will execute when other users view the thread, allowing arbitrary script execution.	6.1	More Details
CVE-2025-67652	An attacker with access to the project file could use the exposed credentials to impersonate users, escalate privileges, or gain unauthorized access to systems and services. The absence of robust encryption or secure handling mechanisms increases the likelihood of this type of exploitation, leaving sensitive information more vulnerable.	6.1	More Details
CVE-2018-25132	MyBB Trending Widget Plugin 1.2 contains a cross-site scripting vulnerability that allows attackers to inject malicious scripts through thread titles. Attackers can modify thread titles with script payloads that will execute when other users view the trending widget.	6.1	More Details
CVE-2025-53240	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in adamlabs WordPress Photo Gallery photo-gallery-portfolio allows Reflected XSS.This issue affects WordPress Photo Gallery: from n/a through <= 1.1.0.	6.1	More Details
CVE-2025-13676	The JustClick registration plugin for WordPress is vulnerable to Reflected Cross-Site Scripting in all versions up to, and including, 0.1. This is due to insufficient input sanitization and output escaping on the `PHP_SELF` server 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.	6.1	More Details
CVE-2025-52762	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in flexostudio flexo-posts-manager flexo-posts-manager allows Reflected XSS.This issue affects flexo-posts-manager: from n/a through <= 1.0001.	6.1	More Details
CVE-2026-1386	A UNIX symbolic link following issue in the jailer component in Firecracker version v1.13.1 and earlier and 1.14.0 on Linux may allow a local host user with write access to the pre-created jailer directories to overwrite arbitrary host files via a symlink attack during the initialization copy at jailer startup, if the jailer is executed with root privileges. To mitigate this issue, users should upgrade to version v1.13.2 or 1.14.1 or above.	6.0	More Details
CVE-2025-69820	Directory Traversal vulnerability in Beam beta9 v.0.1.552 allows a remote attacker to obtain sensitive information via the joinCleanPath function	6.0	More Details
CVE-2026-20092	A vulnerability in the read-only maintenance shell of Cisco Intersight Virtual Appliance could allow an authenticated, local attacker with administrative privileges to elevate privileges to root on the virtual appliance. This vulnerability is due to improper file permissions on configuration files for system accounts within the maintenance shell of the virtual appliance. An attacker could exploit this vulnerability by accessing the maintenance shell as a read-only administrator and manipulating system files to grant root privileges. A successful exploit could allow the attacker to elevate their privileges to&nbsp;root on the	6.0	More Details

	virtual appliance and gain full control of the appliance, giving them the ability to access sensitive information, modify workloads and configurations on the host system, and cause a denial of service (DoS).		
CVE-2026-22388	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Imran Emu Owl Carousel WP owl-carousel-wp allows Stored XSS.This issue affects Owl Carousel WP: from n/a through <= 2.2.2.	5.9	More Details
CVE-2026-24614	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Devsbrain Flex QR Code Generator flex-qr-code-generator allows DOM-Based XSS.This issue affects Flex QR Code Generator: from n/a through <= 1.2.8.	5.9	More Details
CVE-2026-24909	vlt before 1.0.0-rc.10 mishandles path sanitization for tar, leading to path traversal during extraction.	5.9	More Details
CVE-2026-24626	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LogicHunt Logo Slider logo-slider-wp allows Stored XSS.This issue affects Logo Slider: from n/a through <= 4.9.0.	5.9	More Details
CVE-2026-24629	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ability, Inc Web Accessibility with Max Access accessibility-toolbar allows Stored XSS.This issue affects Web Accessibility with Max Access: from n/a through <= 2.1.0.	5.9	More Details
CVE-2025-67231	A reflected cross-site scripting (XSS) vulnerability in ToDesktop Builder v0.33.1 allows attackers to execute arbitrary code in the context of a user's browser via a crafted payload.	5.9	More Details
CVE-2026-24584	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeum Tutor LMS BunnyNet Integration tutor-lms-bunnynet-integration allows DOM-Based XSS.This issue affects Tutor LMS BunnyNet Integration: from n/a through <= 1.0.0.	5.9	More Details
CVE-2026-22262	Suricata is a network IDS, IPS and NSM engine. While saving a dataset a stack buffer is used to prepare the data. Prior to versions 8.0.3 and 7.0.14, if the data in the dataset is too large, this can result in a stack overflow. Versions 8.0.3 and 7.0.14 contain a patch. As a workaround, do not use rules with datasets `save` nor `state` options.	5.9	More Details
CVE-2026-24632	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jagdish1o1 Delay Redirects delay-redirects allows DOM-Based XSS.This issue affects Delay Redirects: from n/a through <= 1.0.0.	5.9	More Details
CVE-2025-59471	A denial of service vulnerability exists in self-hosted Next.js applications that have `remotePatterns` configured for the Image Optimizer. The image optimization endpoint (`/_next/image`) loads external images entirely into memory without enforcing a maximum size limit, allowing an attacker to cause out-of-memory conditions by requesting optimization of arbitrarily large images. This vulnerability requires that `remotePatterns` is configured to allow image optimization from external domains and that the attacker can serve or control a large image on an allowed domain. Strongly consider upgrading to 15.5.10 or 16.1.5 to reduce risk and prevent availability issues in Next applications.	5.9	More Details
CVE-2025-59472	A denial of service vulnerability exists in Next.js versions with Partial Prerendering (PPR) enabled when running in minimal mode. The PPR resume endpoint accepts unauthenticated POST requests with the `Next-Resume: 1` header and processes attacker-controlled postponed state data. Two closely related vulnerabilities allow an attacker to crash the server process through memory exhaustion: 1. **Unbounded request body buffering**: The server buffers the entire POST request body into memory using `Buffer.concat()` without enforcing any size limit, allowing arbitrarily large payloads to exhaust available memory. 2. **Unbounded decompression (zipbomb)**: The resume data cache is decompressed using `inflateSync()` without limiting the decompressed output size. A small compressed payload can expand to hundreds of megabytes or gigabytes, causing memory exhaustion. Both attack vectors result in a fatal V8 out-of-memory error (`FATAL ERROR: Reached heap limit Allocation failed - JavaScript heap out of memory`)	5.9	More Details

	causing the Node.js process to terminate. The zipbomb variant is particularly dangerous as it can bypass reverse proxy request size limits while still causing large memory allocation on the server. To be affected you must have an application running with `experimental.ppr: true` or `cacheComponents: true` configured along with the NEXT_PRIVATE_MINIMAL_MODE=1 environment variable. Strongly consider upgrading to 15.6.0-canary.61 or 16.1.5 to reduce risk and prevent availability issues in Next applications.		
CVE-2026-24620	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PluginOps Landing Page Builder page-builder-add allows Stored XSS.This issue affects Landing Page Builder: from n/a through <= 1.5.3.3.	5.9	More Details
CVE-2026-24910	In Bun before 1.3.5, the default trusted dependencies list (aka trust allow list) can be spoofed by a non-npm package in the case of a matching name (for file, link, git, or github).	5.9	More Details
CVE-2026-23992	go-tuf is a Go implementation of The Update Framework (TUF). Starting in version 2.0.0 and prior to version 2.3.1, a compromised or misconfigured TUF repository can have the configured value of signature thresholds set to 0, which effectively disables signature verification. This can lead to unauthorized modification to TUF metadata files is possible at rest, or during transit as no integrity checks are made. Version 2.3.1 fixes the issue. As a workaround, always make sure that the TUF metadata roles are configured with a threshold of at least 1.	5.9	More Details
CVE-2026-23991	go-tuf is a Go implementation of The Update Framework (TUF). Starting in version 2.0.0 and prior to version 2.3.1, if the TUF repository (or any of its mirrors) returns invalid TUF metadata JSON (valid JSON but not well formed TUF metadata), the client will panic during parsing, causing a denial of service. The panic happens before any signature is validated. This means that a compromised repository/mirror/cache can DoS clients without having access to any signing key. Version 2.3.1 fixes the issue. No known workarounds are available.	5.9	More Details
CVE-2025-62077	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SEOSEON EUROPE S.L Affiliate Link Tracker affiliate-link-tracker allows Stored XSS.This issue affects Affiliate Link Tracker: from n/a through <= 0.2.	5.9	More Details
CVE-2025-68898	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cjjparadoxmax Synergy Project Manager synergy-project-manager allows Stored XSS.This issue affects Synergy Project Manager: from n/a through <= 1.5.	5.8	More Details
CVE-2026-24137	sigstore framework is a common go library shared across sigstore services and clients. In versions 1.10.3 and below, the legacy TUF client (pkg/tuf/client.go) supports caching target files to disk. It constructs a filesystem path by joining a cache base directory with a target name sourced from signed target metadata; however, it does not validate that the resulting path stays within the cache base directory. A malicious TUF repository can trigger arbitrary file overwriting, limited to the permissions that the calling process has. Note that this should only affect clients that are directly using the TUF client in sigstore/sigstore or are using an older version of Cosign. Public Sigstore deployment users are unaffected, as TUF metadata is validated by a quorum of trusted collaborators. This issue has been fixed in version 1.10.4. As a workaround, users can disable disk caching for the legacy client by setting SIGSTORE_NO_CACHE=true in the environment, migrate to https://github.com/sigstore/sigstore-go/tree/main/pkg/tuf, or upgrade to the latest sigstore/sigstore release.	5.8	More Details
CVE-2026-1425	A security flaw has been discovered in pymumu SmartDNS up to 47.1. This vulnerability affects the function _dns_decode_rr_head/_dns_decode_SVCB_HTTPS of the file src/dns.c of the component SVBC Record Parser. The manipulation results in stack-based buffer overflow. It is possible to launch the attack remotely. A high complexity level is associated with this attack. It is stated that the exploitability is difficult. The patch is identified as 2d57c4b4e1add9b4537aeb403f794a084727e1c8. Applying a patch is advised to resolve this issue.	5.6	More Details

CVE-2026-22276	Dell ECS, versions 3.8.1.0 through 3.8.1.7, and Dell ObjectScale versions prior to 4.2.0.0, contains a Cleartext Storage of Sensitive Information vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	5.5	More Details
CVE-2025-4763	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Aida Computer Information Technology Inc. Hotel Guest Hotspot allows Reflected XSS.This issue affects Hotel Guest Hotspot: through 22012026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2026-23951	SumatraPDF is a multi-format reader for Windows. All versions contain an off-by-one error in the validation code that only triggers with exactly 2 records, causing an integer underflow in the size calculation. This bug exists in PalmDbReader::GetRecord when opening a crafted Mobi file, resulting in an out-of-bounds heap read that crashes the app. There are no published fixes at the time of publication.	5.5	More Details
CVE-2025-65264	The kernel driver of CPUID CPU-Z v2.17 and earlier does not validate user-supplied values passed via its IOCTL interface, allowing an attacker to access sensitive information via a crafted request.	5.5	More Details
CVE-2025-50537	Stack overflow vulnerability in eslint before 9.26.0 when serializing objects with circular references in eslint/lib/shared/serialization.js. The exploit is triggered via the RuleTester.run() method, which validates test cases and checks for duplicates. During validation, the internal function checkDuplicateTestCase() is called, which in turn uses the isSerializable() function for serialization checks. When a circular reference object is passed in, isSerializable() enters infinite recursion, ultimately causing a stack overflow.	5.5	More Details
CVE-2026-24576	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in COP UX Flat ux-flat allows Stored XSS.This issue affects UX Flat: from n/a through <= 5.4.0.	5.4	More Details
CVE-2025-49336	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pondol Pondol BBS pondol-bbs allows Stored XSS.This issue affects Pondol BBS: from n/a through <= 1.1.8.4.	5.4	More Details
CVE-2026-24540	Missing Authorization vulnerability in Prince Integrate Google Drive integrate-google-drive allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Integrate Google Drive: from n/a through <= 1.5.5.	5.4	More Details
CVE-2026-1103	The AIKTP plugin for WordPress is vulnerable to unauthorized modification of data due to missing authorization checks on the /aiktp/getToken REST API endpoint in all versions up to, and including, 5.0.04. The endpoint uses the 'verify_user_logged_in' as a permission callback, which only checks if a user is logged in, but fails to verify if the user has administrative capabilities. This makes it possible for authenticated attackers with Subscriber-level access and above to retrieve the administrator's 'aiktpz_token' access token, which can then be used to create posts, upload media library files, and access private content as the administrator.	5.4	More Details
CVE-2026-24365	Cross-Site Request Forgery (CSRF) vulnerability in storeapps Stock Manager for WooCommerce woocommerce-stock-manager allows Cross Site Request Forgery.This issue affects Stock Manager for WooCommerce: from n/a through < 3.6.0.	5.4	More Details
CVE-2026-24550	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kaira Blockons blockons allows Stored XSS.This issue affects Blockons: from n/a through <= 1.2.15.	5.4	More Details
CVE-2025-14797	The Same Category Posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the widget title placeholder functionality in all versions up to, and including, 1.1.19. This is due to the use of `htmlspecialchars_decode()` on taxonomy term names before output, which decodes HTML entities that WordPress intentionally encodes for safety. 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.	5.4	More Details
CVE-	Missing Authorization vulnerability in monetagwp Monetag Official Plugin monetag-official		

2026-24551	allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Monetag Official Plugin: from n/a through <= 1.1.3.	5.4	More Details
CVE-2026-24374	Cross-Site Request Forgery (CSRF) vulnerability in Metagauss RegistrationMagic custom-registration-form-builder-with-submission-manager allows Cross Site Request Forgery.This issue affects RegistrationMagic: from n/a through <= 6.0.6.9.	5.4	More Details
CVE-2026-24558	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in antoniobg ABG Rich Pins abg-rich-pins allows Stored XSS.This issue affects ABG Rich Pins: from n/a through <= 1.1.	5.4	More Details
CVE-2026-24381	Server-Side Request Forgery (SSRF) vulnerability in ThemeGoods PhotoMe photome allows Server Side Request Forgery.This issue affects PhotoMe: from n/a through < 5.7.2.	5.4	More Details
CVE-2026-24559	Insertion of Sensitive Information Into Sent Data vulnerability in CRM Perks Integration for Contact Form 7 HubSpot cf7-hubspot allows Retrieve Embedded Sensitive Data.This issue affects Integration for Contact Form 7 HubSpot: from n/a through <= 1.4.3.	5.4	More Details
CVE-2026-24384	Cross-Site Request Forgery (CSRF) vulnerability in launchinteractive Merge + Minify + Refresh merge-minify-refresh allows Cross Site Request Forgery.This issue affects Merge + Minify + Refresh: from n/a through <= 2.14.	5.4	More Details
CVE-2026-22358	Server-Side Request Forgery (SSRF) vulnerability in SmartDataSoft Electrician - Electrical Service WordPress electrician allows Server Side Request Forgery.This issue affects Electrician - Electrical Service WordPress: from n/a through <= 5.6.	5.4	More Details
CVE-2025-47500	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Benjamin Intal Stackable stackable-ultimate-gutenberg-blocks allows Stored XSS.This issue affects Stackable: from n/a through <= 3.19.5.	5.4	More Details
CVE-2026-24560	Missing Authorization vulnerability in Cloudinary Cloudinary cloudinary-image-management-and-manipulation-in-the-cloud-cdn allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Cloudinary: from n/a through <= 3.3.0.	5.4	More Details
CVE-2026-24581	Missing Authorization vulnerability in WP Swings Points and Rewards for WooCommerce points-and-rewards-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Points and Rewards for WooCommerce: from n/a through <= 2.9.5.	5.4	More Details
CVE-2026-24127	Typemill is a flat-file, Markdown-based CMS designed for informational documentation websites. A reflected Cross-Site Scripting (XSS) exists in the login error view template `login.twig` of versions 2.19.1 and below. The `username` value can be echoed back without proper contextual encoding when authentication fails. An attacker can execute script in the login page context. This issue has been fixed in version 2.19.2.	5.4	More Details
CVE-2025-70458	A DOM-based Cross-Site Scripting (XSS) vulnerability exists in the DomainCheckerApp class within domain/script.js of Sourcecodester Domain Availability Checker v1.0. The vulnerability occurs because the application improperly handles user-supplied data in the createResultElement method by using the unsafe innerHTML property to render domain search results.	5.4	More Details
CVE-2025-63026	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand Restaurant Theme Elements for Elementor grandrestaurant-elementor allows Stored XSS.This issue affects Grand Restaurant Theme Elements for Elementor: from n/a through <= 2.1.1.	5.4	More Details
CVE-2026-24561	Missing Authorization vulnerability in Mahmudul Hasan Arif FluentBoards fluent-boards allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects FluentBoards: from n/a through <= 1.91.1.	5.4	More Details
CVE-2026-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in favethemes Houzez Theme - Functionality houzez-theme-functionality allows Stored XSS.This issue affects Houzez Theme - Functionality: from n/a through <=	5.4	More Details

24355	4.2.6.		
CVE-2026-24631	Authorization Bypass Through User-Controlled Key vulnerability in Mikado-Themes Rosebud rosebud allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Rosebud: from n/a through <= 1.4.	5.4	More Details
CVE-2026-24622	Missing Authorization vulnerability in Sergiy Dzysyak Suggestion Toolkit suggestion-toolkit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Suggestion Toolkit: from n/a through <= 5.0.	5.4	More Details
CVE-2026-24601	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Pay Writer penci-pay-writer allows Stored XSS.This issue affects Penci Pay Writer: from n/a through <= 1.5.	5.4	More Details
CVE-2026-24600	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Review penci-review allows Stored XSS.This issue affects Penci Review: from n/a through <= 3.5.	5.4	More Details
CVE-2026-24570	Missing Authorization vulnerability in WisdmLabs Edwiser Bridge edwiser-bridge allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Edwiser Bridge: from n/a through <= 4.3.2.	5.4	More Details
CVE-2026-24595	Missing Authorization vulnerability in zohocrm Zoho CRM Lead Magnet zoho-crm-forms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Zoho CRM Lead Magnet: from n/a through <= 1.8.1.5.	5.4	More Details
CVE-2026-24591	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in yasir129 Turn Yoast SEO FAQ Block to Accordion faq-schema-block-to-accordion allows Stored XSS.This issue affects Turn Yoast SEO FAQ Block to Accordion: from n/a through <= 1.0.6.	5.4	More Details
CVE-2026-24587	Missing Authorization vulnerability in kutsy AJAX Hits Counter + Popular Posts Widget ajax-hits-counter allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AJAX Hits Counter + Popular Posts Widget: from n/a through <= 0.10.210305.	5.4	More Details
CVE-2025-66140	Missing Authorization vulnerability in merkulove Uper for Elementor uper-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Uper for Elementor: from n/a through <= 1.0.5.	5.4	More Details
CVE-2026-22349	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in linux4me2 Menu In Post menu-in-post allows DOM-Based XSS.This issue affects Menu In Post: from n/a through <= 1.4.1.	5.4	More Details
CVE-2026-1429	Single Sign-On Portal System developed by WellChoose has a Reflected Cross-site Scripting vulnerability, allowing authenticated remote attackers to execute arbitrary JavaScript codes in user's browser through phishing attacks.	5.4	More Details
CVE-2026-22404	Authorization Bypass Through User-Controlled Key vulnerability in Mikado-Themes Innovio innovio allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Innovio: from n/a through <= 1.7.	5.4	More Details
CVE-2026-1489	A flaw was found in GLib. An integer overflow vulnerability in its Unicode case conversion implementation can lead to memory corruption. By processing specially crafted and extremely large Unicode strings, an attacker could trigger an undersized memory allocation, resulting in out-of-bounds writes. This could cause applications utilizing GLib for string conversion to crash or become unstable.	5.4	More Details
CVE-2026-22406	Authorization Bypass Through User-Controlled Key vulnerability in Mikado-Themes Overton overton allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Overton: from n/a through <= 1.3.	5.4	More Details
CVE-2026-22400	Authorization Bypass Through User-Controlled Key vulnerability in Mikado-Themes Holmes holmes allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Holmes: from n/a through <= 1.7.	5.4	More Details

CVE-2026-22398	Authorization Bypass Through User-Controlled Key vulnerability in Mikado-Themes Fleur fleur allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fleur: from n/a through <= 2.0.	5.4	More Details
CVE-2021-47817	OpenEMR 5.0.2.1 contains a cross-site scripting vulnerability that allows authenticated attackers to inject malicious JavaScript through user profile parameters. Attackers can exploit the vulnerability by crafting a malicious payload to download and execute a web shell, enabling remote command execution on the vulnerable OpenEMR instance.	5.4	More Details
CVE-2026-22396	Authorization Bypass Through User-Controlled Key vulnerability in Mikado-Themes Fiorello fiorello allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fiorello: from n/a through <= 1.0.	5.4	More Details
CVE-2026-22393	Authorization Bypass Through User-Controlled Key vulnerability in Mikado-Themes Curly curly allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Curly: from n/a through <= 3.3.	5.4	More Details
CVE-2026-22391	Authorization Bypass Through User-Controlled Key vulnerability in Mikado-Themes Cocco cocco allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Cocco: from n/a through <= 1.5.1.	5.4	More Details
CVE-2025-57681	The WorklogPRO - Timesheets for Jira plugin in Jira Data Center before version 4.23.6-jira10 and before version 4.23.5-jira9 allows users and attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability. The vulnerability is exploited via a specially crafted payload placed in an issue's summary field	5.4	More Details
CVE-2026-22407	Authorization Bypass Through User-Controlled Key vulnerability in Mikado-Themes Roam roam allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Roam: from n/a through <= 2.1.1.	5.4	More Details
CVE-2026-22430	Authorization Bypass Through User-Controlled Key vulnerability in Mikado-Themes Verdure verdure allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Verdure: from n/a through <= 1.6.	5.4	More Details
CVE-2026-22483	Cross-Site Request Forgery (CSRF) vulnerability in winkm89 teachPress teachpress allows Cross Site Request Forgery.This issue affects teachPress: from n/a through <= 9.0.12.	5.4	More Details
CVE-2026-24034	Horilla is a free and open source Human Resource Management System (HRMS). In versions prior to 1.5.0, a cross-site scripting vulnerability can be triggered because the extension and content-type are not checked during the profile photo update step. Version 1.5.0 fixes the issue.	5.4	More Details
CVE-2026-22382	Cross-Site Request Forgery (CSRF) vulnerability in Mikado-Themes PawFriends - Pet Shop and Veterinary WordPress Theme pawfriends allows Cross Site Request Forgery.This issue affects PawFriends - Pet Shop and Veterinary WordPress Theme: from n/a through <= 1.3.	5.4	More Details
CVE-2026-22409	Authorization Bypass Through User-Controlled Key vulnerability in Mikado-Themes Justicia justicia allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Justicia: from n/a through <= 1.2.	5.4	More Details
CVE-2025-70368	Worklenz version 2.1.5 contains a Stored Cross-Site Scripting (XSS) vulnerability in the Project Updates feature. An attacker can submit a malicious payload in the Updates text field which is then rendered in the reporting view without proper sanitization. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2026-22411	Authorization Bypass Through User-Controlled Key vulnerability in Mikado-Themes Dolcino dolcino allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Dolcino: from n/a through <= 1.6.	5.4	More Details
CVE-2026-	Authorization Bypass Through User-Controlled Key vulnerability in Elated-Themes Sweet Jane sweetjane allows Exploiting Incorrectly Configured Access Control Security Levels.This	5.4	More Details

22426	issue affects Sweet Jane: from n/a through <= 1.2.		
CVE-2025-69300	Missing Authorization vulnerability in Leap13 Premium Addons for Elementor premium-addons-for-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Premium Addons for Elementor: from n/a through <= 4.11.63.	5.4	More Details
CVE-2026-24599	Authorization Bypass Through User-Controlled Key vulnerability in XLPlugins NextMove Lite woo-thank-you-page-nextmove-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects NextMove Lite: from n/a through <= 2.23.0.	5.3	More Details
CVE-2026-24593	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Strategy11 Team AWP Classifieds another-wordpress-classifieds-plugin allows Retrieve Embedded Sensitive Data.This issue affects AWP Classifieds: from n/a through <= 4.4.3.	5.3	More Details
CVE-2026-24589	Insertion of Sensitive Information Into Sent Data vulnerability in Cargus eCommerce Cargus cargus allows Retrieve Embedded Sensitive Data.This issue affects Cargus: from n/a through <= 1.5.8.	5.3	More Details
CVE-2026-24602	Missing Authorization vulnerability in Raptive Raptive Ads adthrive-ads allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Raptive Ads: from n/a through <= 3.10.0.	5.3	More Details
CVE-2026-24568	Missing Authorization vulnerability in WP Travel WP Travel wp-travel allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Travel: from n/a through <= 11.0.0.	5.3	More Details
CVE-2026-24583	Missing Authorization vulnerability in sumup SumUp Payment Gateway For WooCommerce sumup-payment-gateway-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SumUp Payment Gateway For WooCommerce: from n/a through <= 2.7.9.	5.3	More Details
CVE-2026-24577	Missing Authorization vulnerability in Genetech Products Pie Register pie-register allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Pie Register: from n/a through <= 3.8.4.7.	5.3	More Details
CVE-2026-20080	A vulnerability in the SSH service of Cisco IEC6400 Wireless Backhaul Edge Compute Software could allow an unauthenticated, remote attacker to cause the SSH service to stop responding. This vulnerability exists because the SSH service lacks effective flood protection. An attacker could exploit this vulnerability by initiating a denial of service (DoS) attack against the SSH port. A successful exploit could allow the attacker to cause the SSH service to be unresponsive during the period of the DoS attack. All other operations remain stable during the attack.	5.3	More Details
CVE-2026-24604	Missing Authorization vulnerability in themebeez Simple GDPR Cookie Compliance simple-gdpr-cookie-compliance allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Simple GDPR Cookie Compliance: from n/a through <= 2.0.0.	5.3	More Details
CVE-2026-24562	Missing Authorization vulnerability in Ryviu Ryviu &#8211; Product Reviews for WooCommerce ryviu allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ryviu &#8211; Product Reviews for WooCommerce: from n/a through <= 3.1.26.	5.3	More Details
CVE-2026-24557	Insertion of Sensitive Information Into Sent Data vulnerability in WEN Solutions Contact Form 7 GetResponse Extension contact-form-7-getresponse-extension allows Retrieve Embedded Sensitive Data.This issue affects Contact Form 7 GetResponse Extension: from n/a through <= 1.0.8.	5.3	More Details
CVE-2026-24556	Missing Authorization vulnerability in wpdive ElementCamp element-camp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ElementCamp: from n/a through <= 2.3.2.	5.3	More Details
CVE-2026-22263	Suricata is a network IDS, IPS and NSM engine. Starting in version 8.0.0 and prior to version 8.0.3, inefficiency in http1 headers parsing can lead to slowdown over multiple packets. Version 8.0.3 patches the issue. No known workarounds are available.	5.3	More Details

CVE-2026-24548	Server-Side Request Forgery (SSRF) vulnerability in Prince Radio Player radio-player allows Server Side Request Forgery.This issue affects Radio Player: from n/a through <= 2.0.91.	5.3	More Details
CVE-2026-24541	Missing Authorization vulnerability in mkscripts Download After Email download-after-email allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Download After Email: from n/a through <= 2.1.9.	5.3	More Details
CVE-2026-24472	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to version 4.11.7, Cache Middleware contains an information disclosure vulnerability caused by improper handling of HTTP cache control directives. The middleware does not respect standard cache control headers such as `Cache-Control: private` or `Cache-Control: no-store`, which may result in private or authenticated responses being cached and subsequently exposed to unauthorized users. Version 4.11.7 has a patch for the issue.	5.3	More Details
CVE-2026-24539	Missing Authorization vulnerability in ABCdatos Protección de datos &#8211; RGPD proteccion-datos-rgpd allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Protección de datos &#8211; RGPD: from n/a through <= 0.68.	5.3	More Details
CVE-2026-24603	Missing Authorization vulnerability in themebeez Universal Google Adsense and Ads manager universal-google-adsense-and-ads-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Universal Google Adsense and Ads manager: from n/a through <= 1.1.8.	5.3	More Details
CVE-2026-24612	Missing Authorization vulnerability in themebeez Orchid Store orchid-store allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Orchid Store: from n/a through <= 1.5.15.	5.3	More Details
CVE-2026-24606	Missing Authorization vulnerability in Web Impian Bayarcash WooCommerce bayarcash-wc allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Bayarcash WooCommerce: from n/a through <= 4.3.11.	5.3	More Details
CVE-2026-24607	Missing Authorization vulnerability in wptravelengine Travel Monster travel-monster allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Travel Monster: from n/a through <= 1.3.3.	5.3	More Details
CVE-2026-1418	A security vulnerability has been detected in GPAC up to 2.4.0. This affects the function gf_text_import_srt_bifs of the file src/scene_manager/text_to_bifs.c of the component SRT Subtitle Import. Such manipulation leads to out-of-bounds write. The attack needs to be performed locally. The exploit has been disclosed publicly and may be used. The name of the patch is 10c73b82cf0e367383d091db38566a0e4fe71772. It is best practice to apply a patch to resolve this issue.	5.3	More Details
CVE-2026-0593	The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the processBackgroundAction() function in all versions up to, and including, 10.0.04. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify global map engine settings.	5.3	More Details
CVE-2025-13920	The WP Directory Kit plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.4.9 via the wdk_public_action AJAX handler. This makes it possible for unauthenticated attackers to extract email addresses for users with Directory Kit-specific user roles.	5.3	More Details
CVE-2025-11065	A flaw was found in github.com/go-viper/mapstructure/v2, in the field processing component using mapstructure.WeakDecode. This vulnerability allows information disclosure through detailed error messages that may leak sensitive input values via malformed user-supplied data processed in security-critical contexts.	5.3	More Details
CVE-	Horilla is a free and open source Human Resource Management System (HRMS). Versions 1.4.0 and above expose unpublished job postings through the /recruitment/recruitment-details// endpoint without authentication. The response includes draft job titles,		More

2026-24036	descriptions and application link allowing unauthenticated users to view unpublished roles and access the application workflow for unpublished jobs. Unauthorized access to unpublished job posts can leak sensitive internal hiring information and cause confusion among candidates. This issue has been fixed in version 1.5.0.	5.3	Details
CVE-2025-14843	The Wizit Gateway for WooCommerce plugin for WordPress is vulnerable to Unauthenticated Arbitrary Order Cancellation in all versions up to, and including, 1.2.9. This is due to a lack of authentication and authorization checks in the 'handle_checkout_redirecturl_response' function. This makes it possible for unauthenticated attackers to cancel arbitrary WooCommerce orders by sending a crafted request with a valid order ID.	5.3	More Details
CVE-2025-14629	The Alchemist Ajax Upload plugin for WordPress is vulnerable to unauthorized media file deletion due to a missing capability check on the 'delete_file' function in all versions up to, and including, 1.1. This makes it possible for unauthenticated attackers to delete arbitrary WordPress media attachments.	5.3	More Details
CVE-2025-14609	The Wise Analytics plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.1.9. This is due to missing capability checks on the REST API endpoint '/wise-analytics/v1/report'. This makes it possible for unauthenticated attackers to access sensitive analytics data including administrator usernames, login timestamps, visitor tracking information, and business intelligence data via the 'name' parameter granted they can send unauthenticated requests.	5.3	More Details
CVE-2026-23961	Mastodon is a free, open-source social network server based on ActivityPub. Mastodon allows server administrators to suspend remote users to prevent interactions. However, some logic errors allow already-known posts from such suspended users to appear in timelines if boosted. Furthermore, under certain circumstances, previously-unknown posts from suspended users can be processed. This issue allows old posts from suspended users to occasionally end up on timelines on all Mastodon versions. Additionally, on Mastodon versions from v4.5.0 to v4.5.4, v4.4.5 to v4.4.11, v4.3.13 to v4.3.17, and v4.2.26 to v4.2.29, remote suspended users can partially bypass the suspension to get new posts in. Mastodon versions v4.5.5, v4.4.12, v4.3.18 are patched.	5.3	More Details
CVE-2026-0927	The KiviCare – Clinic & Patient Management System (EHR) plugin for WordPress is vulnerable to arbitrary file uploads due to missing authorization checks in the uploadMedicalReport() function in all versions up to, and including, 3.6.15. This makes it possible for unauthenticated attackers to upload text files and PDF documents to the affected site's server which may be leveraged for further attacks such as hosting malicious content or phishing pages via PDF files.	5.3	More Details
CVE-2026-24489	Gakido is a Python HTTP client focused on browser impersonation and anti-bot evasion. A vulnerability was discovered in Gakido prior to version 0.1.1 that allowed HTTP header injection through CRLF (Carriage Return Line Feed) sequences in user-supplied header values and names. When making HTTP requests with user-controlled header values containing `\r\n` (CRLF), `\n` (LF), or `\x00` (null byte) characters, an attacker could inject arbitrary HTTP headers into the request. The fix in version 0.1.1 adds a `_sanitize_header()` function that strips `\r`, `\n`, and `\x00` characters from both header names and values before they are included in HTTP requests.	5.3	More Details
CVE-2025-27377	Altium Designer version 24.9.0 does not validate self-signed server certificates for cloud connections. An attacker capable of performing a man-in-the-middle (MITM) attack could exploit this issue to intercept or manipulate network traffic, potentially exposing authentication credentials or sensitive design data.	5.3	More Details
CVE-2026-1102	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.3 before 18.6.4, 18.7 before 18.7.2, and 18.8 before 18.8.2 that could have allowed an unauthenticated user to create a denial of service condition by sending repeated malformed SSH authentication requests.	5.3	More Details
CVE-	A security flaw has been discovered in Sangfor Operation and Maintenance Security Management System up to 3.0.12. This affects the function edit_pwd_mall of the file		

2026-1325	/fort/login/edit_pwd_mall. The manipulation of the argument flag results in weak password recovery. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-14971	The Link Invoice Payment for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the createPartialPayment and cancelPartialPayment functions in all versions up to, and including, 2.8.0. This makes it possible for unauthenticated attackers to create partial payments on any order or cancel any existing partial payment via ID enumeration.	5.3	More Details
CVE-2026-1036	The Photo Gallery by 10Web – Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the delete_comment() function in all versions up to, and including, 1.8.36. This makes it possible for unauthenticated attackers to delete arbitrary image comments. Note: comments functionality is only available in the Pro version of the plugin.	5.3	More Details
CVE-2026-23990	The Flux Operator is a Kubernetes CRD controller that manages the lifecycle of CNCF Flux CD and the ControlPlane enterprise distribution. Starting in version 0.36.0 and prior to version 0.40.0, a privilege escalation vulnerability exists in the Flux Operator Web UI authentication code that allows an attacker to bypass Kubernetes RBAC impersonation and execute API requests with the operator's service account privileges. In order to be vulnerable, cluster admins must configure the Flux Operator with an OIDC provider that issues tokens lacking the expected claims (e.g., `email`, `groups`), or configure custom CEL expressions that can evaluate to empty values. After OIDC token claims are processed through CEL expressions, there is no validation that the resulting `username` and `groups` values are non-empty. When both values are empty, the Kubernetes client-go library does not add impersonation headers to API requests, causing them to be executed with the flux-operator service account's credentials instead of the authenticated user's limited permissions. This can result in privilege escalation, data exposure, and/or information disclosure. Version 0.40.0 patches the issue.	5.3	More Details
CVE-2025-41728	A low privileged remote attacker may be able to disclose confidential information from the memory of a privileged process by sending specially crafted calls to the Device Manager web service that cause an out-of-bounds read operation under certain circumstances due to ASLR and thereby potentially copy confidential information into a response.	5.3	More Details
CVE-2026-22796	Issue summary: A type confusion vulnerability exists in the signature verification of signed PKCS#7 data where an ASN1_TYPE union member is accessed without first validating the type, causing an invalid or NULL pointer dereference when processing malformed PKCS#7 data. Impact summary: An application performing signature verification of PKCS#7 data or calling directly the PKCS7_digest_from_attributes() function can be caused to dereference an invalid or NULL pointer when reading, resulting in a Denial of Service. The function PKCS7_digest_from_attributes() accesses the message digest attribute value without validating its type. When the type is not V_ASN1_OCTET_STRING, this results in accessing invalid memory through the ASN1_TYPE union, causing a crash. Exploiting this vulnerability requires an attacker to provide a malformed signed PKCS#7 to an application that verifies it. The impact of the exploit is just a Denial of Service, the PKCS7 API is legacy and applications should be using the CMS API instead. For these reasons the issue was assessed as Low severity. The FIPS modules in 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the PKCS#7 parsing implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0, 1.1.1 and 1.0.2 are vulnerable to this issue.	5.3	More Details
CVE-2025-52023	A vulnerability in the PHP backend of gemscms.aptsys.com.sg thru 2025-05-28 allows unauthenticated remote attackers to trigger detailed error messages that disclose internal file paths, code snippets, and stack traces. This occurs when specially crafted HTTP GET/POST requests are sent to public API endpoints, exposing potentially sensitive information useful for further exploitation. This issue is classified under CWE-209: Information Exposure Through an Error Message.	5.3	More Details
CVE-	A vulnerability in the PHP backend of gemsloyalty.aptsys.com.sg thru 2025-05-28 allows unauthenticated remote attackers to trigger detailed error messages that disclose internal file paths, code snippets, and stack traces. This occurs when specially crafted HTTP		More

2025-52022	GET/POST requests are sent to public API endpoints, exposing potentially sensitive information useful for further exploitation. This issue is classified under CWE-209: Information Exposure Through an Error Message.	5.3	Details
CVE-2021-47860	GetSimple CMS Custom JS 0.1 plugin contains a cross-site request forgery vulnerability that allows unauthenticated attackers to inject arbitrary client-side code into administrator browsers. Attackers can craft a malicious website that triggers a cross-site scripting payload to execute remote code on the hosting server when an authenticated administrator visits the page.	5.3	More Details
CVE-2026-24634	Authorization Bypass Through User-Controlled Key vulnerability in Rustaurius Ultimate Reviews ultimate-reviews allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ultimate Reviews: from n/a through <= 3.2.16.	5.3	More Details
CVE-2026-24633	Missing Authorization vulnerability in Passionate Brains Add Expires Headers & Optimized Minify add-expires-headers allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Add Expires Headers & Optimized Minify: from n/a through <= 3.1.0.	5.3	More Details
CVE-2026-24625	Missing Authorization vulnerability in Imaginate Solutions File Uploads Addon for WooCommerce woo-addon-uploads allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects File Uploads Addon for WooCommerce: from n/a through <= 1.7.3.	5.3	More Details
CVE-2026-24619	Missing Authorization vulnerability in PopCash PopCash.Net Code Integration Tool popcashnet-code-integration-tool allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PopCash.Net Code Integration Tool: from n/a through <= 1.8.	5.3	More Details
CVE-2026-24615	Missing Authorization vulnerability in themebeez Cream Magazine cream-magazine allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Cream Magazine: from n/a through <= 2.1.10.	5.3	More Details
CVE-2026-24613	Missing Authorization vulnerability in Ecwid by Lightspeed Ecommerce Shopping Cart Ecwid Shopping Cart ecwid-shopping-cart allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ecwid Shopping Cart: from n/a through <= 7.0.5.	5.3	More Details
CVE-2025-57783	Improper header parsing may lead to request smuggling has been identified in Hiawatha webserver version 11.7 which allows an unauthenticated attacker to access restricted resources managed by Hiawatha webserver.	5.3	More Details
CVE-2026-1332	MeetingHub developed by HAMASTAR Technology has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to access specific API functions and obtain meeting-related information.	5.3	More Details
CVE-2026-24422	phpMyFAQ is an open source FAQ web application. In versions 4.0.16 and below, multiple public API endpoints improperly expose sensitive user information due to insufficient access controls. The OpenQuestionController::list() endpoint calls Question::getAll() with showAll=true by default, returning records marked as non-public (isVisible=false) along with user email addresses, with similar exposures present in comment, news, and FAQ APIs. This information disclosure vulnerability could enable attackers to harvest email addresses for phishing campaigns or access content that was explicitly marked as private. This issue has been fixed in version 4.0.17.	5.3	More Details
CVE-2026-23831	Rekor is a software supply chain transparency log. In versions 1.4.3 and below, the entry implementation can panic on attacker-controlled input when canonicalizing a proposed entry with an empty spec.message, causing nil Pointer Dereference. Function validate() returns nil (success) when message is empty, leaving sign1Msg uninitialized, and Canonicalize() later dereferences v.sign1Msg.Payload. A malformed proposed entry of the cose/v0.0.1 type can cause a panic on a thread within the Rekor process. The thread is recovered so the client receives a 500 error message and service still continues, so the availability impact of this is minimal. This issue has been fixed in version 1.5.0.	5.3	More Details

CVE-2026-22469	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in mwtemplates DeepDigital deepdigital allows Code Injection.This issue affects DeepDigital: from n/a through <= 1.0.2.	5.3	More Details
CVE-2026-24366	Missing Authorization vulnerability in YITHEMES YITH WooCommerce Request A Quote yith-woocommerce-request-a-quote allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects YITH WooCommerce Request A Quote: from n/a through <= 2.46.0.	5.3	More Details
CVE-2026-24117	Rekor is a software supply chain transparency log. In versions 1.4.3 and below, attackers can trigger SSRF to arbitrary internal services because /api/v1/index/retrieve supports retrieving a public key via user-provided URL. Since the SSRF only can trigger GET requests, the request cannot mutate state. The response from the GET request is not returned to the caller so data exfiltration is not possible. A malicious actor could attempt to probe an internal network through Blind SSRF. The issue has been fixed in version 1.5.0. To workaround this issue, disable the search endpoint with --enable_retrieve_api=false.	5.3	More Details
CVE-2026-22445	Missing Authorization vulnerability in Proptech Plugin Apimo Connector apimo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Apimo Connector: from n/a through <= 2.6.4.	5.3	More Details
CVE-2026-22348	Missing Authorization vulnerability in Tasos Fel Civic Cookie Control civic-cookie-control-8 allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Civic Cookie Control: from n/a through <= 1.53.	5.3	More Details
CVE-2025-22234	The fix applied in CVE-2025-22228 inadvertently broke the timing attack mitigation implemented in DaoAuthenticationProvider. This can allow attackers to infer valid usernames or other authentication behavior via response-time differences under certain configurations.	5.3	More Details
CVE-2026-1446	There is a Cross Site Scripting issue in Esri ArcGIS Pro versions 3.6.0 and earlier. A local attacker could supply malicious strings into ArcGIS Pro which may execute when a specific dialog is opened. This issue is fixed in ArcGIS Pro 3.6.1.	5.0	More Details
CVE-2026-22280	Dell PowerScale OneFS, versions 9.5.0.0 through 9.5.1.5, versions 9.6.0.0 through 9.7.1.10, versions 9.8.0.0 through 9.10.1.3, versions starting from 9.11.0.0 and prior to 9.13.0.0, contains an incorrect permission assignment for critical resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service.	5.0	More Details
CVE-2026-0806	The WP-ClanWars plugin for WordPress is vulnerable to SQL Injection via the 'orderby' parameter in all versions up to, and including, 2.0.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2026-1224	Tanium addressed an uncontrolled resource consumption vulnerability in Discover.	4.9	More Details
CVE-2026-20055	Multiple vulnerabilities in the web-based management interface of Cisco Packaged Contact Center Enterprise (Packaged CCE) and Cisco Unified Contact Center Enterprise (Unified CCE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device.&nbsp; These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker must have valid administrative credentials.	4.8	More Details
	Horilla is a free and open source Human Resource Management System (HRMS). In version		

CVE-2026-24037	1.4.0, the has_xss() function attempts to block XSS by matching input against a set of regex patterns. However, the regexes are incomplete and context-agnostic, making them easy to bypass. Attackers are able to redirect users to malicious domains, run external JavaScript, and steal CSRF tokens that can be used to craft CSRF attacks against admins. This issue has been fixed in version 1.5.0.	4.8	More Details
CVE-2026-24621	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vladimir Statsenko Terms descriptions terms-descriptions allows DOM-Based XSS.This issue affects Terms descriptions: from n/a through <= 3.4.9.	4.8	More Details
CVE-2026-20109	Multiple vulnerabilities in the web-based management interface of Cisco Packaged Contact Center Enterprise (Packaged CCE) and Cisco Unified Contact Center Enterprise (Unified CCE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device.&nbsp; These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker must have valid administrative credentials.	4.8	More Details
CVE-2026-24398	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to version 4.11.7, IP Restriction Middleware in Hono is vulnerable to an IP address validation bypass. The \`IPV4_REGEX\` pattern and \`convertIPv4ToBinary\` function in \`src/utils/ipaddr.ts\` do not properly validate that IPv4 octet values are within the valid range of 0-255, allowing attackers to craft malformed IP addresses that bypass IP-based access controls. Version 4.11.7 contains a patch for the issue.	4.8	More Details
CVE-2026-24594	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in livemesh Livemesh Addons for WPBakery Page Builder addons-for-visual-composer allows Stored XSS.This issue affects Livemesh Addons for WPBakery Page Builder: from n/a through <= 3.9.4.	4.8	More Details
CVE-2025-68138	EVerest is an EV charging software stack, and EVerest libocpp is a C++ implementation of the Open Charge Point Protocol. In libocpp prior to version 0.30.1, pointers returned by the \`strdup\` calls are never freed. At each connection attempt, the newly allocated memory area will be leaked, potentially causing memory exhaustion and denial of service. Version 0.30.1 fixes the issue.	4.7	More Details
CVE-2025-2204	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tapandsign Technologies Software Inc. Tap&Sign allows Cross-Site Scripting (XSS).This issue affects Tap&Sign: through 23012026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-24596	Cross-Site Request Forgery (CSRF) vulnerability in marynixie Related Posts Thumbnails Plugin for WordPress related-posts-thumbnails allows Cross Site Request Forgery.This issue affects Related Posts Thumbnails Plugin for WordPress: from n/a through <= 4.3.1.	4.7	More Details
CVE-2026-1419	A weakness has been identified in D-Link DCS700l 1.03.09. Affected is an unknown function of the file /setDayNightMode of the component Web Form Handler. Executing a manipulation of the argument LightSensorControl can lead to command injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	4.7	More Details
CVE-2026-24771	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to version 4.11.7, a Cross-Site Scripting (XSS) vulnerability exists in the \`ErrorBoundary\` component of the hono/jsx library. Under certain usage patterns, untrusted user-controlled strings may be rendered as raw HTML, allowing arbitrary script execution in the victim's browser. Version 4.11.7 patches the issue.	4.7	More Details
CVE-	go-tuf is a Go implementation of The Update Framework (TUF). go-tuf's TAP 4 Multirepo Client uses the map file repository name string (\`repoName\`) as a filesystem path component when selecting the local metadata cache directory. Starting in version 2.0.0		

2026-24686	and prior to version 2.4.1, if an application accepts a map file from an untrusted source, an attacker can supply a `repoName` containing traversal (e.g., `../escaped-repo`) and cause go-tuf to create directories and write the root metadata file outside the intended `LocalMetadataDir` cache base, within the running process's filesystem permissions. Version 2.4.1 contains a patch.	4.7	More Details
CVE-2026-1445	A vulnerability was found in iJason-Liu Books_Manager up to 298ba736387ca37810466349af13a0fdf828e99c. This vulnerability affects unknown code of the file controllers/books_center/upload_bookCover.php. Performing a manipulation of the argument book_cover results in unrestricted upload. The attack may be initiated remotely. The exploit has been made public and could be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available.	4.7	More Details
CVE-2026-1424	A vulnerability was identified in PHPGurukul News Portal 1.0. This affects an unknown part of the component Profile Pic Handler. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	4.7	More Details
CVE-2026-24360	Server-Side Request Forgery (SSRF) vulnerability in Craig Hewitt Seriously Simple Podcasting seriously-simple-podcasting allows Server Side Request Forgery.This issue affects Seriously Simple Podcasting: from n/a through <= 3.14.1.	4.6	More Details
CVE-2026-1300	The Responsive Header plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple plugin settings parameters in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. 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 an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-1302	The Meta-box GalleryMeta plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-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-2026-1266	The Postalicious plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.0.1 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-2026-1084	The Cookie consent for developers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple settings fields in all versions up to, and including, 1.7.1 due to insufficient input sanitization and output escaping. 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 an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-1191	The JavaScript Notifier plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin settings in all versions up to, and including, 1.2.8. This is due to insufficient input sanitization and output escaping on user-supplied attributes in the `wp_footer` action. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Details
CVE-2025-67125	A signed integer overflow in docopt.cpp v0.6.2 (LeafPattern::match in docopt_private.h) when merging occurrence counters (e.g., default LONG_MAX + first user "-v/--verbose") can cause counter wrap (negative/unbounded semantics) and lead to logic/policy bypass in applications that rely on occurrence-based limits, rate-gating, or safety toggles. In hardened builds (e.g., UBSan or -ftrapv), the overflow may also result in process abort (DoS).	4.4	More Details

CVE-2026-22275	Dell ECS, versions 3.8.1.0 through 3.8.1.7, and Dell ObjectScale versions prior to 4.2.0.0, contains an Inclusion of Sensitive Information in Source Code vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure.	4.4	More Details
CVE-2026-24544	Missing Authorization vulnerability in Harmonic Design HD Quiz hd-quiz allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects HD Quiz: from n/a through <= 2.0.9.	4.3	More Details
CVE-2026-23963	Mastodon is a free, open-source social network server based on ActivityPub. Prior to versions 4.5.5, 4.4.12, and 4.3.18, the server does not enforce a maximum length for the names of lists or filters, or for filter keywords, allowing any user to set an arbitrarily long string as the name or keyword. Any local user can abuse the list or filter fields to cause disproportionate storage and computing resource usage. They can additionally cause their own web interface to be unusable, although they must intentionally do this to themselves or unknowingly approve a malicious API client. Mastodon versions v4.5.5, v4.4.12, v4.3.18 are patched.	4.3	More Details
CVE-2026-1081	The Set Bulk Post Categories 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 bulk category update functionality. This makes it possible for unauthenticated attackers to modify post categories in bulk 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-2026-1076	The Star Review Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.2. This is due to missing nonce validation on the settings page. This makes it possible for unauthenticated attackers to update the plugin's CSS 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-2026-1088	The Login Page Editor plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2. This is due to missing nonce validation on the devotion_loginform_process() AJAX action. This makes it possible for unauthenticated attackers to update the plugin's login page 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-2026-1075	The ZT Captcha plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.4. This is due to improper nonce validation on the save_ztcpt_captcha_settings action where the nonce check can be bypassed by sending an empty token value. This makes it possible for unauthenticated attackers to modify 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-2026-1070	The Alex User Counter plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.0. This is due to missing nonce validation on the alex_user_counter_function() function. This makes it possible for unauthenticated attackers to update the plugin 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-2026-24549	Cross-Site Request Forgery (CSRF) vulnerability in Paolo GeoDirectory geodirectory allows Cross Site Request Forgery.This issue affects GeoDirectory: from n/a through <= 2.8.147.	4.3	More Details
CVE-2026-24039	Horilla is a free and open source Human Resource Management System (HRMS). Version 1.4.0 has Improper Access Control, allowing low-privileged employees to self-approve documents they have uploaded. The document-approval UI is intended to be restricted to administrator or high-privilege roles only; however, an insufficient server-side authorization check on the approval endpoint lets a standard employee modify the approval status of their own uploaded document. A successful exploitation allows users with only employee-level permissions to alter application state reserved for administrators. This undermines the integrity of HR processes (for example, acceptance of credentials, certifications, or supporting materials), and may enable submission of unvetted documents. This issue is fixed in version 1.5.0.	4.3	More Details

CVE-2026-24543	Missing Authorization vulnerability in Horea Radu Materialis Companion materialis-companion allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Materialis Companion: from n/a through <= 1.3.52.	4.3	More Details
CVE-2026-24563	Missing Authorization vulnerability in Ashan Perera LifePress lifepress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects LifePress: from n/a through <= 2.1.3.	4.3	More Details
CVE-2026-24542	Cross-Site Request Forgery (CSRF) vulnerability in John James Jacoby WP Term Order wp-term-order allows Cross Site Request Forgery.This issue affects WP Term Order: from n/a through <= 2.1.0.	4.3	More Details
CVE-2025-13139	The SurveyJS: Drag & Drop WordPress Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.12.20. This is due to missing nonce validation on the SurveyJS_AddSurvey AJAX action. This makes it possible for unauthenticated attackers to create surveys 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-2026-24535	Missing Authorization vulnerability in webdevstudios Automatic Featured Images from Videos automatic-featured-images-from-videos allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Automatic Featured Images from Videos: from n/a through <= 1.2.7.	4.3	More Details
CVE-2025-13194	The SurveyJS: Drag & Drop WordPress Form Builder to create, style and embed multiple forms of any complexity plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.12.20. This is due to missing nonce verification on the 'SurveyJS_RenameSurvey' AJAX action. This makes it possible for unauthenticated attackers to rename surveys 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-2025-13205	The SurveyJS: Drag & Drop WordPress Form Builder to create, style and embed multiple forms of any complexity plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.12.20. This is due to missing or incorrect nonce validation on the `SurveyJS_CloneSurvey` AJAX action. This makes it possible for unauthenticated attackers to duplicate surveys 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-2025-14630	The AdminQuickbar plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.9.3. This is due to missing or incorrect nonce validation on the 'saveSettings' and 'renamePost' AJAX actions. This makes it possible for unauthenticated attackers to modify plugin settings and update post titles 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-2025-14907	The Moderate Selected Posts plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4. This is due to missing nonce verification on the msp_admin_page() function. This makes it possible for unauthenticated attackers to modify plugin 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-2025-15516	The All-in-One Video Gallery plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ajax_callback_store_user_meta() function in versions 4.1.0 to 4.6.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update arbitrary string-based user meta keys for their own account.	4.3	More Details
CVE-2026-23683	SAP Fiori App Intercompany Balance Reconciliation does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This has low impact on confidentiality, integrity and availability are not impacted.	4.3	More Details
CVE-2025-	The WP Youtube Video Gallery plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing nonce verification on the wpYTVideoGallerySettingSave() function. This makes it possible for unauthenticated	4.3	More Details

14906	attackers to modify plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.		
CVE-2026-24564	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Israpil Textmetrics webtexttool allows Code Injection.This issue affects Textmetrics: from n/a through <= 3.6.3.	4.3	More Details
CVE-2026-24332	Discord through 2026-01-16 allows gathering information about whether a user's client state is Invisible (and not actually offline) because the response to a WebSocket API request includes the user in the presences array (with "status": "offline"), whereas offline users are omitted from the presences array. This is arguably inconsistent with the UI description of Invisible as "You will appear offline."	4.3	More Details
CVE-2025-14969	A flaw was found in Hibernate Reactive. When an HTTP endpoint is exposed to perform database operations, a remote client can prematurely close the HTTP connection. This action may lead to leaking connections from the database connection pool, potentially causing a Denial of Service (DoS) by exhausting available database connections.	4.3	More Details
CVE-2026-24388	Missing Authorization vulnerability in Ludwig You WPMasterToolKit wpmastertoolkit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPMasterToolKit: from n/a through <= 2.14.0.	4.3	More Details
CVE-2026-24387	Missing Authorization vulnerability in Arul Prasad J WP Quick Post Duplicator wp-quick-post-duplicator allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Quick Post Duplicator: from n/a through <= 2.1.	4.3	More Details
CVE-2026-20888	Gitea does not properly verify authorization when canceling scheduled auto-merges via the web interface. A user with read access to pull requests may be able to cancel auto-merges scheduled by other users.	4.3	More Details
CVE-2026-24386	Missing Authorization vulnerability in Element Invader Element Invader &#8211; Template Kits for Elementor elementinvader allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Element Invader &#8211; Template Kits for Elementor: from n/a through <= 1.2.4.	4.3	More Details
CVE-2026-24636	Missing Authorization vulnerability in Syed Balkhi Sugar Calendar (Lite) sugar-calendar-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sugar Calendar (Lite): from n/a through <= 3.10.1.	4.3	More Details
CVE-2026-24605	Missing Authorization vulnerability in pencilwp X Addons for Elementor x-addons-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects X Addons for Elementor: from n/a through <= 1.0.23.	4.3	More Details
CVE-2026-22279	Dell PowerScale OneFS, versions prior 9.13.0.0, contains an insufficient logging vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to information tampering.	4.3	More Details
CVE-2026-24598	Missing Authorization vulnerability in bestwebsoft Multilanguage by BestWebSoft multilanguage allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Multilanguage by BestWebSoft: from n/a through <= 1.5.2.	4.3	More Details
CVE-2026-24035	Horilla is a free and open source Human Resource Management System (HRMS). An Improper Access Control vulnerability exists in Horilla HR Software starting in version 1.4.0 and prior to version 1.5.0, allowing any authenticated employee to upload documents on behalf of another employee without proper authorization. This occurs due to insufficient server-side validation of the employee_id parameter during file upload operations, allowing any authenticated employee to upload document in behalf of any employee. Version 1.5.0 fixes the issue.	4.3	More Details
CVE-2026-22466	Missing Authorization vulnerability in Chandni Patel WP MapIt wp-mapit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP MapIt: from n/a through <= 3.0.3.	4.3	More Details
CVE-	Missing Authorization vulnerability in topdevs Smart Product Viewer smart-product-viewer		

2026-24588	allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Smart Product Viewer: from n/a through <= 1.5.4.	4.3	More Details
CVE-2026-22468	Missing Authorization vulnerability in AbsolutePlugins Absolute Addons For Elementor absolute-addons allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Absolute Addons For Elementor: from n/a through <= 1.0.14.	4.3	More Details
CVE-2026-22458	Missing Authorization vulnerability in Mikado-Themes Wanderland wanderland allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Wanderland: from n/a through <= 1.5.	4.3	More Details
CVE-2026-24003	EVerest is an EV charging software stack. In versions up to and including 2025.12.1, it is possible to bypass the sequence state verification including authentication, and send requests that transition to forbidden states relative to the current one, thereby updating the current context with illegitimate data.cThanks to the modular design of EVerest, authorization is handled in a separate module and EVSEManager Charger internal state machine cannot transition out of the `WaitingForAuthentication` state through ISO 15118-2 communication. From this state, it was however possible through ISO 15118-2 messages which are published to the MQTT server to trick it into preparing to charge, and even to prepare to send current. The final requirement to actually send current to the EV was the closure of the contactors, which does not appear to be possible without leaving the `WaitingForAuthentication` state and leveraging ISO 15118-2 messages. As of time of publication, no fixed versions are available.	4.3	More Details
CVE-2026-22462	Cross-Site Request Forgery (CSRF) vulnerability in richardevcom Add Polylang support for Customizer add-polylang-support-for-customizer allows Cross Site Request Forgery.This issue affects Add Polylang support for Customizer: from n/a through <= 1.4.5.	4.3	More Details
CVE-2026-24580	Missing Authorization vulnerability in Ecwid by Lightspeed Ecommerce Shopping Cart Ecwid Shopping Cart ecwid-shopping-cart allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ecwid Shopping Cart: from n/a through <= 7.0.5.	4.3	More Details
CVE-2026-24579	Missing Authorization vulnerability in WP Messiah Ai Image Alt Text Generator for WP ai-image-alt-text-generator-for-wp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ai Image Alt Text Generator for WP: from n/a through <= 1.1.9.	4.3	More Details
CVE-2026-24578	Missing Authorization vulnerability in Jahid Hasan Admin login URL Change admin-login-url-change allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Admin login URL Change: from n/a through <= 1.1.5.	4.3	More Details
CVE-2026-24571	Missing Authorization vulnerability in boxnow BOX NOW Delivery box-now-delivery allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects BOX NOW Delivery: from n/a through <= 3.0.2.	4.3	More Details
CVE-2026-24569	Missing Authorization vulnerability in Sully Media Library File Size media-library-file-size allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Media Library File Size: from n/a through <= 1.6.7.	4.3	More Details
CVE-2025-14903	The Simple Crypto Shortcodes plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.2. This is due to missing nonce validation on the scs_backend function. This makes it possible for unauthenticated attackers to update plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-24567	Missing Authorization vulnerability in briarinc Anything Order by Terms anything-order-by-terms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Anything Order by Terms: from n/a through <= 1.4.0.	4.3	More Details
CVE-2026-24627	Missing Authorization vulnerability in Trusona Trusona for WordPress trusona allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Trusona for WordPress: from n/a through <= 2.0.0.	4.3	More Details
	The Meta-box GalleryMeta plugin for WordPress is vulnerable to unauthorized modification		

CVE-2026-0687	of data due to a missing capability check on the 'mb_gallery' custom post type in all versions up to, and including, 3.0.1. This makes it possible for authenticated attackers, with Author-level access and above, to create and publish galleries.	4.3	More Details
CVE-2026-24553	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Dotstore Fraud Prevention For Woocommerce woo-blocker-lite-prevent-fake-orders-and-blacklist-fraud-customers allows Retrieve Embedded Sensitive Data.This issue affects Fraud Prevention For Woocommerce: from n/a through <= 2.3.1.	4.3	More Details
CVE-2026-22450	Missing Authorization vulnerability in Select-Themes Don Peppe donpeppe allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Don Peppe: from n/a through <= 1.3.	4.3	More Details
CVE-2025-68140	EVerest is an EV charging software stack. Prior to version 2025.9.0, once the validity of the received V2G message has been verified, it is checked whether the submitted session ID matches the registered one. However, if no session has been registered, the default value is 0. Therefore, a message submitted with a session ID of 0 is accepted, as it matches the registered value. This could allow unauthorized and anonymous indirect emission of MQTT messages and communication with V2G messages handlers, updating a session context. Version 2025.9.0 fixes the issue.	4.3	More Details
CVE-2025-13921	The weDocs: AI Powered Knowledge Base, Docs, Documentation, Wiki & AI Chatbot plugin for WordPress is vulnerable to unauthorized modification or loss of data due to a missing capability check on the 'wedocs_user_documentation_handling_capabilities' function in all versions up to, and including, 2.1.16. This makes it possible for authenticated attackers, with Subscriber-level access and above, to edit any documentation post. The vulnerability was partially patched in version 2.1.16.	4.3	More Details
CVE-2025-46699	Dell Data Protection Advisor, versions prior to 19.12, contains an Improper Neutralization of Special Elements Used in a Template Engine vulnerability in the Server. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	4.3	More Details
CVE-2026-22447	Missing Authorization vulnerability in Select-Themes Prowess prowess allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Prowess: from n/a through <= 1.8.1.	4.3	More Details
CVE-2026-1208	The Friendly Functions for Welcart plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.5. This is due to missing or incorrect nonce validation on the settings page. This makes it possible for unauthenticated attackers to update plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-68139	EVerest is an EV charging software stack. In all versions up to and including 2025.12.1, the default value for `terminate_connection_on_failed_response` is `False`, which leaves the responsibility for session and connection termination to the EV. In this configuration, any errors encountered by the module are logged but do not trigger countermeasures such as session and connection reset or termination. This could be abused by a malicious user in order to exploit other weaknesses or vulnerabilities. While the default will stay at the setting that is described as potentially problematic in this reported issue, a mitigation is available by changing the `terminate_connection_on_failed_response` setting to `true`. However this cannot be set to this value by default since it can trigger errors in vehicle ECUs requiring ECU resets and lengthy unavailability in charging for vehicles. The maintainers judge this to be a much more important workaround then short-term unavailability of an EVSE, therefore this setting will stay at the current value.	4.3	More Details
CVE-2026-24522	Missing Authorization vulnerability in MyThemeShop WP Subscribe wp-subscribe allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Subscribe: from n/a through <= 1.2.16.	4.3	More Details
CVE-	The CubeWP – All-in-One Dynamic Content Framework plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.1.27 via the search feature in		More

2025-6461	class-cubewp-search-ajax-hooks.php due to insufficient restrictions on which posts can be included. This makes it possible for unauthenticated attackers to extract data from password protected, private, or draft posts that they should not have access to.	4.3	Details
CVE-2026-22359	Cross-Site Request Forgery (CSRF) vulnerability in AA-Team Wordpress Movies Bulk Importer movies importer allows Cross Site Request Forgery.This issue affects Wordpress Movies Bulk Importer: from n/a through <= 1.0.	4.3	More Details
CVE-2026-22360	Cross-Site Request Forgery (CSRF) vulnerability in AA-Team SearchAzon searchazon allows Cross Site Request Forgery.This issue affects SearchAzon: from n/a through <= 1.4.	4.3	More Details
CVE-2026-24521	Cross-Site Request Forgery (CSRF) vulnerability in Timur Kamaev Kama Thumbnail kama-thumbnail allows Cross Site Request Forgery.This issue affects Kama Thumbnail: from n/a through <= 3.5.1.	4.3	More Details
CVE-2025-55095	The function _ux_host_class_storage_media_mount() is responsible for mounting partitions on a USB mass storage device. When it encounters an extended partition entry in the partition table, it recursively calls itself to mount the next logical partition. This recursion occurs in _ux_host_class_storage_partition_read(), which parses up to four partition entries. If an extended partition is found (with type UX_HOST_CLASS_STORAGE_PARTITION_EXTENDED or EXTENDED_LBA_MAPPED), the code invokes: _ux_host_class_storage_media_mount(storage, sector + _ux_utility_long_get(...)); There is no limit on the recursion depth or tracking of visited sectors. As a result, a malicious or malformed disk image can include cyclic or excessively deep chains of extended partitions, causing the function to recurse until stack overflow occurs.	4.2	More Details
CVE-2026-23955	EVerest is an EV charging software stack. Prior to version 2025.9.0, in several places, integer values are concatenated to literal strings when throwing errors. This results in pointers arithmetic instead of printing the integer value as expected, like most of interpreted languages. This can be used by malicious operator to read unintended memory regions, including the heap and the stack. Version 2025.9.0 fixes the issue.	4.2	More Details
CVE-2026-1484	A flaw was found in the GLib Base64 encoding routine when processing very large input data. Due to incorrect use of integer types during length calculation, the library may miscalculate buffer boundaries. This can cause memory writes outside the allocated buffer. Applications that process untrusted or extremely large Base64 input using GLib may crash or behave unpredictably.	4.2	More Details
CVE-2021-47899	YetiShare File Hosting Script 5.1.0 contains a server-side request forgery vulnerability that allows attackers to read local system files through the remote file upload feature. Attackers can exploit the url parameter in the url_upload_handler endpoint to access sensitive files like /etc/passwd by using file:/// protocol.	4.0	More Details
CVE-2025-9820	A flaw was found in the GnuTLS library, specifically in the gnutls_pkcs11_token_init() function that handles PKCS#11 token initialization. When a token label longer than expected is processed, the function writes past the end of a fixed-size stack buffer. This programming error can cause the application using GnuTLS to crash or, in certain conditions, be exploited for code execution. As a result, systems or applications relying on GnuTLS may be vulnerable to a denial of service or local privilege escalation attacks.	4.0	More Details
CVE-2025-32056	The anti-theft protection mechanism can be bypassed by attackers due to weak response generation algorithms for the head unit. It is possible to reveal all 32 corresponding responses by sniffing CAN traffic or by pre-calculating the values, which allow to bypass the protection. First identified on Nissan Leaf ZE1 manufactured in 2020.	4.0	More Details
CVE-2025-57784	Tomahawk auth timing attack due to usage of `strcmp` has been identified in Hiawatha webserver version 11.7 which allows a local attacker to access the management client.	4.0	More Details
CVE-2026-	A flaw was found in glib. Missing validation of offset and count parameters in the g_buffered_input_stream_peek() function can lead to an integer overflow during length calculation. When specially crafted values are provided, this overflow results in an incorrect	3.7	More Details

0988	size being passed to memcpy(), triggering a buffer overflow. This can cause application crashes, leading to a Denial of Service (DoS).		
CVE-2026-24656	Deserialization of Untrusted Data vulnerability in Apache Karaf Decanter. The Decanter log socket collector exposes the port 4560, without authentication. If the collector exposes allowed classes property, this configuration can be bypassed. It means that the log socket collector is vulnerable to deserialization of untrusted data, eventually causing DoS. NB: Decanter log socket collector is not installed by default. Users who have not installed Decanter log socket are not impacted by this issue. This issue affects Apache Karaf Decanter before 2.12.0. Users are recommended to upgrade to version 2.12.0, which fixes the issue.	3.7	More Details
CVE-2026-24883	In GnuPG before 2.5.17, a long signature packet length causes parse_signature to return success with sig->data[] set to a NULL value, leading to a denial of service (application crash).	3.7	More Details
CVE-2026-0633	The MetForm – Contact Form, Survey, Quiz, & Custom Form Builder for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 4.1.0. This is due to the use of a forgeable cookie value derived only from the entry ID and current user ID without a server-side secret. This makes it possible for unauthenticated attackers to access form submission entry data via MetForm shortcodes for entries created within the transient TTL (default is 15 minutes).	3.7	More Details
CVE-2026-24870	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in ixray-team ixray-1.6-stcop.This issue affects ixray-1.6-stcop: before 1.3.	3.7	More Details
CVE-2026-23996	FastAPI Api Key provides a backend-agnostic library that provides an API key system. Version 1.1.0 has a timing side-channel vulnerability in verify_key(). The method applied a random delay only on verification failures, allowing an attacker to statistically distinguish valid from invalid API keys by measuring response latencies. With enough repeated requests, an adversary could infer whether a key_id corresponds to a valid key, potentially accelerating brute-force or enumeration attacks. All users relying on verify_key() for API key authentication prior to the fix are affected. Users should upgrade to version 1.1.0 to receive a patch. The patch applies a uniform random delay (min_delay to max_delay) to all responses regardless of outcome, eliminating the timing correlation. Some workarounds are available. Add an application-level fixed delay or random jitter to all authentication responses (success and failure) before the fix is applied and/or use rate limiting to reduce the feasibility of statistical timing attacks.	3.7	More Details
CVE-2026-22261	Suricata is a network IDS, IPS and NSM engine. Prior to versions 8.0.3 and 7.0.14, various inefficiencies in xff handling, especially for alerts not triggered in a tx, can lead to severe slowdowns. Versions 8.0.3 and 7.0.14 contain a patch. As a workaround, disable XFF support in the eve configuration. The setting is disabled by default.	3.7	More Details
CVE-2026-1406	A vulnerability was determined in lcg0124 BootDo up to 5ccd963c74058036b466e038cff37de4056c1600. Affected by this vulnerability is the function redirectToLogin of the file AccessControlFilter.java of the component Host Header Handler. This manipulation of the argument Hostname causes open redirect. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available.	3.5	More Details
CVE-2026-0798	Gitea may send release notification emails for private repositories to users whose access has been revoked. When a repository is changed from public to private, users who previously watched the repository may continue to receive release notifications, potentially disclosing release titles, tags, and content.	3.5	More Details
CVE-2026-1421	A vulnerability has been found in code-projects Online Examination System 1.0. Affected is an unknown function of the component Add Pages. Such manipulation leads to cross site scripting. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details

CVE-2026-24048	Backstage is an open framework for building developer portals, and @backstage/backend-defaults provides the default implementations and setup for a standard Backstage backend app. Prior to versions 0.12.2, 0.13.2, 0.14.1, and 0.15.0, the `FetchUrlReader` component, used by the catalog and other plugins to fetch content from URLs, followed HTTP redirects automatically. This allowed an attacker who controls a host listed in `backend.reading.allow` to redirect requests to internal or sensitive URLs that are not on the allowlist, bypassing the URL allowlist security control. This is a Server-Side Request Forgery (SSRF) vulnerability that could allow access to internal resources, but it does not allow attackers to include additional request headers. This vulnerability is fixed in `@backstage/backend-defaults` version 0.12.2, 0.13.2, 0.14.1, and 0.15.0. Users should upgrade to this version or later. Some workarounds are available. Restrict `backend.reading.allow` to only trusted hosts that you control and that do not issue redirects, ensure allowed hosts do not have open redirect vulnerabilities, and/or use network-level controls to block access from Backstage to sensitive internal endpoints.	3.5	More Details
CVE-2026-22281	Dell PowerScale OneFS, versions 9.5.0.0 through 9.5.1.5, versions 9.6.0.0 through 9.7.1.10, versions 9.8.0.0 through 9.10.1.3, versions starting from 9.11.0.0 and prior to 9.13.0.0, contains a Time-of-check Time-of-use (TOCTOU) race condition vulnerability. A low privileged attacker with adjacent network access could potentially exploit this vulnerability, leading to denial of service.	3.5	More Details
CVE-2026-1417	A weakness has been identified in GPAC up to 2.4.0. Affected by this issue is the function dump_isom_rtp of the file applications/mp4box/filedump.c. This manipulation causes null pointer dereference. The attack needs to be launched locally. The exploit has been made available to the public and could be used for attacks. Patch name: f96bd57c3ccdcde4335a0be28cd3e8fe296993de. Applying a patch is the recommended action to fix this issue.	3.3	More Details
CVE-2026-1415	A vulnerability was identified in GPAC up to 2.4.0. Affected is the function gf_media_export_webvtt_metadata of the file src/media_tools/media_export.c. The manipulation of the argument Name leads to null pointer dereference. The attack must be carried out locally. The exploit is publicly available and might be used. The identifier of the patch is af951b892dfbaaa38336ba2eba6d6a42c25810fd. To fix this issue, it is recommended to deploy a patch.	3.3	More Details
CVE-2026-1416	A security flaw has been discovered in GPAC up to 2.4.0. Affected by this vulnerability is the function DumpMovieInfo of the file applications/mp4box/filedump.c. The manipulation results in null pointer dereference. The attack must be initiated from a local position. The exploit has been released to the public and may be used for attacks. The patch is identified as d45c264c20addf0c1cc05124ede33f8ffa800e68. It is advisable to implement a patch to correct this issue.	3.3	More Details
CVE-2026-1190	A flaw was found in Keycloak's SAML brokering functionality. When Keycloak is configured as a client in a Security Assertion Markup Language (SAML) setup, it fails to validate the `NotOnOrAfter` timestamp within the `SubjectConfirmationData`. This allows an attacker to delay the expiration of SAML responses, potentially extending the time a response is considered valid and leading to unexpected session durations or resource consumption.	3.1	More Details
CVE-2026-1035	A flaw was found in the Keycloak server during refresh token processing, specifically in the TokenManager class responsible for enforcing refresh token reuse policies. When strict refresh token rotation is enabled, the validation and update of refresh token usage are not performed atomically. This allows concurrent refresh requests to bypass single-use enforcement and issue multiple access tokens from the same refresh token. As a result, Keycloak’s refresh token rotation hardening can be undermined.	3.1	More Details
CVE-2026-24515	In libexpat before 2.7.4, XML_ExternalEntityParserCreate does not copy unknown encoding handler user data.	2.9	More Details
CVE-2026-1485	A flaw was found in Glib's content type parsing logic. This buffer underflow vulnerability occurs because the length of a header line is stored in a signed integer, which can lead to integer wraparound for very large inputs. This results in pointer underflow and out-of-bounds memory access. Exploitation requires a local user to install or process a specially	2.8	More Details

	crafted treemagic file, which can lead to local denial of service or application instability.		
CVE-2025-14083	A flaw was found in the Keycloak Admin REST API. This vulnerability allows the exposure of backend schema and rules, potentially leading to targeted attacks or privilege escalation via improper access control.	2.7	More Details
CVE-2026-0925	Tanium addressed an improper input validation vulnerability in Discover.	2.7	More Details
CVE-2026-24140	MyTube is a self-hosted downloader and player for several video websites. Versions 1.7.78 and below have a Mass Assignment vulnerability in the settings management functionality due to insufficient input validation. The application's saveSettings() function accepts arbitrary key-value pairs without validating property names against allowed settings. The function uses Record<string, any> as input type and iterates over all entries using Object.entries() without filtering unauthorized properties. Any field sent by the attacker is directly persisted to the database, regardless of whether it corresponds to a legitimate application setting. This issue has been fixed in version 1.7.78.	2.7	More Details
CVE-2026-1444	A vulnerability has been found in iJason-Liu Books_Manager up to 298ba736387ca37810466349af13a0fdf828e99c. This affects an unknown part of the file controllers/books_center/add_book_check.php. Such manipulation of the argument mark leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	2.4	More Details
CVE-2026-1408	A weakness has been identified in Beetel 777VR1 up to 01.00.09/01.00.09_55. This vulnerability affects unknown code of the component UART Interface. Executing a manipulation can lead to weak password requirements. The physical device can be targeted for the attack. The attack requires a high level of complexity. It is stated that the exploitability is difficult. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2.0	More Details
CVE-2026-1409	A security vulnerability has been detected in Beetel 777VR1 up to 01.00.09/01.00.09_55. This issue affects some unknown processing of the component UART Interface. The manipulation leads to improper restriction of excessive authentication attempts. It is possible to launch the attack on the physical device. The attack's complexity is rated as high. The exploitability is assessed as difficult. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.0	More Details
CVE-2026-1407	A security flaw has been discovered in Beetel 777VR1 up to 01.00.09/01.00.09_55. This affects an unknown part of the component UART Interface. Performing a manipulation results in information disclosure. The attack may be carried out on the physical device. The attack is considered to have high complexity. It is indicated that the exploitability is difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2.0	More Details
CVE-2026-24408	sigstore-python is a Python tool for generating and verifying Sigstore signatures. Prior to version 4.2.0, the sigstore-python OAuth authentication flow is susceptible to Cross-Site Request Forgery. `_OAuthSession` creates a unique "state" and sends it as a parameter in the authentication request but the "state" in the server response seems not not be cross-checked with this value. Version 4.2.0 contains a patch for the issue.	0.0	More Details
CVE-2026-23763	VB-Audio Matrix and Matrix Coconut (versions ending in 1.0.2.2 and 2.0.2.2 and earlier, respectively), contain a local privilege escalation vulnerability in the VBMatrix VAIO virtual audio driver (vbmatrixvaio64*_win10.sys). The driver allocates a 128-byte non-paged pool buffer and, upon receiving IOCTL 0x222060, maps it into user space using an MDL and MmMapLockedPagesSpecifyCache. Because the allocation size is not page-aligned, the mapping exposes the entire 0x1000-byte kernel page containing the buffer plus adjacent non-paged pool allocations with read/write permissions. An unprivileged local attacker can open a device handle (using the required 0x800 attribute flag), invoke the IOCTL to obtain	N/A	More Details

	the mapping, and then read or modify live kernel objects and pointers present on that page. This enables bypass of KASLR, arbitrary kernel memory read/write within the exposed page, corruption of kernel objects, and escalation to SYSTEM.		
CVE-2025-69066	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Indoor Plants indoor-plants allows PHP Local File Inclusion.This issue affects Indoor Plants: from n/a through <= 1.2.7.	N/A	More Details
CVE-2025-41082	Illegal HTTP request traffic vulnerability (CL.0) in Altitude Communication Server, caused by inconsistent analysis of multiple HTTP requests over a single Keep-Alive connection using Content-Length headers. This can cause a desynchronization of requests between frontend and backend servers, which could allow request hiding, cache poisoning or security bypass.	N/A	More Details
CVE-2026-24400	AssertJ provides Fluent testing assertions for Java and the Java Virtual Machine (JVM). Starting in version 1.4.0 and prior to version 3.27.7, an XML External Entity (XXE) vulnerability exists in `org.assertj.core.util.xml.XmlStringPrettyFormatter`: the `toXmlDocument(String)` method initializes `DocumentBuilderFactory` with default settings, without disabling DTDs or external entities. This formatter is used by the `isXmlEqualTo(CharSequence)` assertion for `CharSequence` values. An application is vulnerable only when it uses untrusted XML input with either `isXmlEqualTo(CharSequence)` from `org.assertj.core.api.AbstractCharSequenceAssert` or `xmlPrettyFormat(String)` from `org.assertj.core.util.xml.XmlStringPrettyFormatter`. If untrusted XML input is processed by tone of these methods, an attacker couldnread arbitrary local files via `file://` URIs (e.g., `/etc/passwd`, application configuration files); perform Server-Side Request Forgery (SSRF) via HTTP/HTTPS URIs, and/or cause Denial of Service via "Billion Laughs" entity expansion attacks. `isXmlEqualTo(CharSequence)` has been deprecated in favor of XMLUnit in version 3.18.0 and will be removed in version 4.0. Users of affected versions should, in order of preference: replace `isXmlEqualTo(CharSequence)` with XMLUnit, upgrade to version 3.27.7, or avoid using `isXmlEqualTo(CharSequence)` or `XmlStringPrettyFormatter` with untrusted input. `XmlStringPrettyFormatter` has historically been considered a utility for `isXmlEqualTo(CharSequence)` rather than a feature for AssertJ users, so it is deprecated in version 3.27.7 and removed in version 4.0, with no replacement.	N/A	More Details
CVE-2026-23764	VB-Audio Voicemeeter, Voicemeeter Banana, and Voicemeeter Potato (versions ending in 1.1.1.9, 2.1.1.9, and 3.1.1.9 and earlier, respectively), as well as VB-Audio Matrix and Matrix Coconut (versions ending in 1.0.2.2 and 2.0.2.2 and earlier, respectively), contain a vulnerability in their virtual audio drivers (vbvoicemeetervaio64*.sys, vbmatrixvaio64*.sys, vbaudio_vmauxvaio*.sys, vbaudio_vmvaio*.sys, and vbaudio_vmvaio3*.sys). The drivers allocate non-paged pool and map it into user space, where a length value associated with the allocation is exposed and can be modified by an unprivileged local attacker. On subsequent IOCTL handling, the corrupted length is used directly as the IoAllocateMdl length argument without adequate integrity checks before building and mapping the MDL, which can cause a kernel crash (BSoD), typically PAGE_FAULT_IN_NONPAGED_AREA. This flaw allows a local user to trigger a denial-of-service on affected Windows systems.	N/A	More Details
CVE-2023-22926	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2020-8451	Rejected reason: The reserved CVE was never used.	N/A	More Details
CVE-2025-30248	DLL hijacking in the WD Discovery Installer in Western Digital WD Discovery 5.2.730 on Windows allows a local attacker to execute arbitrary code via placement of a crafted dll in the installer's search path.	N/A	More Details
CVE-	Langfuse is an open source large language model engineering platform. In versions 3.146.0 and below, the /api/public/slack/install endpoint initiates Slack OAuth using a projectId provided by the client without authentication or authorization. The projectId is preserved throughout the OAuth flow, and the callback stores installations based on this untrusted		

2026- 24055	metadata. This allows an attacker to bind their Slack workspace to any project and potentially receive changes to prompts stored in Langfuse Prompt Management. An attacker can replace existing Prompt Slack Automation integrations or pre-register a malicious one, though the latter requires an authenticated user to unknowingly configure it despite visible workspace and channel indicators in the UI. This issue has been fixed in version 3.147.0.	N/A	More Details
CVE- 2026- 24131	pnpm is a package manager. Prior to version 10.28.2, when pnpm processes a package's \`directories.bin\` field, it uses \`path.join()\` without validating the result stays within the package root. A malicious npm package can specify \`"directories": {"bin": "../../../../tmp"}\` to escape the package directory, causing pnpm to chmod 755 files at arbitrary locations. This issue only affects Unix/Linux/macOS. Windows is not affected (\`fixBin\` gated by \`EXECUTABLE_SHEBANG_SUPPORTED\`). Version 10.28.2 contains a patch.	N/A	More Details
CVE- 2026- 24056	pnpm is a package manager. Prior to version 10.28.2, when pnpm installs a \`file:\` (directory) or \`git:\` dependency, it follows symlinks and reads their target contents without constraining them to the package root. A malicious package containing a symlink to an absolute path (e.g., \`/etc/passwd\`, \`~/.ssh/id_rsa\`) causes pnpm to copy that file's contents into \`node_modules\`, leaking local data. The vulnerability only affects \`file:\` and \`git:\` dependencies. Registry packages (npm) have symlinks stripped during publish and are NOT affected. The issue impacts developers installing local/file dependencies andCI/CD pipelines installing git dependencies. It can lead to credential theft via symlinks to \`~/.aws/credentials\`, \`~/.npmrc\`, \`~/.ssh/id_rsa\`. Version 10.28.2 contains a patch.	N/A	More Details
CVE- 2022- 32150	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE- 2023- 22925	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE- 2022- 43560	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE- 2025- 69067	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Tails tails allows PHP Local File Inclusion.This issue affects Tails: from n/a through <= 1.4.12.	N/A	More Details
CVE- 2025- 69072	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Prider prider allows PHP Local File Inclusion.This issue affects Prider: from n/a through <= 1.1.3.1.	N/A	More Details
CVE- 2025- 9520	An IDOR vulnerability exists in Omada Controllers that allows an attacker with Administrator permissions to manipulate requests and potentially hijack the Owner account.	N/A	More Details
CVE- 2022- 43559	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE- 2026- 23761	VB-Audio Voicemeeter, Voicemeeter Banana, and Voicemeeter Potato (versions ending in 1.1.1.9, 2.1.1.9, and 3.1.1.9 and earlier, respectively), as well as VB-Audio Matrix and Matrix Coconut (versions ending in 1.0.2.2 and 2.0.2.2 and earlier, respectively), contain a vulnerability in their virtual audio drivers (vbvoicemeetervaio64*.sys, vbmatrixvaio64*.sys, vbaudio_vmauxvaio*.sys, vbaudio_vmvaio*.sys, and vbaudio_vmvaio3*.sys). When a handle is opened with a special file attribute value, the drivers improperly initialize FILE_OBJECT->FsContext to a non-pointer magic value. If subsequent operations are not handled by the VB-Audio driver and are forwarded down the audio driver stack (e.g., via PortCls to ks.sys), the invalid FsContext value can be dereferenced, causing a kernel crash (BSoD), typically SYSTEM_SERVICE_EXCEPTION with STATUS_ACCESS_VIOLATION. This flaw allows a local unprivileged user to trigger a denial-of-service on affected Windows systems.	N/A	More Details

CVE-2025-9521	Password Confirmation Bypass vulnerability in Omada Controllers, allowing an attacker with a valid session token to bypass secondary verification, and change the user’s password without proper confirmation, leading to weakened account security.	N/A	More Details
CVE-2025-9522	Blind Server-Side Request Forgery (SSRF) in Omada Controllers through webhook functionality, enabling crafted requests to internal services, which may lead to enumeration of information.	N/A	More Details
CVE-2025-9615	A flaw was found in NetworkManager. The NetworkManager package allows access to files that may belong to other users. NetworkManager allows non-root users to configure the system's network. The daemon runs with root privileges and can access files owned by users different from the one who added the connection.	N/A	More Details
CVE-2022-34214	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2026-24001	jsdiff is a JavaScript text differencing implementation. Prior to versions 8.0.3, 5.2.2, and 4.0.4, attempting to parse a patch whose filename headers contain the line break characters `\r`, `\u2028`, or `\u2029` can cause the `parsePatch` method to enter an infinite loop. It then consumes memory without limit until the process crashes due to running out of memory. Applications are therefore likely to be vulnerable to a denial-of-service attack if they call `parsePatch` with a user-provided patch as input. A large payload is not needed to trigger the vulnerability, so size limits on user input do not provide any protection. Furthermore, some applications may be vulnerable even when calling `parsePatch` on a patch generated by the application itself if the user is nonetheless able to control the filename headers (e.g. by directly providing the filenames of the files to be diffed). The `applyPatch` method is similarly affected if (and only if) called with a string representation of a patch as an argument, since under the hood it parses that string using `parsePatch`. Other methods of the library are unaffected. Finally, a second and lesser interdependent bug - a ReDOS - also exhibits when those same line break characters are present in a patch's *patch* header (also known as its "leading garbage"). A maliciously-crafted patch header of length *n* can take `parsePatch` O(*n*^{3}) time to parse. Versions 8.0.3, 5.2.2, and 4.0.4 contain a fix. As a workaround, do not attempt to parse patches that contain any of these characters: `\r`, `\u2028`, or `\u2029`.	N/A	More Details
CVE-2026-22696	dcap-qvl implements the quote verification logic for DCAP (Data Center Attestation Primitives). A vulnerability present in versions prior to 0.3.9 involves a critical gap in the cryptographic verification process within the dcap-qvl. The library fetches QE Identity collateral (including qe_identity, qe_identity_signature, and qe_identity_issuer_chain) from the PCCS. However, it skips to verify the QE Identity signature against its certificate chain and does not enforce policy constraints on the QE Report. An attacker can forge the QE Identity data to whitelist a malicious or non-Intel Quoting Enclave. This allows the attacker to forge the QE and sign untrusted quotes that the verifier will accept as valid. Effectively, this bypasses the entire remote attestation security model, as the verifier can no longer trust the entity responsible for signing the quotes. All deployments utilizing the dcap-qvl library for SGX or TDX quote verification are affected. The vulnerability has been patched in dcap-qvl version 0.3.9. The fix implements the missing cryptographic verification for the QE Identity signature and enforces the required checks for MRSIGNER, ISVPRODID, and ISVSVN against the QE Report. Users of the `@phala/dcap-qvl-node` and `@phala/dcap-qvl-web` packages should switch to the pure JavaScript implementation, `@phala/dcap-qvl`. There are no known workarounds for this vulnerability. Users must upgrade to the patched version to ensure that QE Identity collateral is properly verified.	N/A	More Details
CVE-2025-59473	SQL Injection vulnerability in the Structure for Admin authenticated user	N/A	More Details
CVE-2022-43558	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details

CVE-2026-24010	Horilla is a free and open source Human Resource Management System (HRMS). A critical File Upload vulnerability in versions prior to 1.5.0, with Social Engineering, allows authenticated users to deploy phishing attacks. By uploading a malicious HTML file disguised as a profile picture, an attacker can create a convincing login page replica that steals user credentials. When a victim visits the uploaded file URL, they see an authentic-looking "Session Expired" message prompting them to re-authenticate. All entered credentials are captured and sent to the attacker's server, enabling Account Takeover. Version 1.5.0 patches the issue.	N/A	More Details
CVE-2026-23762	VB-Audio Voicemeeter, Voicemeeter Banana, and Voicemeeter Potato (versions ending in 1.1.1.9, 2.1.1.9, and 3.1.1.9 and earlier, respectively), as well as VB-Audio Matrix and Matrix Coconut (versions ending in 1.0.2.2 and 2.0.2.2 and earlier, respectively), contain a vulnerability in their virtual audio drivers (vbvoicemeetervaio64*.sys, vbmatrixvaio64*.sys, vbaudio_vmauxvaio*.sys, vbaudio_vmvaio*.sys, and vbaudio_vmvaio3*.sys). The drivers map non-paged pool memory into user space via MmMapLockedPagesSpecifyCache using UserMode access without proper exception handling. If the mapping fails, such as when a process has exhausted available virtual address space, MmMapLockedPagesSpecifyCache raises an exception that is not caught, causing a kernel crash (BSoD), typically SYSTEM_SERVICE_EXCEPTION with STATUS_NO_MEMORY. This flaw allows a local unprivileged user to trigger a denial-of-service on affected Windows systems.	N/A	More Details
CVE-2025-41083	Vulnerability in Altitude Authentication Service and Altitude Communication Server v8.5.3290.0 by Altitude, where manipulation of Host header in HTTP requests allows redirection to an arbitrary URL or modification of the base URL to trick the victim into sending login credentials to a malicious website. This behavior can be used to redirect clients to endpoints controlled by the attacker.	N/A	More Details
CVE-2020-8459	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2025-69071	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes TanTum tantum allows PHP Local File Inclusion.This issue affects TanTum: from n/a through <= 1.1.13.	N/A	More Details
CVE-2020-8452	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2025-59103	The Access Manager 92xx in hardware revision K7 is based on Linux instead of Windows CE embedded in older hardware revisions. In this new hardware revision it was noticed that an SSH service is exposed on port 22. By analyzing the firmware of the devices, it was noticed that there are two users with hardcoded and weak passwords that can be used to access the devices via SSH. The passwords can be also guessed very easily. The password of at least one user is set to a random value after the first deployment, with the restriction that the password is only randomized if the configured date is prior to 2022. Therefore, under certain circumstances, the passwords are not randomized. For example, if the clock is never set on the device, the battery of the clock module has been changed, the Access Manager has been factory reset and has not received a time yet.	N/A	More Details
CVE-2025-59104	With physical access to the device and enough time an attacker is able to solder test leads to the debug footprint (or use the 6-Pin tag-connect cable). Thus, the attacker gains access to the bootloader, where the kernel command line can be changed. An attacker is able to gain a root shell through this vulnerability.	N/A	More Details
CVE-2025-59105	With physical access to the device and enough time an attacker can desolder the flash memory, modify it and then reinstall it because of missing encryption. Thus, essential files, such as "/etc/passwd", as well as stored certificates, cryptographic keys, stored PINs and so on can be modified and read, in order to gain SSH root access on the Linux-based K7 model. On the Windows CE based K5 model, the password for the Access Manager can additionally be read in plain text from the stored SQLite database.	N/A	More Details

CVE-2022-24911	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2025-59107	Dormakaba provides the software FWServiceTool to update the firmware version of the Access Managers via the network. The firmware in some instances is provided in an encrypted ZIP file. Within this tool, the password used to decrypt the ZIP and extract the firmware is set statically and can be extracted. This password was valid for multiple observed firmware versions.	N/A	More Details
CVE-2025-69070	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Tornados tornados allows PHP Local File Inclusion.This issue affects Tornados: from n/a through <= 2.1.	N/A	More Details
CVE-2025-59108	By default, the password for the Access Manager's web interface, is set to 'admin'. In the tested version changing the password was not enforced.	N/A	More Details
CVE-2020-8453	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2025-59109	The dormakaba registration units 9002 (PIN Pad Units) have an exposed UART header on the backside. The PIN pad is sending every button press to the UART interface. An attacker can use the interface to exfiltrate PINs. As the devices are explicitly built as Plug-and-Play to be easily replaced, an attacker is easily able to remove the device, install a hardware implant which connects to the UART and exfiltrates the data exposed via UART to another system (e.g. via WiFi).	N/A	More Details
CVE-2026-23959	CoreShop is a Pimcore enhanced eCommerce solution. An error-based SQL Injection vulnerability was identified in versions prior to 4.1.9 in the `CustomerTransformerController` within the CoreShop admin panel. The affected endpoint improperly interpolates user-supplied input into a SQL query, leading to database error disclosure and potential data extraction. Version 4.1.9 fixes the issue.	N/A	More Details
CVE-2022-24380	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2020-8454	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2020-8455	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2022-22147	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2022-21130	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2020-8456	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2020-8457	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-			

2020-8458	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2025-69068	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Muji muji allows PHP Local File Inclusion.This issue affects Muji: from n/a through <= 1.2.0.	N/A	More Details
CVE-2021-3926	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2020-8460	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2025-59102	The web server of the Access Manager offers a functionality to download a backup of the local database stored on the device. This database contains the whole configuration. This includes encrypted MIFARE keys, card data, user PINs and much more. The PINs are even stored unencrypted. Combined with the fact that an attacker can easily get access to the backup functionality by abusing the session management issue (CVE-2025-59101), or by exploiting the weak default password (CVE-2025-59108), or by simply setting a new password without prior authentication via the SOAP API (CVE-2025-59097), it is easily possible to access the sensitive data on the device.	N/A	More Details
CVE-2025-59101	Instead of typical session tokens or cookies, it is verified on a per-request basis if the originating IP address has once successfully logged in. As soon as an authentication request from a certain source IP is successful, the IP address is handled as authenticated. No other session information is stored. Therefore, it is possible to spoof the IP address of a logged-in user to gain access to the Access Manager web interface.	N/A	More Details
CVE-2025-14756	Command injection vulnerability was found in the admin interface component of TP-Link Archer MR600 v5 firmware, allowing authenticated attackers to execute system commands with a limited character length via crafted input in the browser developer console, possibly leading to service disruption or full compromise.	N/A	More Details
CVE-2025-59100	The web interface offers a functionality to export the internal SQLite database. After executing the database export, an automatic download is started and the device reboots. After rebooting, the exported database is deleted and cannot be accessed anymore. However, it was noticed that sometimes the device does not reboot and therefore the exported database is not deleted, or the device reboots and the export is not deleted for unknown reasons. The path where the database export is located can be accessed without prior authentication. This leads to the fact that an attacker might be able to get access to the exported database without prior authentication. The database includes sensitive data like passwords, card pins, encrypted Mifare sitekeys and much more.	N/A	More Details
CVE-2026-24440	Shenzhen Tenda W30E V2 firmware versions up to and including V16.01.0.19(5037) allow account passwords to be changed through the maintenance interface without requiring verification of the existing password. This enables unauthorized password changes when access to the affected endpoint is obtained.	N/A	More Details
CVE-2026-24439	Shenzhen Tenda W30E V2 firmware versions up to and including V16.01.0.19(5037) fail to include the X-Content-Type-Options: nosniff response header on web management interfaces. As a result, browsers that perform MIME sniffing may incorrectly interpret attacker-influenced responses as executable script.	N/A	More Details
CVE-2026-24437	Shenzhen Tenda W30E V2 firmware versions up to and including V16.01.0.19(5037) serve sensitive administrative content without appropriate cache-control directives. As a result, browsers may store credential-bearing responses locally, exposing them to subsequent unauthorized access.	N/A	More Details
CVE-2026-	Shenzhen Tenda W30E V2 firmware versions up to and including V16.01.0.19(5037) do not enforce rate limiting or account lockout mechanisms on authentication endpoints. This allows attackers to perform unrestricted brute-force attempts against administrative	N/A	More Details

24436	credentials.		
CVE-2025-59090	On the exos 9300 server, a SOAP API is reachable on port 8002. This API does not require any authentication prior to sending requests. Therefore, network access to the exos server allows e.g. the creation of arbitrary access log events as well as querying the 2FA PINs associated with the enrolled chip cards.	N/A	More Details
CVE-2026-24433	Shenzhen Tenda W30E V2 firmware versions up to and including V16.01.0.19(5037) contain a stored cross-site scripting vulnerability in the user creation functionality. Insufficient input validation allows attacker-controlled script content to be stored and later executed when administrative users access the affected management pages.	N/A	More Details
CVE-2025-59091	Multiple hardcoded credentials have been identified, which are allowed to sign-in to the exos 9300 datapoint server running on port 1004 and 1005. This server is used for relaying status information from and to the Access Managers. This information, among other things, is used to graphically visualize open doors and alerts. However, controlling the Access Managers via this interface is also possible. To send and receive status information, authentication is necessary. The Kaba exos 9300 application contains hard-coded credentials for four different users, which are allowed to login to the datapoint server and receive as well as send information, including commands to open arbitrary doors.	N/A	More Details
CVE-2026-24432	Shenzhen Tenda W30E V2 firmware versions up to and including V16.01.0.19(5037) lack cross-site request forgery (CSRF) protections on administrative endpoints, including those used to change administrator account credentials. As a result, an attacker can craft malicious requests that, when triggered by an authenticated user’s browser, modify administrative passwords and other configuration settings.	N/A	More Details
CVE-2026-24431	Shenzhen Tenda W30E V2 firmware versions up to and including V16.01.0.19(5037) display stored user account passwords in plaintext within the administrative web interface. Any user with access to the affected management pages can directly view credentials.	N/A	More Details
CVE-2025-59092	An RPC service, which is part of exos 9300, is reachable on port 4000, run by the process FSMobilePhoneInterface.exe. This service is used for interprocess communication between services and the Kaba exos 9300 GUI, containing status information about the Access Managers. Interacting with the service does not require any authentication. Therefore, it is possible to send arbitrary status information about door contacts etc. without prior authentication.	N/A	More Details
CVE-2025-59093	Exos 9300 instances are using a randomly generated database password to connect to the configured MSSQL server. The password is derived from static random values, which are concatenated to the hostname and a random string that can be read by every user from the registry. This allows an attacker to derive the database password and get authenticated access to the central exos 9300 database as the user Exos9300Common. The user has the roles ExosDialog and ExosDialogDotNet assigned, which are able to read most tables of the database as well as update and insert into many tables.	N/A	More Details
CVE-2026-24430	Shenzhen Tenda W30E V2 firmware versions up to and including V16.01.0.19(5037) disclose sensitive account credentials in cleartext within HTTP responses generated by the maintenance interface. Because the management interface is accessible over unencrypted HTTP by default, credentials may be exposed to network-based interception.	N/A	More Details
CVE-2025-59094	A local privilege escalation vulnerability has been identified in the Kaba exos 9300 System management application (d9sysdef.exe). Within this application it is possible to specify an arbitrary executable as well as the weekday and start time, when the specified executable should be run with SYSTEM privileges.	N/A	More Details
CVE-2026-24429	Shenzhen Tenda W30E V2 firmware versions up to and including V16.01.0.19(5037) ship with a predefined default password for a built-in authentication account that is not required to be changed during initial configuration. An attacker can leverage these default credentials to gain authenticated access to the management interface.	N/A	More Details
CVE-	Shenzhen Tenda W30E V2 firmware versions up to and including V16.01.0.19(5037) contain an authorization flaw in the user management API that allows a low-privileged		More

2026-24428	authenticated user to change the administrator account password. By sending a crafted request directly to the backend endpoint, an attacker can bypass role-based restrictions enforced by the web interface and obtain full administrative privileges.	N/A	Details
CVE-2025-59095	The program libraries (DLL) and binaries used by exos 9300 contain multiple hard-coded secrets. One notable example is the function "EncryptAndDecrypt" in the library Kaba.EXOS.common.dll. This algorithm uses a simple XOR encryption technique combined with a cryptographic key (cryptoKey) to transform each character of the input string. However, it's important to note that this implementation does not provide strong encryption and should not be considered secure for sensitive data. It's more of a custom encryption approach rather than a common algorithm used in cryptographic applications. The key itself is static and based on the founder's name of the company. The functionality is for example used to encrypt the user PINs before storing them in the MSSQL database.	N/A	More Details
CVE-2025-59096	The default password for the extended admin user mode in the application U9ExosAdmin.exe ("Kaba 9300 Administration") is hard-coded in multiple locations as well as documented in the locally stored user documentation.	N/A	More Details
CVE-2025-59097	The exos 9300 application can be used to configure Access Managers (e.g. 92xx, 9230 and 9290). The configuration is done in a graphical user interface on the dormakaba exos server. As soon as the save button is clicked in exos 9300, the whole configuration is sent to the selected Access Manager via SOAP. The SOAP request is sent without any prior authentication or authorization by default. Though authentication and authorization can be configured using IPsec for 92xx-K5 devices and mTLS for 92xx-K7 devices, it is not enabled by default and must therefore be activated with additional steps. This insecure default allows an attacker with network level access to completely control the whole environment. An attacker is for example easily able to conduct the following tasks without prior authentication: - Re-configure Access Managers (e.g. remove alarming system requirements) - Freely re-configure the inputs and outputs - Open all connected doors permanently - Open all doors for a defined time interval - Change the admin password - and many more Network level access can be gained due to an insufficient network segmentation as well as missing LAN firewalls. Devices with an insecure configuration have been identified to be directly exposed to the internet.	N/A	More Details
CVE-2025-71178	Crucial Storage Executive installer versions prior to 11.08.082025.00 contain a DLL preloading vulnerability. During installation, the installer runs with elevated privileges and loads Windows DLLs using an uncontrolled search path, which can cause a malicious DLL placed alongside the installer to be loaded instead of the intended system library. A local attacker who can convince a victim to run the installer from a directory containing the attacker-supplied DLL can achieve arbitrary code execution with administrator privileges.	N/A	More Details
CVE-2025-59098	The Access Manager is offering a trace functionality to debug errors and issues with the device. The trace functionality is implemented as a simple TCP socket. A tool called TraceClient.exe, provided by dormakaba via the Access Manager web interface, is used to connect to the socket and receive debug information. The data is permanently broadcasted on the TCP socket. The socket can be accessed without any authentication or encryption. The transmitted data is based on the set verbosity level. The verbosity level can be set using the http(s) endpoint with the service interface password or with the guessable identifier of the device via the SOAP interface. The transmitted data contains sensitive data like the Card ID as well as all button presses on Registration units. This allows an attacker with network level access to retrieve all entered PINs on a registration unit.	N/A	More Details
CVE-2025-59099	The Access Manager is using the open source web server CompactWebServer written in C#. This web server is affected by a path traversal vulnerability, which allows an attacker to directly access files via simple GET requests without prior authentication. Hence, it is possible to retrieve all files stored on the file system, including the SQLite database Database.sq3, containing badge information and the corresponding PIN codes. Additionally, when trying to access certain files, the web server crashes and becomes unreachable for about 60 seconds. This can be abused to continuously send the request and cause denial of service.	N/A	More Details
	Shenzhen Tenda W30E V2 firmware versions up to and including V16.01.0.19(5037)		

CVE-2026-24435	implement an insecure Cross-Origin Resource Sharing (CORS) policy on authenticated administrative endpoints. The device sets Access-Control-Allow-Origin: * in combination with Access-Control-Allow-Credentials: true, allowing attacker-controlled origins to issue credentialed cross-origin requests.	N/A	More Details
CVE-2026-0759	Katana Network Development Starter Kit executeCommand Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Katana Network Development Starter Kit. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the executeCommand method. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-27786.	N/A	More Details
CVE-2026-24476	Shaarli is a personal bookmarking service. Prior to version 0.16.0, crafting a malicious tag which starting with `"` prematurely ends the `<input>` tag on the start page and allows an attacker to add arbitrary html leading to a possible XSS attack. Version 0.16.0 fixes the issue.	N/A	More Details
CVE-2026-1474	An out-of-band SQL injection vulnerability (OOB SQLi) has been detected in the Performance Evaluation (EDD) application developed by Gabinete Técnico de Programación. Exploiting this vulnerability in the parameter 'Id_usuario' and 'Id_evaluacion' en ‘/evaluacion_inicio.aspx’, could allow an attacker to extract sensitive information from the database through external channels, without the affected application returning the data directly, compromising the confidentiality of the stored information.	N/A	More Details
CVE-2025-69562	code-projects Mobile Shop Management System 1.0 is vulnerable to SQL Injection in /insertmessage.php via the userid parameter.	N/A	More Details
CVE-2025-69563	code-projects Mobile Shop Management System 1.0 is vulnerable to SQL Injection in /ExLogin.php via the Password parameter.	N/A	More Details
CVE-2025-69564	code-projects Mobile Shop Management System 1.0 is vulnerable to SQL Injection in /ExAddNewUser.php via the Name, Address, email, UserName, Password, confirm_password, Role, Branch, and Activate parameters.	N/A	More Details
CVE-2026-0705	Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis Cloud Manager (Windows) before build 6.4.25342.354.	N/A	More Details
CVE-2026-1472	An out-of-band SQL injection vulnerability (OOB SQLi) has been detected in the Performance Evaluation (EDD) application developed by Gabinete Técnico de Programación. Exploiting this vulnerability in the parameter 'txAny' in '/evaluacion_competencias_autoeval_list.aspx', could allow an attacker to extract sensitive information from the database through external channels, without the affected application returning the data directly, compromising the confidentiality of the stored information.	N/A	More Details
CVE-2026-1473	An out-of-band SQL injection vulnerability (OOB SQLi) has been detected in the Performance Evaluation (EDD) application developed by Gabinete Técnico de Programación. Exploiting this vulnerability in the parameter 'Id_usuario’ in '/evaluacion_competencias_evalua.aspx', could allow an attacker to extract sensitive information from the database through external channels, without the affected application returning the data directly, compromising the confidentiality of the stored information.	N/A	More Details
CVE-2026-1475	An out-of-band SQL injection vulnerability (OOB SQLi) has been detected in the Performance Evaluation (EDD) application developed by Gabinete Técnico de Programación. Exploiting this vulnerability in the parameter ‘Id_usuario' in ‘/evaluacion_acciones_evalua.aspx’, could allow an attacker to extract sensitive information from the database through external channels, without the affected application returning the data directly, compromising the confidentiality of the stored information.	N/A	More Details
	ArduinoCore-avr contains the source code and configuration files of the Arduino AVR		

CVE-2025-69209	Boards platform. A vulnerability in versions prior to 1.8.7 allows an attacker to trigger a stack-based buffer overflow when converting floating-point values to strings with high precision. By passing very large `decimalPlaces` values to the affected String constructors or concat methods, the `dtostrf` function writes beyond fixed-size stack buffers, causing memory corruption and denial of service. Under specific conditions, this could enable arbitrary code execution on AVR-based Arduino boards. ### Patches - The Fix is included starting from the `1.8.7` release available from the following link [ArduinoCore-avr v1.8.7](https://github.com/arduino/ArduinoCore-avr) - The Fixing Commit is available at the following link [1a6a417f89c8901dad646efce74ae9d3ddebfd59](https://github.com/arduino/ArduinoCore-avr/pull/613/commits/1a6a417f89c8901dad646efce74ae9d3ddebfd59) ### References - [ASEC-26-001 ArduinoCore-avr vXXXX Resolves Buffer Overflow Vulnerability](https://support.arduino.cc/hc/en-us/articles/XXXXX) ### Credits - Maxime Rossi Bellom and Ramtine Tofighi Shirazi from SecMate (https://secmate.dev/)	N/A	More Details
CVE-2026-1476	An out-of-band SQL injection vulnerability (OOB SQLi) has been detected in the Performance Evaluation (EDD) application developed by Gabinete Técnico de Programación. Exploiting this vulnerability in the parameter 'Id_usuario' in '/evaluacion_acciones_ver_auto.aspx', could allow an attacker to extract sensitive information from the database through external channels, without the affected application returning the data directly, compromising the confidentiality of the stored information.	N/A	More Details
CVE-2026-1477	An out-of-band SQL injection vulnerability (OOB SQLi) has been detected in the Performance Evaluation (EDD) application developed by Gabinete Técnico de Programación. Exploiting this vulnerability in the parameter 'Id_usuario' and 'Id_evaluacion' in '/evaluacion_competencias_evalua_old.aspx', could allow an attacker to extract sensitive information from the database through external channels, without the affected application returning the data directly, compromising the confidentiality of the stored information.	N/A	More Details
CVE-2026-1478	An out-of-band SQL injection vulnerability (OOB SQLi) has been detected in the Performance Evaluation (EDD) application developed by Gabinete Técnico de Programación. Exploiting this vulnerability in the parameter 'Id_usuario' and 'Id_evaluacion' in '/evaluacion_hca_evalua.aspx', could allow an attacker to extract sensitive information from the database through external channels, without the affected application returning the data directly, compromising the confidentiality of the stored information.	N/A	More Details
CVE-2026-1479	An out-of-band SQL injection vulnerability (OOB SQLi) has been detected in the Performance Evaluation (EDD) application developed by Gabinete Técnico de Programación. Exploiting this vulnerability in the parameters 'Id_usuario' and 'Id_evaluacion' in '/evaluacion_hca_ver_auto.asp', could allow an attacker to extract sensitive information from the database through external channels, without the affected application returning the data directly, compromising the confidentiality of the stored information.	N/A	More Details
CVE-2026-1480	An out-of-band SQL injection vulnerability (OOB SQLi) has been detected in the Performance Evaluation (EDD) application developed by Gabinete Técnico de Programación. Exploiting this vulnerability in the parameter 'Id_usuario' in '/evaluacion_objetivos_anyo_sig_evalua.aspx', could allow an attacker to extract sensitive information from the database through external channels, without the affected application returning the data directly, compromising the confidentiality of the stored information.	N/A	More Details
CVE-2026-1481	An out-of-band SQL injection vulnerability (OOB SQLi) has been detected in the Performance Evaluation (EDD) application developed by Gabinete Técnico de Programación. Exploiting this vulnerability in the parameter 'Id_usuario' in '/evaluacion_objetivos_anyo_sig_ver_auto.aspx', could allow an attacker to extract sensitive information from the database through external channels, without the affected application returning the data directly, compromising the confidentiality of the stored information.	N/A	More Details
CVE-2025-69559	code-projects Computer Book Store 1.0 is vulnerable to File Upload in admin_add.php.	N/A	More Details

CVE-2026-24871	Improper Control of Generation of Code ('Code Injection') vulnerability in pilgrimage233 Minecraft-Rcon-Manage.This issue affects Minecraft-Rcon-Manage: before 3.0.	N/A	More Details
CVE-2025-15467	Issue summary: Parsing CMS AuthEnvelopedData message with maliciously crafted AEAD parameters can trigger a stack buffer overflow. Impact summary: A stack buffer overflow may lead to a crash, causing Denial of Service, or potentially remote code execution. When parsing CMS AuthEnvelopedData structures that use AEAD ciphers such as AES-GCM, the IV (Initialization Vector) encoded in the ASN.1 parameters is copied into a fixed-size stack buffer without verifying that its length fits the destination. An attacker can supply a crafted CMS message with an oversized IV, causing a stack-based out-of-bounds write before any authentication or tag verification occurs. Applications and services that parse untrusted CMS or PKCS#7 content using AEAD ciphers (e.g., S/MIME AuthEnvelopedData with AES-GCM) are vulnerable. Because the overflow occurs prior to authentication, no valid key material is required to trigger it. While exploitability to remote code execution depends on platform and toolchain mitigations, the stack-based write primitive represents a severe risk. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the CMS implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3 and 3.0 are vulnerable to this issue. OpenSSL 1.1.1 and 1.0.2 are not affected by this issue.	N/A	More Details
CVE-2025-69418	Issue summary: When using the low-level OCB API directly with AES-NI or other hardware-accelerated code paths, inputs whose length is not a multiple of 16 bytes can leave the final partial block unencrypted and unauthenticated. Impact summary: The trailing 1-15 bytes of a message may be exposed in cleartext on encryption and are not covered by the authentication tag, allowing an attacker to read or tamper with those bytes without detection. The low-level OCB encrypt and decrypt routines in the hardware-accelerated stream path process full 16-byte blocks but do not advance the input/output pointers. The subsequent tail-handling code then operates on the original base pointers, effectively reprocessing the beginning of the buffer while leaving the actual trailing bytes unprocessed. The authentication checksum also excludes the true tail bytes. However, typical OpenSSL consumers using EVP are not affected because the higher-level EVP and provider OCB implementations split inputs so that full blocks and trailing partial blocks are processed in separate calls, avoiding the problematic code path. Additionally, TLS does not use OCB ciphersuites. The vulnerability only affects applications that call the low-level CRYPTO_ocb128_encrypt() or CRYPTO_ocb128_decrypt() functions directly with non-block-aligned lengths in a single call on hardware-accelerated builds. For these reasons the issue was assessed as Low severity. The FIPS modules in 3.6, 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as OCB mode is not a FIPS-approved algorithm. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0 and 1.1.1 are vulnerable to this issue. OpenSSL 1.0.2 is not affected by this issue.	N/A	More Details
CVE-2025-15469	Issue summary: The 'openssl dgst' command-line tool silently truncates input data to 16MB when using one-shot signing algorithms and reports success instead of an error. Impact summary: A user signing or verifying files larger than 16MB with one-shot algorithms (such as Ed25519, Ed448, or ML-DSA) may believe the entire file is authenticated while trailing data beyond 16MB remains unauthenticated. When the 'openssl dgst' command is used with algorithms that only support one-shot signing (Ed25519, Ed448, ML-DSA-44, ML-DSA-65, ML-DSA-87), the input is buffered with a 16MB limit. If the input exceeds this limit, the tool silently truncates to the first 16MB and continues without signaling an error, contrary to what the documentation states. This creates an integrity gap where trailing bytes can be modified without detection if both signing and verification are performed using the same affected codepath. The issue affects only the command-line tool behavior. Verifiers that process the full message using library APIs will reject the signature, so the risk primarily affects workflows that both sign and verify with the affected 'openssl dgst' command. Streaming digest algorithms for 'openssl dgst' and library users are unaffected. The FIPS modules in 3.5 and 3.6 are not affected by this issue, as the command-line tools are outside the OpenSSL FIPS module boundary. OpenSSL 3.5 and 3.6 are vulnerable to this issue. OpenSSL 3.4, 3.3, 3.0, 1.1.1 and 1.0.2 are not affected by this issue.	N/A	More Details

CVE-2025-28162	Buffer Overflow vulnerability in libpng 1.6.43-1.6.46 allows a local attacker to cause a denial of service via the pngimage with AddressSanitizer (ASan), the program leaks memory in various locations, eventually leading to high memory usage and causing the program to become unresponsive	N/A	More Details
CVE-2025-28164	Buffer Overflow vulnerability in libpng 1.6.43-1.6.46 allows a local attacker to cause a denial of service via png_create_read_struct() function.	N/A	More Details
CVE-2025-55102	A denial-of-service vulnerability exists in the NetX IPv6 component functionality of Eclipse ThreadX NetX Duo. A specially crafted network packet of "Packet Too Big" with more than 15 different source address can lead to denial of service. An attacker can send a malicious packet to trigger this vulnerability.	N/A	More Details
CVE-2025-66199	Issue summary: A TLS 1.3 connection using certificate compression can be forced to allocate a large buffer before decompression without checking against the configured certificate size limit. Impact summary: An attacker can cause per-connection memory allocations of up to approximately 22 MiB and extra CPU work, potentially leading to service degradation or resource exhaustion (Denial of Service). In affected configurations, the peer-supplied uncompressed certificate length from a CompressedCertificate message is used to grow a heap buffer prior to decompression. This length is not bounded by the max_cert_list setting, which otherwise constrains certificate message sizes. An attacker can exploit this to cause large per-connection allocations followed by handshake failure. No memory corruption or information disclosure occurs. This issue only affects builds where TLS 1.3 certificate compression is compiled in (i.e., not OPENSSL_NO_COMP_ALG) and at least one compression algorithm (brotli, zlib, or zstd) is available, and where the compression extension is negotiated. Both clients receiving a server CompressedCertificate and servers in mutual TLS scenarios receiving a client CompressedCertificate are affected. Servers that do not request client certificates are not vulnerable to client-initiated attacks. Users can mitigate this issue by setting SSL_OP_NO_RX_CERTIFICATE_COMPRESSION to disable receiving compressed certificates. The FIPS modules in 3.6, 3.5, 3.4 and 3.3 are not affected by this issue, as the TLS implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4 and 3.3 are vulnerable to this issue. OpenSSL 3.0, 1.1.1 and 1.0.2 are not affected by this issue.	N/A	More Details
CVE-2025-68160	Issue summary: Writing large, newline-free data into a BIO chain using the line-buffering filter where the next BIO performs short writes can trigger a heap-based out-of-bounds write. Impact summary: This out-of-bounds write can cause memory corruption which typically results in a crash, leading to Denial of Service for an application. The line-buffering BIO filter (BIO_f_linebuffer) is not used by default in TLS/SSL data paths. In OpenSSL command-line applications, it is typically only pushed onto stdout/stderr on VMS systems. Third-party applications that explicitly use this filter with a BIO chain that can short-write and that write large, newline-free data influenced by an attacker would be affected. However, the circumstances where this could happen are unlikely to be under attacker control, and BIO_f_linebuffer is unlikely to be handling non-curated data controlled by an attacker. For that reason the issue was assessed as Low severity. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the BIO implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0, 1.1.1 and 1.0.2 are vulnerable to this issue.	N/A	More Details
CVE-2025-	Issue summary: Calling PKCS12_get_friendlyname() function on a maliciously crafted PKCS#12 file with a BMPString (UTF-16BE) friendly name containing non-ASCII BMP code point can trigger a one byte write before the allocated buffer. Impact summary: The out-of-bounds write can cause a memory corruption which can have various consequences including a Denial of Service. The OPENSSL_uni2utf8() function performs a two-pass conversion of a PKCS#12 BMPString (UTF-16BE) to UTF-8. In the second pass, when emitting UTF-8 bytes, the helper function bmp_to_utf8() incorrectly forwards the remaining UTF-16 source byte count as the destination buffer capacity to UTF8_putc(). For BMP code points above U+07FF, UTF-8 requires three bytes, but the forwarded capacity can be just two bytes. UTF8_putc() then returns -1, and this negative value is added to the output length without validation, causing the length to become negative. The subsequent trailing	N/A	More

69419	NUL byte is then written at a negative offset, causing write outside of heap allocated buffer. The vulnerability is reachable via the public PKCS12_get_friendlyname() API when parsing attacker-controlled PKCS#12 files. While PKCS12_parse() uses a different code path that avoids this issue, PKCS12_get_friendlyname() directly invokes the vulnerable function. Exploitation requires an attacker to provide a malicious PKCS#12 file to be parsed by the application and the attacker can just trigger a one zero byte write before the allocated buffer. For that reason the issue was assessed as Low severity according to our Security Policy. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the PKCS#12 implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0 and 1.1.1 are vulnerable to this issue. OpenSSL 1.0.2 is not affected by this issue.		Details
CVE-2026-24868	Mitigation bypass in the Privacy: Anti-Tracking component. This vulnerability affects Firefox < 147.0.2.	N/A	More Details
CVE-2025-69420	Issue summary: A type confusion vulnerability exists in the TimeStamp Response verification code where an ASN1_TYPE union member is accessed without first validating the type, causing an invalid or NULL pointer dereference when processing a malformed TimeStamp Response file. Impact summary: An application calling TS_RESP_verify_response() with a malformed TimeStamp Response can be caused to dereference an invalid or NULL pointer when reading, resulting in a Denial of Service. The functions ossl_ess_get_signing_cert() and ossl_ess_get_signing_cert_v2() access the signing cert attribute value without validating its type. When the type is not V_ASN1_SEQUENCE, this results in accessing invalid memory through the ASN1_TYPE union, causing a crash. Exploiting this vulnerability requires an attacker to provide a malformed TimeStamp Response to an application that verifies timestamp responses. The TimeStamp protocol (RFC 3161) is not widely used and the impact of the exploit is just a Denial of Service. For these reasons the issue was assessed as Low severity. The FIPS modules in 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the TimeStamp Response implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0 and 1.1.1 are vulnerable to this issue. OpenSSL 1.0.2 is not affected by this issue.	N/A	More Details
CVE-2025-69421	Issue summary: Processing a malformed PKCS#12 file can trigger a NULL pointer dereference in the PKCS12_item_decrypt_d2i_ex() function. Impact summary: A NULL pointer dereference can trigger a crash which leads to Denial of Service for an application processing PKCS#12 files. The PKCS12_item_decrypt_d2i_ex() function does not check whether the oct parameter is NULL before dereferencing it. When called from PKCS12_unpack_p7encdata() with a malformed PKCS#12 file, this parameter can be NULL, causing a crash. The vulnerability is limited to Denial of Service and cannot be escalated to achieve code execution or memory disclosure. Exploiting this issue requires an attacker to provide a malformed PKCS#12 file to an application that processes it. For that reason the issue was assessed as Low severity according to our Security Policy. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the PKCS#12 implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0, 1.1.1 and 1.0.2 are vulnerable to this issue.	N/A	More Details
CVE-2025-69565	code-projects Mobile Shop Management System 1.0 is vulnerable to File Upload in /ExAddProduct.php.	N/A	More Details
CVE-2026-21852	Claude Code is an agentic coding tool. Prior to version 2.0.65, vulnerability in Claude Code's project-load flow allowed malicious repositories to exfiltrate data including Anthropic API keys before users confirmed trust. An attacker-controlled repository could include a settings file that sets ANTHROPIC_BASE_URL to an attacker-controlled endpoint and when the repository was opened, Claude Code would read the configuration and immediately issue API requests before showing the trust prompt, potentially leaking the user's API keys. Users on standard Claude Code auto-update have received this fix already. Users performing manual updates are advised to update to version 2.0.65, which contains a patch, or to the latest version.	N/A	More Details
	Issue summary: An invalid or NULL pointer dereference can happen in an application		

CVE-2026-22795	processing a malformed PKCS#12 file. Impact summary: An application processing a malformed PKCS#12 file can be caused to dereference an invalid or NULL pointer on memory read, resulting in a Denial of Service. A type confusion vulnerability exists in PKCS#12 parsing code where an ASN1_TYPE union member is accessed without first validating the type, causing an invalid pointer read. The location is constrained to a 1-byte address space, meaning any attempted pointer manipulation can only target addresses between 0x00 and 0xFF. This range corresponds to the zero page, which is unmapped on most modern operating systems and will reliably result in a crash, leading only to a Denial of Service. Exploiting this issue also requires a user or application to process a maliciously crafted PKCS#12 file. It is uncommon to accept untrusted PKCS#12 files in applications as they are usually used to store private keys which are trusted by definition. For these reasons, the issue was assessed as Low severity. The FIPS modules in 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the PKCS12 implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0 and 1.1.1 are vulnerable to this issue. OpenSSL 1.0.2 is not affected by this issue.	N/A	More Details
CVE-2025-69285	SQLBot is an intelligent data query system based on a large language model and RAG. Versions prior to 1.5.0 contain a missing authentication vulnerability in the /api/v1/datasource/uploadExcel endpoint, allowing a remote unauthenticated attacker to upload arbitrary Excel/CSV files and inject data directly into the PostgreSQL database. The endpoint is explicitly added to the authentication whitelist, causing the TokenMiddleware to bypass all token validation. Uploaded files are parsed by pandas and inserted into the database via to_sql() with if_exists='replace' mode. The vulnerability has been fixed in v1.5.0. No known workarounds are available.	N/A	More Details
CVE-2026-1482	An out-of-band SQL injection vulnerability (OOB SQLi) has been detected in the Performance Evaluation (EDD) application developed by Gabinete Técnico de Programación. Exploiting this vulnerability in the parameter 'Id_evaluacion' in '/evaluacion_objetivos_evalua_definido.aspx', could allow an attacker to extract sensitive information from the database through external channels, without the affected application returning the data directly, compromising the confidentiality of the stored information.	N/A	More Details
CVE-2026-1483	An out-of-band SQL injection vulnerability (OOB SQLi) has been detected in the Performance Evaluation (EDD) application developed by Gabinete Técnico de Programación. Exploiting this vulnerability in the parameter 'Id_usuario' in '/evaluacion_objetivos_ver_auto.aspx', could allow an attacker to extract sensitive information from the database through external channels, without the affected application returning the data directly, compromising the confidentiality of the stored information.	N/A	More Details
CVE-2025-13465	Lodash versions 4.0.0 through 4.17.22 are vulnerable to prototype pollution in the _.unset and _.omit functions. An attacker can pass crafted paths which cause Lodash to delete methods from global prototypes. The issue permits deletion of properties but does not allow overwriting their original behavior. This issue is patched on 4.17.23	N/A	More Details
CVE-2026-24740	Dozzle is a realtime log viewer for docker containers. Prior to version 9.0.3, a flaw in Dozzle’s agent-backed shell endpoints allows a user restricted by label filters (for example, \`label=env=dev\`) to obtain an interactive root shell in out-of-scope containers (for example, \`env=prod\`) on the same agent host by directly targeting their container IDs. Version 9.0.3 contains a patch for the issue.	N/A	More Details
CVE-2025-12810	Improper Authentication vulnerability in Delinea Inc. Secret Server On-Prem (RPC Password Rotation modules).This issue affects Secret Server On-Prem: 11.8.1, 11.9.6, 11.9.25. A secret with "change password on check in" enabled automatically checks in even when the password change fails after reaching its retry limit. This leaves the secret in an inconsistent state with the wrong password. Remediation: Upgrade to 11.9.47 or later. The secret will remain checked out when the password change fails.	N/A	More Details
CVE-2025-14988	A security issue has been identified in ibaPDA that could allow unauthorized actions on the file system under certain conditions. This may impact the confidentiality, integrity, or availability of the system.	N/A	More Details
CVE-	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to version 4.11.7, Serve static Middleware for the Cloudflare Workers adapter contains		

2026-24473	an information disclosure vulnerability that may allow attackers to read arbitrary keys from the Workers environment. Improper validation of user-controlled paths can result in unintended access to internal asset keys. Version 4.11.7 contains a patch for the issue.	N/A	More Details
CVE-2026-24688	pypdf is a free and open-source pure-python PDF library. An attacker who uses an infinite loop vulnerability that is present in versions prior to 6.6.2 can craft a PDF which leads to an infinite loop. This requires accessing the outlines/bookmarks. This has been fixed in pypdf 6.6.2. If projects cannot upgrade yet, consider applying the changes from PR #3610 manually.	N/A	More Details
CVE-2026-22976	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_qfq: Fix NULL deref when deactivating inactive aggregate in qfq_reset `qfq_class->leaf_qdisc->q.qlen > 0` does not imply that the class itself is active. Two qfq_class objects may point to the same leaf_qdisc. This happens when: 1. one QFQ qdisc is attached to the dev as the root qdisc, and 2. another QFQ qdisc is temporarily referenced (e.g., via qdisc_get() / qdisc_put()) and is pending to be destroyed, as in function tc_new_tfilter. When packets are enqueued through the root QFQ qdisc, the shared leaf_qdisc->q.qlen increases. At the same time, the second QFQ qdisc triggers qdisc_put and qdisc_destroy: the qdisc enters qfq_reset() with its own q->q.qlen == 0, but its class's leaf qdisc->q.qlen > 0. Therefore, the qfq_reset would wrongly deactivate an inactive aggregate and trigger a null-deref in qfq_deactivate_agg: [0.903172] BUG: kernel NULL pointer dereference, address: 0000000000000000 [0.903571] #PF: supervisor write access in kernel mode [0.903860] #PF: error_code(0x0002) - not-present page [0.904177] PGD 10299b067 P4D 10299b067 PUD 10299c067 PMD 0 [0.904502] Oops: Oops: 0002 [#1] SMP NOPTI [0.904737] CPU: 0 UID: 0 PID: 135 Comm: exploit Not tainted 6.19.0-rc3+ #2 NONE [0.905157] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.17.0-0-gb52ca86e094d-prebuilt.qemu.org 04/01/2014 [0.905754] RIP: 0010:qfq_deactivate_agg (include/linux/list.h:992 (discriminator 2) include/linux/list.h:1006 (discriminator 2) net/sched/sch_qfq.c:1367 (discriminator 2) net/sched/sch_qfq.c:1393 (discriminator 2)) [0.906046] Code: 0f 84 4d 01 00 00 48 89 70 18 8b 4b 10 48 c7 c2 ff ff ff ff 48 8b 78 08 48 d3 e2 48 21 f2 48 2b 13 48 8b 30 48 d3 ea 8b 4b 18 0 Code starting with the faulting instruction == 0: 0f 84 4d 01 00 00 je 0x153 6: 48 89 70 18 mov %rsi,0x18(%rax) a: 8b 4b 10 mov 0x10(%rbx),%ecx d: 48 c7 c2 ff ff ff ff mov $0xffffffffffffffff,%rdx 14: 48 8b 78 08 mov 0x8(%rax),%rdi 18: 48 d3 e2 shl %cl,%rdx 1b: 48 21 f2 and %rsi,%rdx 1e: 48 2b 13 sub (%rbx),%rdx 21: 48 8b 30 mov (%rax),%rsi 24: 48 d3 ea shr %cl,%rdx 27: 8b 4b 18 mov 0x18(%rbx),%ecx ... [0.907095] RSP: 0018:ffffc900004a39a0 EFLAGS: 00010246 [0.907368] RAX: ffff8881043a0880 RBX: ffff888102953340 RCX: 0000000000000000 [0.907723] RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 [0.908100] RBP: ffff888102952180 R08: 0000000000000000 R09: 0000000000000000 [0.908451] R10: ffff8881043a0000 R11: 0000000000000000 R12: ffff888102952000 [0.908804] R13: ffff888102952180 R14: ffff8881043a0ad8 R15: ffff8881043a0880 [0.909179] FS: 000000002a1a0380(0000) GS:ffff888196d8d000(0000) knlGS:0000000000000000 [0.909572] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [0.909857] CR2: 0000000000000000 CR3: 000000102993002 CR4: 0000000000772ef0 [0.910247] PKRU: 55555554 [0.910391] Call Trace: [0.910527] <TASK> [0.910638] qfq_reset_qdisc (net/sched/sch_qfq.c:357 net/sched/sch_qfq.c:1485) [0.910826] qdisc_reset (include/linux/skbuff.h:2195 include/linux/skbuff.h:2501 include/linux/skbuff.h:3424 include/linux/skbuff.h:3430 net/sched/sch_generic.c:1036) [0.911040] __qdisc_destroy (net/sched/sch_generic.c:1076) [0.911236] tc_new_tfilter (net/sched/cls_api.c:2447) [0.911447] rtnetlink_rcv_msg (net/core/rtnetlink.c:6958) [0.911663] ? __pfx_rtnetlink_rcv_msg (net/core/rtnetlink.c:6861) [0.911894] netlink_rcv_skb (net/netlink/af_netlink.c:2550) [0.912100] netlink_unicast (net/netlink/af_netlink.c:1319 net/netlink/af_netlink.c:1344) [0.912296] ? __alloc_skb (net/core/skbuff.c:706) [0.912484] netlink_sendmsg (net/netlink/af ---truncated---	N/A	More Details
	gmrtd is a Go library for reading Machine Readable Travel Documents (MRTDs). Prior to version 0.17.2, ReadFile accepts TLVs with lengths that can range up to 4GB, which can cause unconstrained resource consumption in both memory and cpu cycles. ReadFile can consume an extended TLV with lengths well outside what would be available in ICs. It can accept something all the way up to 4GB which would take too many iterations in 256 byte		

CVE-2026-24738	chunks, and would also try to allocate memory that might not be available in constrained environments like phones. Or if an API sends data to ReadFile, the same problem applies. The very small chunked read also locks the goroutine in accepting data for a very large number of iterations. projects using the gmrtd library to read files from NFCs can experience extreme slowdowns or memory consumption. A malicious NFC can just behave like the mock transceiver described above and by just sending dummy bytes as each chunk to be read, can make the receiving thread unresponsive and fill up memory on the host system. Version 0.17.2 patches the issue.	N/A	More Details
CVE-2026-24026	Rejected reason: Not used	N/A	More Details
CVE-2025-12781	When passing data to the b64decode(), standard_b64decode(), and urlsafe_b64decode() functions in the "base64" module the characters "+/" will always be accepted, regardless of the value of "altchars" parameter, typically used to establish an "alternative base64 alphabet" such as the URL safe alphabet. This behavior matches what is recommended in earlier base64 RFCs, but newer RFCs now recommend either dropping characters outside the specified base64 alphabet or raising an error. The old behavior has the possibility of causing data integrity issues. This behavior can only be insecure if your application uses an alternate base64 alphabet (without "+/"). If your application does not use the "altchars" parameter or the urlsafe_b64decode() function, then your application does not use an alternative base64 alphabet. The attached patches DOES NOT make the base64-decode behavior raise an error, as this would be a change in behavior and break existing programs. Instead, the patch deprecates the behavior which will be replaced with the newly recommended behavior in a future version of Python. Users are recommended to mitigate by verifying user-controlled inputs match the base64 alphabet they are expecting or verify that their application would not be affected if the b64decode() functions accepted "+" or "/" outside of altchars.	N/A	More Details
CVE-2026-24748	Kargo manages and automates the promotion of software artifacts. Prior to versions 1.8.7, 1.7.7, and 1.6.3, a bug was found with authentication checks on the `GetConfig()` API endpoint. This allowed unauthenticated users to access this endpoint by specifying an `Authorization` header with any non-empty `Bearer` token value, regardless of validity. This vulnerability did allow for exfiltration of configuration data such as endpoints for connected Argo CD clusters. This data could allow an attacker to enumerate cluster URLs and namespaces for use in subsequent attacks. Additionally, the same bug affected the `RefreshResource` endpoint. This endpoint does not lead to any information disclosure, but could be used by an unauthenticated attacker to perform a denial-of-service style attack against the Kargo API. `RefreshResource` sets an annotation on specific Kubernetes resources to trigger reconciliations. If run on a constant loop, this could also slow down legitimate requests to the Kubernetes API server. This problem has been patched in Kargo versiosn 1.8.7, 1.7.7, and 1.6.3. There are no workarounds for this issue.	N/A	More Details
CVE-2026-24025	Rejected reason: Not used	N/A	More Details
CVE-2026-24024	Rejected reason: Not used	N/A	More Details
CVE-2026-24023	Rejected reason: Not used	N/A	More Details
CVE-2026-24022	Rejected reason: Not used	N/A	More Details
CVE-2026-24021	Rejected reason: Not used	N/A	More Details

CVE-2026-24016	The installer of ServerView Agents for Windows provided by Fsas Technologies Inc. may insecurely load Dynamic Link Libraries. Arbitrary code may be executed with the administrator privilege when the installer is executed.	N/A	More Details
CVE-2026-0663	Denial-of-service vulnerability in M-Files Server versions before 26.1.15632.3 allows an authenticated attacker with vault administrator privileges to crash the M-Files Server process by calling a vulnerable API endpoint.	N/A	More Details
CVE-2026-24116	Wasmtime is a runtime for WebAssembly. Starting in version 29.0.0 and prior to version 36.0.5, 40.0.3, and 41.0.1, on x86-64 platforms with AVX, Wasmtime's compilation of the `f64.copysign` WebAssembly instruction with Cranelift may load 8 more bytes than is necessary. When signals-based-traps are disabled this can result in a uncaught segfault due to loading from unmapped guard pages. With guard pages disabled it's possible for out-of-sandbox data to be loaded, but unless there is another bug in Cranelift this data is not visible to WebAssembly guests. Wasmtime 36.0.5, 40.0.3, and 41.0.1 have been released to fix this issue. Users are recommended to upgrade to the patched versions of Wasmtime. Other affected versions are not patched and users should updated to supported major version instead. This bug can be worked around by enabling signals-based-traps. While disabling guard pages can be a quick fix in some situations, it's not recommended to disabled guard pages as it is a key defense-in-depth measure of Wasmtime.	N/A	More Details
CVE-2026-23892	OctoPrint provides a web interface for controlling consumer 3D printers. OctoPrint versions up to and including 1.11.5 are affected by a (theoretical) timing attack vulnerability that allows API key extraction over the network. Due to using character based comparison that short-circuits on the first mismatched character during API key validation, rather than a cryptographical method with static runtime regardless of the point of mismatch, an attacker with network based access to an affected OctoPrint could extract API keys valid on the instance by measuring the response times of the denied access responses and guess an API key character by character. The vulnerability is patched in version 1.11.6. The likelihood of this attack actually working is highly dependent on the network's latency, noise and similar parameters. An actual proof of concept was not achieved so far. Still, as always administrators are advised to not expose their OctoPrint instance on hostile networks, especially not on the public Internet.	N/A	More Details
CVE-2026-22977	In the Linux kernel, the following vulnerability has been resolved: net: sock: fix hardened usercopy panic in sock_recv_errqueue skbuff_fclone_cache was created without defining a usercopy region, [1] unlike skbuff_head_cache which properly whitelists the cb[] field. [2] This causes a usercopy BUG() when CONFIG_HARDENED_USERCOPY is enabled and the kernel attempts to copy sk_buff.cb data to userspace via sock_recv_errqueue() -> put_cmsg(). The crash occurs when: 1. TCP allocates an skb using alloc_skb_fclone() (from skbuff_fclone_cache) [1] 2. The skb is cloned via skb_clone() using the pre-allocated fclone [3] 3. The cloned skb is queued to sk_error_queue for timestamp reporting 4. Userspace reads the error queue via recvmsg(MSG_ERRQUEUE) 5. sock_recv_errqueue() calls put_cmsg() to copy serr->ee from skb->cb [4] 6. __check_heap_object() fails because skbuff_fclone_cache has no usercopy whitelist [5] When cloned skbs allocated from skbuff_fclone_cache are used in the socket error queue, accessing the sock_exterr_skb structure in skb->cb via put_cmsg() triggers a usercopy hardening violation: [5.379589] usercopy: Kernel memory exposure attempt detected from SLUB object 'skbuff_fclone_cache' (offset 296, size 16)! [5.382796] kernel BUG at mm/usercopy.c:102! [5.383923] Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI [5.384903] CPU: 1 UID: 0 PID: 138 Comm: poc_put_cmsg Not tainted 6.12.57 #7 [5.384903] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [5.384903] RIP: 0010:usercopy_abort+0x6c/0x80 [5.384903] Code: 1a 86 51 48 c7 c2 40 15 1a 86 41 52 48 c7 c7 c0 15 1a 86 48 0f 45 d6 48 c7 c6 80 15 1a 86 48 89 c1 49 0f 45 f3 e8 84 27 88 ff <0f> 0b 490 [5.384903] RSP: 0018:ffffc900006f77a8 EFLAGS: 00010246 [5.384903] RAX: 000000000000006f RBX: ffff88800f0ad2a8 RCX: 1ffffffff0f72e74 [5.384903] RDX: 0000000000000000 RSI: 0000000000000004 RDI: ffffffff87b973a0 [5.384903] RBP: 0000000000000010 R08: 0000000000000000 R09: fffffbfff0f72e74 [5.384903] R10: 0000000000000003 R11: 79706f6372657375 R12: 0000000000000001 [5.384903] R13: ffff88800f0ad2b8 R14: ffffea00003c2b40 R15: ffffea00003c2b00 [5.384903] FS: 0000000011bc4380(0000) GS:ffff8880bf100000(0000) knlGS:0000000000000000 [5.384903] CS: 0010 DS: 0000 ES: 0000 CR0:	N/A	More Details

	0000000080050033 [5.384903] CR2: 000056aa3b8e5fe4 CR3: 000000000ea26004 CR4: 0000000000770ef0 [5.384903] PKRU: 55555554 [5.384903] Call Trace: [5.384903] <TASK> [5.384903] __check_heap_object+0x9a/0xd0 [5.384903] __check_object_size+0x46c/0x690 [5.384903] put_cmsg+0x129/0x5e0 [5.384903] sock_recv_errqueue+0x22f/0x380 [5.384903] tls_sw_recvmsg+0x7ed/0x1960 [5.384903] ? srso_alias_return_thunk+0x5/0xfbef5 [5.384903] ? schedule+0x6d/0x270 [5.384903] ? srso_alias_return_thunk+0x5/0xfbef5 [5.384903] ? mutex_unlock+0x81/0xd0 [5.384903] ? __pfx_mutex_unlock+0x10/0x10 [5.384903] ? __pfx_tls_sw_recvmsg+0x10/0x10 [5.384903] ? _raw_spin_lock_irqsave+0x8f/0xf0 [5.384903] ? _raw_read_unlock_irqrestore+0x20/0x40 [5.384903] ? srso_alias_return_thunk+0x5/0xfbef5 The crash offset 296 corresponds to skb2->cb within skbuff_fclones: - sizeof(struct sk_buff) = 232 - offsetof(struct sk_buff, cb) = 40 - offset of skb2.cb in fclones = 232 + 40 = 272 - crash offset 296 = 272 + 24 (inside sock_exterr_skb.ee) This patch uses a local stack variable as a bounce buffer to avoid the hardened usercopy check failure. [1] https://elixir.bootlin.com/linux/v6.12.62/source/net/ipv4/tcp.c#L885 [2] https://elixir.bootlin.com/linux/v6.12.62/source/net/core/skbuff.c#L5104 [3] https://elixir.bootlin.com/linux/v6.12.62/source/net/core/skbuff.c#L5566 [4] https://elixir.bootlin.com/linux/v6.12.62/source/net/core/skbuff.c#L5491 [5] https://elixir.bootlin.com/linux/v6.12.62/source/mm/slub.c#L5719		
CVE-2026-1290	Authentication Bypass by Primary Weakness vulnerability in Jamf Jamf Pro allows unspecified impact.This issue affects Jamf Pro: from 11.20 through 11.24.	N/A	More Details
CVE-2026-1260	Invalid memory access in Sentencepiece versions less than 0.2.1 when using a vulnerable model file, which is not created in the normal training procedure.	N/A	More Details
CVE-2021-47778	GetSimple CMS My SMTP Contact Plugin 1.1.2 contains a PHP code injection vulnerability. An authenticated administrator can inject arbitrary PHP code through plugin configuration parameters, leading to remote code execution on the server.	N/A	More Details
CVE-2021-47830	GetSimple CMS My SMTP Contact Plugin 1.1.1 contains a cross-site request forgery (CSRF) vulnerability. Attackers can craft a malicious webpage that, when visited by an authenticated administrator, can change SMTP configuration settings in the plugin. This may allow unauthorized changes but does not directly enable remote code execution.	N/A	More Details
CVE-2021-47870	GetSimple CMS My SMTP Contact Plugin 1.1.2 suffers from a Stored Cross-Site Scripting (XSS) vulnerability. The plugin attempts to sanitize user input using htmlspecialchars(), but this can be bypassed by passing dangerous characters as escaped hex bytes. This allows attackers to inject arbitrary client-side code that executes in the administrator's browser when visiting a malicious page.	N/A	More Details
CVE-2026-0834	Logic vulnerability in TP-Link Archer C20 v6.0 and Archer AX53 v1.0 (TDDP module) allows unauthenticated adjacent attackers to execute administrative commands including factory reset and device reboot without credentials. Attackers on the adjacent network can remotely trigger factory resets and reboots without credentials, causing configuration loss and interruption of device availability.This issue affects Archer C20 v6.0 < V6_251031. Archer AX53 v1.0 < V1_251215	N/A	More Details
CVE-2026-23754	D-Link D-View 8 versions 2.0.1.107 and below contain an improper access control vulnerability in backend API endpoints. Any authenticated user can supply an arbitrary user_id value to retrieve sensitive credential data belonging to other users, including super administrators. The exposed credential material can be reused directly as a valid authentication secret, allowing full impersonation of the targeted account. This results in complete account takeover and full administrative control over the D-View system.	N/A	More Details
CVE-2026-23755	D-Link D-View 8 versions 2.0.1.107 and below contain an uncontrolled search path vulnerability in the installer. When executed with elevated privileges via UAC, the installer attempts to load version.dll from its execution directory, allowing DLL preloading. An attacker can supply a malicious version.dll alongside the legitimate installer so that, when	N/A	More Details

	a victim runs the installer and approves the UAC prompt, attacker-controlled code executes with administrator privileges. This can lead to full system compromise.		
CVE-2026-1315	By sending crafted files to the firmware update endpoint of Tapo C220 v1 and C520WS v2, the device terminates core system services before verifying authentication or firmware integrity. An unauthenticated attacker can trigger a persistent denial of service, requiring a manual reboot or application initiated restart to restore normal device operation.	N/A	More Details
CVE-2026-0919	The HTTP parser of Tapo C220 v1 and C520WS v2 cameras improperly handles requests containing an excessively long URL path. An invalid-URL error path continues into cleanup code that assumes allocated buffers exist, leading to a crash and service restart. An unauthenticated attacker can force repeated service crashes or device reboots, causing denial of service.	N/A	More Details
CVE-2026-0918	The Tapo C220 v1 and C520WS v2 cameras' HTTP service does not safely handle POST requests containing an excessively large Content-Length header. The resulting failed memory allocation triggers a NULL pointer dereference, causing the main service process to crash. An unauthenticated attacker can repeatedly crash the service, causing temporary denial of service. The device restarts automatically, and repeated requests can keep it unavailable.	N/A	More Details
CVE-2025-68132	EVerest is an EV charging software stack. Prior to version 2025.12.0, \`is_message_crc_correct\` in the DZG_GSH01 powermeter SLIP parser reads \`vec[vec.size()-1]\` and \`vec[vec.size()-2]\` without checking that at least two bytes are present. Malformed SLIP frames on the serial link can reach \`is_message_crc_correct\` with \`vec.size() < 2\` (only via the multi-message path), causing an out-of-bounds read before CRC verification and \`pop_back\` underflow. Therefore, an attacker controlling the serial input can reliably crash the process. Version 2025.12.0 fixes the issue.	N/A	More Details
CVE-2025-15468	Issue summary: If an application using the SSL_CIPHER_find() function in a QUIC protocol client or server receives an unknown cipher suite from the peer, a NULL dereference occurs. Impact summary: A NULL pointer dereference leads to abnormal termination of the running process causing Denial of Service. Some applications call SSL_CIPHER_find() from the client_hello_cb callback on the cipher ID received from the peer. If this is done with an SSL object implementing the QUIC protocol, NULL pointer dereference will happen if the examined cipher ID is unknown or unsupported. As it is not very common to call this function in applications using the QUIC protocol and the worst outcome is Denial of Service, the issue was assessed as Low severity. The vulnerable code was introduced in the 3.2 version with the addition of the QUIC protocol support. The FIPS modules in 3.6, 3.5, 3.4 and 3.3 are not affected by this issue, as the QUIC implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4 and 3.3 are vulnerable to this issue. OpenSSL 3.0, 1.1.1 and 1.0.2 are not affected by this issue.	N/A	More Details
CVE-2025-11187	Issue summary: PBMAC1 parameters in PKCS#12 files are missing validation which can trigger a stack-based buffer overflow, invalid pointer or NULL pointer dereference during MAC verification. Impact summary: The stack buffer overflow or NULL pointer dereference may cause a crash leading to Denial of Service for an application that parses untrusted PKCS#12 files. The buffer overflow may also potentially enable code execution depending on platform mitigations. When verifying a PKCS#12 file that uses PBMAC1 for the MAC, the PBKDF2 salt and keylength parameters from the file are used without validation. If the value of keylength exceeds the size of the fixed stack buffer used for the derived key (64 bytes), the key derivation will overflow the buffer. The overflow length is attacker-controlled. Also, if the salt parameter is not an OCTET STRING type this can lead to invalid or NULL pointer dereference. Exploiting this issue requires a user or application to process a maliciously crafted PKCS#12 file. It is uncommon to accept untrusted PKCS#12 files in applications as they are usually used to store private keys which are trusted by definition. For this reason the issue was assessed as Moderate severity. The FIPS modules in 3.6, 3.5 and 3.4 are not affected by this issue, as PKCS#12 processing is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5 and 3.4 are vulnerable to this issue. OpenSSL 3.3, 3.0, 1.1.1 and 1.0.2 are not affected by this issue as they do not support PBMAC1 in PKCS#12.	N/A	More Details
CVE-2025-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Piqes piqes allows PHP Local File	N/A	More

69073	Inclusion.This issue affects Piqes: from n/a through <= 1.0.11.		Details
CVE-2026-24804	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in coolsnowwolf lede (package/lean/mt/drivers/mt7603e/src/mt7603_wifi/common modules). This vulnerability is associated with program files bn_lib.C. This issue affects lede: through r25.10.1.	N/A	More Details
CVE-2026-24798	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in GaijinEntertainment DagorEngine (prog/3rdPartyLibs/miniupnpc modules). This vulnerability is associated with program files upnpreplyparse.C. This issue affects DagorEngine: through dagor_2025_01_15.	N/A	More Details
CVE-2026-24799	Out-of-bounds Write, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in davisking dlib (dlib/external/zlib modules). This vulnerability is associated with program files inflate.C. This issue affects dlib: before v19.24.9.	N/A	More Details
CVE-2026-24800	Out-of-bounds Write, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in tildearrow furnace (extern/zlib modules). This vulnerability is associated with program files inflate.C.	N/A	More Details
CVE-2026-24801	Vulnerability in Ralim IronOS (source/Core/BSP/Pinecilv2/bl_mcu_sdk/components/ble/ble_stack/common/tinycrypt/source modules). This vulnerability is associated with program files ecc_dsa.C. This issue affects IronOS: before v2.23-rc3.	N/A	More Details
CVE-2026-24802	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in briandilley jsonrpc4j (src/main/java/com/googlecode/jsonrpc4j modules). This vulnerability is associated with program files NoCloseOutputStream.Java. This issue affects jsonrpc4j: through 1.6.0.	N/A	More Details
CVE-2026-24803	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in coolsnowwolf lede (package/lean/mt/drivers/mt7615d/src/mt_wifi/embedded/security modules). This vulnerability is associated with program files bn_lib.C. This issue affects lede: through r25.10.1.	N/A	More Details
CVE-2026-24806	Improper Control of Generation of Code ('Code Injection') vulnerability in liuyueyi quick-media (plugins/svg-plugin/batik-codec-fix/src/main/java/org/apache/batik/ext/awt/image/codec/png modules). This vulnerability is associated with program files PNGImageEncoder.Java. This issue affects quick-media: before v1.0.	N/A	More Details
CVE-2026-24796	Out-of-bounds Read vulnerability in CloverHackyColor CloverBootloader (MdeModulePkg/Universal/RegularExpressionDxe/Oniguruma modules). This vulnerability is associated with program files regparse.C. This issue affects CloverBootloader: before 5162.	N/A	More Details
CVE-2026-24807	Improper Verification of Cryptographic Signature vulnerability in liuyueyi quick-media (plugins/svg-plugin/batik-codec-fix/src/main/java/org/apache/batik/ext/awt/image/codec/util modules). This vulnerability is associated with program files SeekableOutputStream.Java. This issue affects quick-media: before v1.0.	N/A	More Details
CVE-2026-24808	Integer Overflow or Wraparound vulnerability in RawTherapee (rtengine modules). This vulnerability is associated with program files dcraw.Cc. This issue affects RawTherapee: through 5.11.	N/A	More Details
CVE-2026-24809	An issue from the component luaG_runerror in dependencies/lua/src/ldebug.c in praydog/REFramework version before 1.5.5 leads to a heap-buffer overflow when a recursive error occurs.	N/A	More Details
CVE-2026-24810	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in rethinkdb (src/cjson modules). This vulnerability is associated with program files cJSON.Cc. This issue affects rethinkdb: through v2.4.4.	N/A	More Details
CVE-2026-24811	Vulnerability in root-project root (builtins/zlib modules). This vulnerability is associated with program files inffast.C. This issue affects root.	N/A	More Details

CVE-2026-24812	Vulnerability in root-project root (builtins/zlib modules). This vulnerability is associated with program files inftrees.C. This issue affects root: through 6.36.00-rc1.	N/A	More Details
CVE-2026-24797	Out-of-bounds Write vulnerability in neka-nat cupoch (third_party/libjpeg-turbo/libjpeg-turbo modules). This vulnerability is associated with program files tjbench.C. This issue affects cupoch.	N/A	More Details
CVE-2026-24795	Out-of-bounds Write vulnerability in CloverHackyColor CloverBootloader (MdeModulePkg/Universal/RegularExpressionDxe/Oniguruma modules). This vulnerability is associated with program files regcomp.C. This issue affects CloverBootloader: before 5162.	N/A	More Details
CVE-2026-22598	ManageIQ is an open-source management platform. A flaw was found in the ManageIQ API prior to version radjabov-2 where a malformed TimeProfile could be created causing later UI and API requests to timeout leading to a Denial of Service. Version radjabov-2 contains a patch. One may also apply the patch manually.	N/A	More Details
CVE-2026-23887	Group-Office is an enterprise customer relationship management and groupware tool. In versions 6.8.148 and below, and 25.0.1 through 25.0.79, the application stores unsanitized filenames in the database, which can lead to Stored Cross-Site Scripting (XSS). Users who interact with these specially crafted file names within the Group-Office application are affected. While the scope is limited to the file-viewing context, it could still be used to interfere with user sessions or perform unintended actions in the browser. This issue is fixed in versions 6.8.149 and 25.0.80.	N/A	More Details
CVE-2026-23958	Dataease is an open source data visualization analysis tool. Prior to version 2.10.19, DataEase uses the MD5 hash of the user's password as the JWT signing secret. This deterministic secret derivation allows an attacker to brute-force the admin's password by exploiting unmonitored API endpoints that verify JWT tokens. The vulnerability has been fixed in v2.10.19. No known workarounds are available.	N/A	More Details
CVE-2026-24477	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. If AnythingLLM prior to version 1.10.0 is configured to use Qdrant as the vector database with an API key, this QdrantApiKey could be exposed in plain text to unauthenticated users via the `/api/setup-complete` endpoint. Leakage of QdrantApiKey allows an unauthenticated attacker full read/write access to the Qdrant vector database instance used by AnythingLLM. Since Qdrant often stores the core knowledge base for RAG in AnythingLLM, this can lead to complete compromise of the semantic search / retrieval functionality and indirect leakage of confidential uploaded documents. Version 1.10.0 patches the issue.	N/A	More Details
CVE-2026-23699	AP180 series with firmware versions prior to AP_RGOS 11.9(4)B1P8 contains an OS command injection vulnerability. If this vulnerability is exploited, arbitrary commands may be executed on the devices.	N/A	More Details
CVE-2026-24479	HUSTOF is an open source online judge based on PHP/C++/MySQL/Linux for ACM/ICPC and NOIP training. Prior to version 26.01.24, the problem_import_qduoj.php and problem_import_hoj.php modules fail to properly sanitize filenames within uploaded ZIP archives. Attackers can craft a malicious ZIP file containing files with path traversal sequences (e.g., ../../shell.php). When extracted by the server, this allows writing files to arbitrary locations in the web root, leading to Remote Code Execution (RCE). Version 26.01.24 contains a fix for the issue.	N/A	More Details
CVE-2026-24480	QGIS is a free, open source, cross platform geographical information system (GIS) The repository contains a GitHub Actions workflow called "pre-commit checks" that, before commit 76a693cd91650f9b4e83edac525e5e4f90d954e9, was vulnerable to remote code execution and repository compromise because it used the `pull_request_target` trigger and then checked out and executed untrusted pull request code in a privileged context. Workflows triggered by `pull_request_target` ran with the base repository's credentials and access to secrets. If these workflows then checked out and executed code from the head of an external pull request (which could have been attacker controlled), the attacker could have executed arbitrary commands with elevated privileges. This insecure pattern has been documented as a security risk by GitHub and security researchers. Commit	N/A	More Details

	76a693cd91650f9b4e83edac525e5e4f90d954e9 removed the vulnerable code.		
CVE-2025-69074	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Pearson Specter pearsonspecter allows PHP Local File Inclusion.This issue affects Pearson Specter: from n/a through <= 1.11.3.	N/A	More Details
CVE-2026-21408	beat-access for Windows version 3.0.3 and prior contains an issue with the DLL search path, which may lead to insecurely loading Dynamic Link Libraries. As a result, arbitrary code may be executed with SYSTEM privileges.	N/A	More Details
CVE-2026-24794	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in CardboardPowered cardboard (src/main/java/org/cardboardpowered/impl/world modules). This vulnerability is associated with program files WorldImpl.Java. This issue affects cardboard: before 1.21.4.	N/A	More Details
CVE-2026-1464	Integer Overflow or Wraparound vulnerability in MuntashirAkon AppManager (app/src/main/java/org/apache/commons/compress/archivers/tar modules). This vulnerability is associated with program files TarUtils.Java. This issue affects AppManager: before 4.0.4.	N/A	More Details
CVE-2026-1465	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in anyrtcIO-Community anyRTC-RTMP-OpenSource (third_party/faad2-2.7/libfaad modules). This vulnerability is associated with program files bits.C, syntax.C. This issue affects anyRTC-RTMP-OpenSource: before 1.0.	N/A	More Details
CVE-2026-23873	hustoj is an open source online judge based on PHP/C++/MySQL/Linux for ACM/ICPC and NOIP training. All versions are vulnerable to CSV Injection (Formula Injection) through the contest rank export functionality (contestrank.xls.php and admin/ranklist_export.php). The application fails to sanitize user-supplied input (specifically the "Nickname" field) before exporting it to an .xls file (which renders as an HTML table but is opened by Excel). If a malicious user sets their nickname to an Excel formula when an administrator exports and opens the rank list in Microsoft Excel, the formula will be executed. This can lead to arbitrary command execution (RCE) on the administrator's machine or data exfiltration. A fix was not available at the time of publication.	N/A	More Details
CVE-2025-69075	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Yolox yolox allows PHP Local File Inclusion.This issue affects Yolox: from n/a through <= 1.0.15.	N/A	More Details
CVE-2026-24344	Multiple Buffer Overflows in Admin UI of EZCast Pro II version 1.17478.146 allow attackers to cause a program crash and potential remote code execution	N/A	More Details
CVE-2026-24793	Out-of-bounds Write, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in azerothcore azerothcore-wotlk (deps/zlib modules). This vulnerability is associated with program files inflate.C. This issue affects azerothcore-wotlk: through v4.0.0.	N/A	More Details
CVE-2026-24813	NULL Pointer Dereference vulnerability in abcz316 SKRoot-linuxKernelRoot (testRoot/jni/utils modules). This vulnerability is associated with program files cJSON.Cpp. This issue affects SKRoot-linuxKernelRoot.	N/A	More Details
CVE-2026-24814	Integer Overflow or Wraparound vulnerability in swoole swoole-src (thirdparty/hiredis modules). This vulnerability is associated with program files sds.C. This issue affects swoole-src: before 6.0.2.	N/A	More Details
CVE-2026-24815	Unrestricted Upload of File with Dangerous Type, Deserialization of Untrusted Data vulnerability in datavane tis (tis-plugin/src/main/java/com/qlangtech/tis/extension/impl modules). This vulnerability is associated with program files XmlFile.Java. This issue affects tis: before v4.3.0.	N/A	More Details
CVE-	CVAT is an open source interactive video and image annotation tool for computer vision. In versions 1.0.0 through 2.54.0, users that have the staff status may freely change their permissions, including giving themselves superuser status and joining the admin group,		More

2026-23526	which gives them full access to the data in the CVAT instance. Version 2.55.0 fixes the issue. As a workaround, review the list of users with staff status and revoke it from any users that are not expected to have superuser privileges.	N/A	Details
CVE-2025-12386	Pix-Link LV-WR21Q does not enforce any form of authentication for endpoint /goform/getHomePageInfo. Remote unauthenticated attacker is able to use this endpoint to e.g: retrieve cleartext password to the access point. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version V108_108 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-12387	A vulnerability in the Pix-Link LV-WR21Q router's language module allows remote attackers to trigger a denial of service (DoS) by sending a specially crafted HTTP POST request containing non-existing language parameter. This renders the server unable to serve correct lang.js file, which causes administrator panel to not work, resulting in DoS until the language settings is reverted to a correct value. The Denial of Service affects only the administrator panel and does not affect other router functionalities. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version V108_108 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2026-23630	Docmost is open-source collaborative wiki and documentation software. In versions 0.3.0 through 0.23.2, Mermaid code block rendering is vulnerable to stored Cross-Site Scripting (XSS). The frontend can render attacker-controlled Mermaid diagrams using mermaid.render(), then inject the returned SVG/HTML into the DOM via dangerouslySetInnerHTML without sanitization. Mermaid per-diagram %%{init}%% directives allow overriding securityLevel and enabling htmlLabels, permitting arbitrary HTML/JS execution for any viewer. This issue has been fixed in version 0.24.0.	N/A	More Details
CVE-2026-23960	Argo Workflows is an open source container-native workflow engine for orchestrating parallel jobs on Kubernetes. Prior to versions 3.6.17 and 3.7.8, stored XSS in the artifact directory listing allows any workflow author to execute arbitrary JavaScript in another user's browser under the Argo Server origin, enabling API actions with the victim's privileges. Versions 3.6.17 and 3.7.8 fix the issue.	N/A	More Details
CVE-2026-1213	All versions of askbot before and including 0.12.2 allow an attacker authenticated with normal user permissions to modify the profile picture of other application users.This issue affects askbot: 0.12.2.	N/A	More Details
CVE-2026-22461	Missing Authorization vulnerability in WebAppick CTX Feed webappick-product-feed-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects CTX Feed: from n/a through <= 6.6.18.	N/A	More Details
CVE-2026-23518	Fleet is open source device management software. In versions prior to 4.78.3, 4.77.1, 4.76.2, 4.75.2, and 4.53.3, a vulnerability in Fleet's Windows MDM enrollment flow could allow an attacker to submit forged authentication tokens that are not properly validated. Because JWT signatures were not verified, Fleet could accept attacker-controlled identity claims, enabling enrollment of unauthorized devices under arbitrary Azure AD user identities. Versions 4.78.3, 4.77.1, 4.76.2, 4.75.2, and 4.53.3 fix the issue. If an immediate upgrade is not possible, affected Fleet users should temporarily disable Windows MDM.	N/A	More Details
CVE-2026-24816	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in datavane tis (tis-console/src/main/java/com/qlangtech/tis/runtime/module/action modules). This vulnerability is associated with program files ChangeDomainAction.Java. This issue affects tis: before v4.3.0.	N/A	More Details
CVE-2026-23517	Fleet is open source device management software. A broken access control issue in versions prior to 4.78.3, 4.77.1, 4.76.2, 4.75.2, and 4.53.3 allowed authenticated users to access debug and profiling endpoints regardless of role. As a result, low-privilege users could view internal server diagnostics and trigger resource-intensive profiling operations. Fleet's debug/pprof endpoints are accessible to any authenticated user regardless of role, including the lowest-privilege "Observer" role. This allows low-privilege users to access sensitive server internals, including runtime profiling data and in-memory application state,	N/A	More Details

	and to trigger CPU-intensive profiling operations that could lead to denial of service. Versions 4.78.3, 4.77.1, 4.76.2, 4.75.2, and 4.53.3 fix the issue. If an immediate upgrade is not possible, users should put the debug/pprof endpoints behind an IP allowlist as a workaround.		
CVE-2026-23516	CVAT is an open source interactive video and image annotation tool for computer vision. In versions 2.2.0 through 2.54.0, an attacker is able to execute arbitrary JavaScript in a victim user's CVAT UI session, provided that they are able to create a maliciously crafted label in a CVAT task or project, then get the victim user to either edit that label, or view a shape that refers to that label; and/or get the victim user to upload a maliciously crafted SVG image when configuring a skeleton. This gives the attacker temporary access to all CVAT resources that the victim user can access. Version 2.55.0 fixes the issue.	N/A	More Details
CVE-2026-23499	Saleor is an e-commerce platform. Starting in version 3.0.0 and prior to versions 3.20.108, 3.21.43, and 3.22.27, Saleor allowed authenticated staff users or Apps to upload arbitrary files, including malicious HTML and SVG files containing Javascript. Depending on the deployment strategy, these files may be served from the same domain as the dashboard without any restrictions leading to the execution of malicious scripts in the context of the user's browser. Malicious staff members could craft script injections to target other staff members, possibly stealing their access and/or refresh tokens. Users are vulnerable if they host the media files inside the same domain as the dashboard, e.g., dashboard is at `example.com/dashboard/` and media are under `example.com/media/`. They are not impact if media files are hosted in a different domain, e.g., `media.example.com`. Users are impacted if they do not return a `Content-Disposition: attachment` header for the media files. Saleor Cloud users are not impacted. This issue has been patched in versions: 3.22.27, 3.21.43, and 3.20.108. Some workarounds are available for those unable to upgrade. Configure the servers hosting the media files (e.g., CDN or reverse proxy) to return the Content-Disposition: attachment header. This instructs browsers to download the file instead of rendering them in the browser. Prevent the servers from returning HTML and SVG files. Set-up a `Content-Security-Policy` for media files, such as `Content-Security-Policy: default-src 'none'; base-uri 'none'; frame-ancestors 'none'; form-action 'none';`.	N/A	More Details
CVE-2026-22849	Saleor is an e-commerce platform. Starting in version 3.0.0 and prior to versions 3.20.108, 3.21.43, and 3.22.27, Saleor was allowing users to modify rich text fields with HTML without running any backend HTML cleaners thus allowing malicious actors to perform stored XSS attacks on dashboards and storefronts. Malicious staff members could craft script injections to target other staff members, possibly stealing their access and/or refresh tokens. This issue has been patched in versions 3.22.27, 3.21.43, and 3.20.108. In case of inability to upgrade straight away, a possible workaround is to use client-side cleaner.	N/A	More Details
CVE-2026-22822	External Secrets Operator reads information from a third-party service and automatically injects the values as Kubernetes Secrets. Starting in version 0.20.2 and prior to version 1.2.0, the `getSecretKey` template function, while introduced for senhasegura Devops Secrets Management (DSM) provider, has the ability to fetch secrets cross-namespaces with the roleBinding of the external-secrets controller, bypassing our security mechanisms. This function was completely removed in version 1.2.0, as everything done with that templating function can be done in a different way while respecting External Secrets Operator's safeguards As a workaround, use a policy engine such as Kubernetes, Kyverno, Kubewarden, or OPA to prevent the usage of `getSecretKey` in any ExternalSecret resource.	N/A	More Details
CVE-2026-22808	fleetdm/fleet is open source device management software. Prior to versions 4.78.2, 4.77.1, 4.76.2, 4.75.2, and 4.53.3, if Windows MDM is enabled, an unauthenticated attacker can exploit this XSS vulnerability to steal a Fleet administrator's authentication token (FLEET::auth_token) from localStorage. This could allow unauthorized access to Fleet, including administrative access, visibility into device data, and modification of configuration. Versions 4.78.2, 4.77.1, 4.76.2, 4.75.2, and 4.53.3 fix the issue. If an immediate upgrade is not possible, affected Fleet users should temporarily disable Windows MDM.	N/A	More Details
	Copier is a library and CLI app for rendering project templates. Prior to version 9.11.2, Copier suggests that it's safe to generate a project from a safe template, i.e. one that		

CVE-2026-23968	doesn't use unsafe features like custom Jinja extensions which would require passing the `--UNSAFE,--trust` flag. As it turns out, a safe template can currently include arbitrary files/directories outside the local template clone location by using symlinks along with `_preserve_symlinks: false` (which is Copier's default setting). Version 9.11.2 patches the issue.	N/A	More Details
CVE-2026-23986	Copier is a library and CLI app for rendering project templates. Prior to version 9.11.2, Copier suggests that it's safe to generate a project from a safe template, i.e. one that doesn't use unsafe features like custom Jinja extensions which would require passing the `--UNSAFE,--trust` flag. As it turns out, a safe template can currently write to arbitrary directories outside the destination path by using directory a symlink along with `_preserve_symlinks: true` and a generated directory structure whose rendered path is inside the symlinked directory. This way, a malicious template author can create a template that overwrites arbitrary files (according to the user's write permissions), e.g., to cause havoc. Version 9.11.2 patches the issue.	N/A	More Details
CVE-2025-69102	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Boopathi Rajan WP Test Email wp-test-email allows Reflected XSS.This issue affects WP Test Email: from n/a through <= 1.1.7.	N/A	More Details
CVE-2026-24826	Out-of-bounds Write, Divide By Zero, NULL Pointer Dereference, Use of Uninitialized Resource, Out-of-bounds Read, Reachable Assertion vulnerability in cadaver turso3d.This issue affects .	N/A	More Details
CVE-2026-24348	Multiple cross-site scripting vulnerabilities in Admin UI of EZCast Pro II version 1.17478.146 allow attackers to execute arbitrary JavaScript code in the browser of other Admin UI users.	N/A	More Details
CVE-2026-24347	Improper input validation in Admin UI of EZCast Pro II version 1.17478.146 allows attackers to manipulate files in the /tmp directory	N/A	More Details
CVE-2026-24346	Use of well-known default credentials in Admin UI of EZCast Pro II version 1.17478.146 allows attackers to access protected areas in the web application	N/A	More Details
CVE-2026-24345	Cross-Site Request Forgery in Admin UI of EZCast Pro II version 1.17478.146 allows attackers to bypass authorization checks and gain full access to the admin UI	N/A	More Details
CVE-2026-24825	Missing Release of Memory after Effective Lifetime vulnerability in ydb-platform ydb (contrib/libs/yajl modules). This vulnerability is associated with program files yail_tree.C. This issue affects ydb: through 24.4.4.2.	N/A	More Details
CVE-2026-24824	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in yacy yacy_search_server (source/net/yacy/http/servlets modules). This vulnerability is associated with program files YaCyDefaultServlet.Java. This issue affects yacy_search_server.	N/A	More Details
CVE-2026-24823	Out-of-bounds Write, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in FASTSHIFT X-TRACK (Software/X-Track/USER/App/Utils/lv_img_png/PNGdec/src modules). This vulnerability is associated with program files inflate.C. This issue affects X-TRACK: through v2.7.	N/A	More Details
CVE-2026-24822	Out-of-bounds Write, Heap-based Buffer Overflow vulnerability in ttttupup wxhelper (src modules). This vulnerability is associated with program files mongoose.C. This issue affects wxhelper: through 3.9.10.19-v1.	N/A	More Details
CVE-2026-24821	Out-of-bounds Read vulnerability in turanszkij WickedEngine (WickedEngine/LUA modules). This vulnerability is associated with program files lparser.C. This issue affects WickedEngine: through 0.71.727.	N/A	More Details
CVE-	Out-of-bounds Read vulnerability in turanszkij WickedEngine (WickedEngine/LUA modules).		More

2026-24820	This vulnerability is associated with program files ldebug.C. This issue affects WickedEngine: before 0.71.705.	N/A	Details
CVE-2026-24819	Improperly Controlled Sequential Memory Allocation vulnerability in foxinmy weixin4j (weixin4j-base/src/main/java/com/foxinmy/weixin4j/util modules). This vulnerability is associated with program files CharArrayBuffer.Java, ClassUtil.Java. This issue affects weixin4j.	N/A	More Details
CVE-2026-24818	Out-of-bounds Read vulnerability in praydog UEVR (dependencies/lua/src modules). This vulnerability is associated with program files lparser.C. This issue affects UEVR: before 1.05.	N/A	More Details
CVE-2026-24817	Out-of-bounds Write vulnerability in praydog UEVR (dependencies/lua/src modules). This vulnerability is associated with program files ldebug.C, lvm.C. This issue affects UEVR: before 1.05.	N/A	More Details
CVE-2026-24805	NULL Pointer Dereference vulnerability in visualfc liteide (liteidex/src/3rdparty/libvterm/src modules). This vulnerability is associated with program files screen.C, state.C, vterm.C. This issue affects liteide: before x38.4.	N/A	More Details
CVE-2024-36998	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2023-22927	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2025-15348	Anritsu ShockLine CHX File Parsing Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Anritsu ShockLine. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CHX files. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27833.	N/A	More Details
CVE-2026-0755	gemini-mcp-tool execAsync Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of gemini-mcp-tool. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the execAsync method. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-27783.	N/A	More Details
CVE-2025-68518	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Hoteller hoteller allows Reflected XSS.This issue affects Hoteller: from n/a through < 6.8.9.	N/A	More Details
CVE-2025-15351	Anritsu VectorStar CHX File Parsing Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Anritsu VectorStar. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CHX files. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27040.	N/A	More Details
CVE-2025-15350	Anritsu VectorStar CHX File Parsing Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Anritsu VectorStar. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CHX files. The issue results from the lack of proper	N/A	More Details

	validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27039.		
CVE-2025-15349	Anritsu ShockLine SCPI Race Condition Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Anritsu ShockLine. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SCPI component. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27315.	N/A	More Details
CVE-2025-68008	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mndpsingh287 WP Mail wp-mail allows Reflected XSS.This issue affects WP Mail: from n/a through <= 1.3.	N/A	More Details
CVE-2025-15063	Ollama MCP Server execAsync Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ollama MCP Server. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the execAsync method. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-27683.	N/A	More Details
CVE-2025-67957	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in TangibleWP Listivo Core listivo-core allows PHP Local File Inclusion.This issue affects Listivo Core: from n/a through <= 2.3.77.	N/A	More Details
CVE-2025-15062	Trimble SketchUp SKP File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Trimble SketchUp. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of SKP files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27769.	N/A	More Details
CVE-2025-15061	Framelink Figma MCP Server fetchWithRetry Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Framelink Figma MCP Server. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the fetchWithRetry method. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-27877.	N/A	More Details
CVE-2025-15059	GIMP PSP File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PSP files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28232.	N/A	More Details
CVE-2025-11002	7-Zip ZIP File Parsing Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of 7-Zip. Interaction with this product is required to exploit this vulnerability but attack vectors may vary depending on the implementation. The specific flaw exists within the handling of symbolic links in ZIP files. Crafted data in a ZIP file can cause the process to traverse to unintended directories. An attacker can leverage this vulnerability to execute code in the context of a service account. Was ZDI-CAN-26743.	N/A	More Details
CVE-2025-68520	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods DotLife dotlife allows Reflected XSS.This issue affects DotLife: from n/a through < 4.9.5.	N/A	More Details

CVE-2025-68007	Missing Authorization vulnerability in Event Espresso Event Espresso 4 Decaf event-espresso-decaf allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Event Espresso 4 Decaf: from n/a through <= 5.0.37.decaf.	N/A	More Details
CVE-2026-0756	github-kanban-mcp-server execAsync Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of github-kanban-mcp-server. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the create_issue parameter. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-27784.	N/A	More Details
CVE-2025-68009	Missing Authorization vulnerability in Codeless Slider Templates slider-templates allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Slider Templates: from n/a through <= 1.0.3.	N/A	More Details
CVE-2025-68010	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in netgsm Netgsm netgsm allows Reflected XSS.This issue affects Netgsm: from n/a through <= 2.9.63.	N/A	More Details
CVE-2025-68011	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GLS GLS Shipping for WooCommerce gls-shipping-for-woocommerce allows Reflected XSS.This issue affects GLS Shipping for WooCommerce: from n/a through <= 1.4.0.	N/A	More Details
CVE-2025-68012	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dmytro Shteflyuk CodeColorer codecolorer allows Stored XSS.This issue affects CodeColorer: from n/a through <= 0.10.1.	N/A	More Details
CVE-2025-68013	Missing Authorization vulnerability in cardpaysolutions Payment Gateway Authorize.Net CIM for WooCommerce authnet-cim-for-woo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Payment Gateway Authorize.Net CIM for WooCommerce: from n/a through <= 2.1.2.	N/A	More Details
CVE-2025-68015	Improper Control of Generation of Code ('Code Injection') vulnerability in Vollstart Event Tickets with Ticket Scanner event-tickets-with-ticket-scanner allows Code Injection.This issue affects Event Tickets with Ticket Scanner: from n/a through <= 2.8.3.	N/A	More Details
CVE-2025-68016	Missing Authorization vulnerability in Onepay Sri Lanka onepay Payment Gateway For WooCommerce onepay-payment-gateway-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects onepay Payment Gateway For WooCommerce: from n/a through <= 1.1.2.	N/A	More Details
CVE-2025-68017	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Antideo Antideo Email Validator antideo-email-validator allows Blind SQL Injection.This issue affects Antideo Email Validator: from n/a through <= 1.0.10.	N/A	More Details
CVE-2025-68018	Missing Authorization vulnerability in ilmosys Order Listener for WooCommerce woc-order-alert allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Order Listener for WooCommerce: from n/a through <= 3.6.1.	N/A	More Details
CVE-2025-68019	Missing Authorization vulnerability in cleverplugins SEO Booster seo-booster allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SEO Booster: from n/a through <= 6.1.8.	N/A	More Details
CVE-2025-68020	Missing Authorization vulnerability in WANotifier WANotifier notifier allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WANotifier: from n/a through <= 2.7.12.	N/A	More Details
CVE-2026-	A denial-of-service (DoS) vulnerability exists in google.protobuf.json_format.ParseDict() in Python, where the max_recursion_depth limit can be bypassed when parsing nested google.protobuf.Any messages. Due to missing recursion depth accounting inside the internal Any-handling logic, an attacker can supply deeply nested Any structures that	N/A	More Details

0994	bypass the intended recursion limit, eventually exhausting Python’s recursion stack and causing a RecursionError.		
CVE-2025-71157	In the Linux kernel, the following vulnerability has been resolved: RDMA/core: always drop device refcount in ib_del_sub_device_and_put() Since nldev_deldev() (introduced by commit 060c642b2ab8 ("RDMA/nldev: Add support to add/delete a sub IB device through netlink") grabs a reference using ib_device_get_by_index() before calling ib_del_sub_device_and_put(), we need to drop that reference before returning -EOPNOTSUPP error.	N/A	More Details
CVE-2025-71156	In the Linux kernel, the following vulnerability has been resolved: gve: defer interrupt enabling until NAPI registration Currently, interrupts are automatically enabled immediately upon request. This allows interrupt to fire before the associated NAPI context is fully initialized and cause failures like below: [0.946369] Call Trace: [0.946369] <IRQ> [0.946369] __napi_poll+0x2a/0x1e0 [0.946369] net_rx_action+0x2f9/0x3f0 [0.946369] handle_softirqs+0xd6/0x2c0 [0.946369] ? handle_edge_irq+0xc1/0x1b0 [0.946369] __irq_exit_rcu+0xc3/0xe0 [0.946369] common_interrupt+0x81/0xa0 [0.946369] </IRQ> [0.946369] <TASK> [0.946369] asm_common_interrupt+0x22/0x40 [0.946369] RIP: 0010:pv_native_safe_halt+0xb/0x10 Use the `IRQF_NO_AUTOEN` flag when requesting interrupts to prevent auto enablement and explicitly enable the interrupt in NAPI initialization path (and disable it during NAPI teardown). This ensures that interrupt lifecycle is strictly coupled with readiness of NAPI context.	N/A	More Details
CVE-2025-71155	In the Linux kernel, the following vulnerability has been resolved: KVM: s390: Fix gmap_helper_zap_one_page() again A few checks were missing in gmap_helper_zap_one_page(), which can lead to memory corruption in the guest under specific circumstances. Add the missing checks.	N/A	More Details
CVE-2025-71154	In the Linux kernel, the following vulnerability has been resolved: net: usb: rtl8150: fix memory leak on usb_submit_urb() failure In async_set_registers(), when usb_submit_urb() fails, the allocated async_req structure and URB are not freed, causing a memory leak. The completion callback async_set_reg_cb() is responsible for freeing these allocations, but it is only called after the URB is successfully submitted and completes (successfully or with error). If submission fails, the callback never runs and the memory is leaked. Fix this by freeing both the URB and the request structure in the error path when usb_submit_urb() fails.	N/A	More Details
CVE-2025-68006	Insertion of Sensitive Information Into Sent Data vulnerability in Deetronix Booking Ultra Pro booking-ultra-pro allows Retrieve Embedded Sensitive Data.This issue affects Booking Ultra Pro: from n/a through <= 1.1.23.	N/A	More Details
CVE-2026-24132	Orval generates type-safe JS clients (TypeScript) from any valid OpenAPI v3 or Swagger v2 specification. Versions 7.19.0 and below and 8.0.0-rc.0 through 8.0.2 allow untrusted OpenAPI specifications to inject arbitrary TypeScript/JavaScript into generated mock files via the const keyword on schema properties. These const values are interpolated into the mock scalar generator (getMockScalar in packages/mock/src/faker/getters/scalar.ts) without proper escaping or type-safe serialization, which results in attacker-controlled code being emitted into both interface definitions and faker/MSW handlers. The vulnerability is similar in impact to the previously reported enum x-enumDescriptions (GHSA-h526-wf6g-67jv), but it affects a different code path in the faker-based mock generator rather than @orval/core. The issue has been fixed in versions 7.20.0 and 8.0.3.	N/A	More Details
CVE-2025-68538	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Craft craftcoffee allows DOM-Based XSS.This issue affects Craft: from n/a through <= 2.3.6.	N/A	More Details
CVE-2025-68986	Unrestricted Upload of File with Dangerous Type vulnerability in zozothemes Miion miion allows Upload a Web Shell to a Web Server.This issue affects Miion: from n/a through <= 1.2.7.	N/A	More Details
CVE-2026-	An Authorization Bypass Through User-Controlled Key vulnerability in Hubitat Elevation home automation controllers prior to version 2.4.2.157 could allow a remote authenticated	N/A	More

1201	user to control connected devices outside of their authorized scope via client-side request manipulation.		Details
CVE-2025-67959	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in purethemes WorkScout workscout allows Reflected XSS.This issue affects WorkScout: from n/a through <= 4.1.07.	N/A	More Details
CVE-2025-67960	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in purethemes WorkScout-Core workscout-core allows Reflected XSS.This issue affects WorkScout-Core: from n/a through <= 1.7.06.	N/A	More Details
CVE-2025-69004	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in XpeedStudio Bajaar - Highly Customizable WooCommerce WordPress Theme bajaar allows PHP Local File Inclusion.This issue affects Bajaar - Highly Customizable WooCommerce WordPress Theme: from n/a through <= 2.1.0.	N/A	More Details
CVE-2025-67961	Server-Side Request Forgery (SSRF) vulnerability in Marco van Wieren WPO365 wpo365-login allows Server Side Request Forgery.This issue affects WPO365: from n/a through <= 40.0.	N/A	More Details
CVE-2025-69003	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in QantumThemes KenthaRadio qt-kentharadio allows Reflected XSS.This issue affects KenthaRadio: from n/a through <= 2.2.0.	N/A	More Details
CVE-2025-67963	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ovatheme Movie Booking movie-booking allows Path Traversal.This issue affects Movie Booking: from n/a through <= 1.1.5.	N/A	More Details
CVE-2025-67964	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in favethemes Homey Core homey-core allows Reflected XSS.This issue affects Homey Core: from n/a through <= 2.4.3.	N/A	More Details
CVE-2025-69002	Deserialization of Untrusted Data vulnerability in designthemes OneLife onelife allows Object Injection.This issue affects OneLife: from n/a through <= 3.9.	N/A	More Details
CVE-2025-67966	Incorrect Privilege Assignment vulnerability in e-plugins Lawyer Directory lawyer-directory allows Privilege Escalation.This issue affects Lawyer Directory: from n/a through <= 1.3.3.	N/A	More Details
CVE-2025-69001	Improper Control of Generation of Code ('Code Injection') vulnerability in Shahjahan Jewel FluentForm fluentform allows Code Injection.This issue affects FluentForm: from n/a through <= 6.1.11.	N/A	More Details
CVE-2025-67967	Missing Authorization vulnerability in e-plugins Lawyer Directory lawyer-directory allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Lawyer Directory: from n/a through <= 1.3.3.	N/A	More Details
CVE-2025-67968	Unrestricted Upload of File with Dangerous Type vulnerability in InspiryThemes Real Homes CRM realhomes-crm allows Using Malicious Files.This issue affects Real Homes CRM: from n/a through <= 1.0.0.	N/A	More Details
CVE-2025-68999	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in HappyMonster Happy Addons for Elementor happy-elementor-addons allows Blind SQL Injection.This issue affects Happy Addons for Elementor: from n/a through <= 3.20.4.	N/A	More Details
CVE-2025-68913	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in zozothemes Miion miion allows PHP Local File Inclusion.This issue affects Miion: from n/a through <= 1.2.7.	N/A	More Details
CVE-2025-68004	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kapil Chugh My Post Order my-posts-order allows Reflected XSS.This issue affects My Post Order: from n/a through <= 1.2.1.1.	N/A	More Details

CVE-2026-24058	Soft Serve is a self-hostable Git server for the command line. Versions 0.11.2 and below have a critical authentication bypass vulnerability that allows an attacker to impersonate any user (including admin) by "offering" the victim's public key during the SSH handshake before authenticating with their own valid key. This occurs because the user identity is stored in the session context during the "offer" phase and is not cleared if that specific authentication attempt fails. This issue has been fixed in version 0.11.3.	N/A	More Details
CVE-2025-68912	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Harmonic Design HDForms hdforms allows Path Traversal.This issue affects HDForms: from n/a through <= 1.6.1.	N/A	More Details
CVE-2025-68871	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in noCreativity Dooodl dooodl allows Reflected XSS.This issue affects Dooodl: from n/a through <= 2.3.0.	N/A	More Details
CVE-2025-68869	Incorrect Privilege Assignment vulnerability in LazyCoders LLC LazyTasks lazytasks-project-task-management allows Privilege Escalation.This issue affects LazyTasks: from n/a through <= 1.4.01.	N/A	More Details
CVE-2025-68866	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in woofer696 Dinatur dinatur allows Stored XSS.This issue affects Dinatur: from n/a through <= 1.18.	N/A	More Details
CVE-2025-68864	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Infility Infility Global infility-global allows Stored XSS.This issue affects Infility Global: from n/a through <= 2.14.50.	N/A	More Details
CVE-2025-68859	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in agmorpheus Syntax Highlighter Compress syntax-highlighter-compress allows Reflected XSS.This issue affects Syntax Highlighter Compress: from n/a through <= 3.0.83.3.	N/A	More Details
CVE-2025-68849	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Frank Corso Quote Master quote-master allows Reflected XSS.This issue affects Quote Master: from n/a through <= 7.1.1.	N/A	More Details
CVE-2025-68001	Unrestricted Upload of File with Dangerous Type vulnerability in garidium g-FFL Checkout g-ffl-checkout allows Upload a Web Shell to a Web Server.This issue affects g-FFL Checkout: from n/a through <= 2.1.0.	N/A	More Details
CVE-2025-68003	Missing Authorization vulnerability in renatoatshown Shown Connector shown-connector allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Shown Connector: from n/a through <= 1.2.10.	N/A	More Details
CVE-2026-24124	Dragonfly is an open source P2P-based file distribution and image acceleration system. In versions 2.4.1-rc.0 and below, the Job API endpoints (/api/v1/jobs) lack JWT authentication middleware and RBAC authorization checks in the routing configuration. This allows any unauthenticated user with access to the Manager API to view, update and delete jobs. The issue is fixed in version 2.4.1-rc.1.	N/A	More Details
CVE-2025-68838	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in expresstechsoftware MemberPress Discord Addon expresstechsoftwares-memberpress-discord-add-on allows Reflected XSS.This issue affects MemberPress Discord Addon: from n/a through <= 1.1.4.	N/A	More Details
CVE-2026-24130	Moonraker is a Python web server providing API access to Klipper 3D printing firmware. In versions 0.9.3 and below, instances configured with the "ldap" component enabled are vulnerable to LDAP search filter injection techniques via the login endpoint. The 401 error response message can be used to determine whether or not a search was successful, allowing for brute force methods to discover LDAP entries on the server such as user IDs and user attributes. This issue has been fixed in version 0.10.0.	N/A	More Details
	An authentication weakness was identified in Omada Controllers, Gateways and Access		

CVE-2025-9290	Points, controller-device adoption due to improper handling of random values. Exploitation requires advanced network positioning and allows an attacker to intercept adoption traffic and forge valid authentication through offline precomputation, potentially exposing sensitive information and compromising confidentiality.	N/A	More Details
CVE-2025-71153	In the Linux kernel, the following vulnerability has been resolved: ksmbd: Fix memory leak in get_file_all_info() In get_file_all_info(), if vfs_getattr() fails, the function returns immediately without freeing the allocated filename, leading to a memory leak. Fix this by freeing the filename before returning in this error case.	N/A	More Details
CVE-2025-71152	In the Linux kernel, the following vulnerability has been resolved: net: dsa: properly keep track of conduit reference Problem description ------------------- DSA has a mumbo-jumbo of reference handling of the conduit net device and its kobject which, sadly, is just wrong and doesn't make sense. There are two distinct problems. 1. The OF path, which uses of_find_net_device_by_node(), never releases the elevated refcount on the conduit's kobject. Nominally, the OF and non-OF paths should result in objects having identical reference counts taken, and it is already suspicious that dsa_dev_to_net_device() has a put_device() call which is missing in dsa_port_parse_of(), but we can actually even verify that an issue exists. With CONFIG_DEBUG_KOBJECT_RELEASE=y, if we run this command "before" and "after" applying this patch: (unbind the conduit driver for net device eno2) echo 0000:00:00.2 > /sys/bus/pci/drivers/fsl_enetc/unbind we see these lines in the output diff which appear only with the patch applied: kobject: 'eno2' (ffff002009a3a6b8): kobject_release, parent 0000000000000000 (delayed 1000) kobject: '109' (ffff0020099d59a0): kobject_release, parent 0000000000000000 (delayed 1000) 2. After we find the conduit interface one way (OF) or another (non-OF), it can get unregistered at any time, and DSA remains with a long-lived, but in this case stale, cpu_dp->conduit pointer. Holding the net device's underlying kobject isn't actually of much help, it just prevents it from being freed (but we never need that kobject directly). What helps us to prevent the net device from being unregistered is the parallel netdev reference mechanism (dev_hold() and dev_put()). Actually we actually use that netdev tracker mechanism implicitly on user ports since commit 2f1e8ea726e9 ("net: dsa: link interfaces with the DSA master to get rid of lockdep warnings"), via netdev_upper_dev_link(). But time still passes at DSA switch probe time between the initial of_find_net_device_by_node() code and the user port creation time, time during which the conduit could unregister itself and DSA wouldn't know about it. So we have to run of_find_net_device_by_node() under rtnl_lock() to prevent that from happening, and release the lock only with the netdev tracker having acquired the reference. Do we need to keep the reference until dsa_unregister_switch() / dsa_switch_shutdown()? 1: Maybe yes. A switch device will still be registered even if all user ports failed to probe, see commit 86f8b1c01a0a ("net: dsa: Do not make user port errors fatal"), and the cpu_dp->conduit pointers remain valid. I haven't audited all call paths to see whether they will actually use the conduit in lack of any user port, but if they do, it seems safer to not rely on user ports for that reference. 2. Definitely yes. We support changing the conduit which a user port is associated to, and we can get into a situation where we've moved all user ports away from a conduit, thus no longer hold any reference to it via the net device tracker. But we shouldn't let it go nonetheless - see the next change in relation to dsa_tree_find_first_conduit() and LAG conduits which disappear. We have to be prepared to return to the physical conduit, so the CPU port must explicitly keep another reference to it. This is also to say: the user ports and their CPU ports may not always keep a reference to the same conduit net device, and both are needed. As for the conduit's kobject for the /sys/class/net/ entry, we don't care about it, we can release it as soon as we hold the net device object itself. History and blame attribution ---------------------------- The code has been refactored so many times, it is very difficult to follow and properly attribute a blame, but I'll try to make a short history which I hope to be correct. We have two distinct probing paths: - one for OF, introduced in 2016 i ---truncated---	N/A	More Details
CVE-2025-71151	In the Linux kernel, the following vulnerability has been resolved: cifs: Fix memory and information leak in smb3_reconfigure() In smb3_reconfigure(), if smb3_sync_session_ctx_passwords() fails, the function returns immediately without freeing and erasing the newly allocated new_password and new_password2. This causes both a memory leak and a potential information leak. Fix this by calling kfree_sensitive() on both password buffers before returning in this error case.	N/A	More Details

CVE-2026-0776	Discord Client Uncontrolled Search Path Element Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Discord Client. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the discord_rpc module. The product loads a file from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of a target user. Was ZDI-CAN-27057.	N/A	More Details
CVE-2026-0791	ALGO 8180 IP Audio Alerter SIP INVITE Replaces Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the Replaces header of SIP INVITE requests. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28300.	N/A	More Details
CVE-2026-0790	ALGO 8180 IP Audio Alerter Web UI Direct Request Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the web-based user interface. By navigating directly to a URL, a user can gain unauthorized access to data. An attacker can leverage this vulnerability to disclose information in the context of the device. Was ZDI-CAN-28299.	N/A	More Details
CVE-2026-0789	ALGO 8180 IP Audio Alerter Web UI Inclusion of Authentication Cookie in Response Body Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the web-based user interface. The issue results from the lack of proper management of sensitive information. An attacker can leverage this vulnerability to disclose information in the context of the device. Was ZDI-CAN-28297.	N/A	More Details
CVE-2026-0788	ALGO 8180 IP Audio Alerter Web UI Persistent Cross-Site Scripting Vulnerability. This vulnerability allows remote attackers to execute web requests with a target user's privileges on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the functionality for viewing the syslog. The issue results from the lack of proper validation of user-supplied data, which can lead to the injection of an arbitrary script. An attacker can leverage this vulnerability to interact with the application in the context of the target user. Was ZDI-CAN-28298.	N/A	More Details
CVE-2026-0787	ALGO 8180 IP Audio Alerter SAC Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SAC module. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28296.	N/A	More Details
CVE-2026-0786	ALGO 8180 IP Audio Alerter SCI Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is required to exploit this vulnerability. The specific flaw exists within the SCI module. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28295.	N/A	More Details
CVE-2026-	ALGO 8180 IP Audio Alerter API Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is required to exploit this vulnerability. The specific flaw exists within the API interface. The issue results from	N/A	More Details

0785	the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28294.		
CVE-2026-0784	ALGO 8180 IP Audio Alerter Web UI Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is required to exploit this vulnerability. The specific flaw exists within the web-based user interface. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28293.	N/A	More Details
CVE-2026-0783	ALGO 8180 IP Audio Alerter Web UI Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is required to exploit this vulnerability. The specific flaw exists within the web-based user interface. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28292.	N/A	More Details
CVE-2026-0782	ALGO 8180 IP Audio Alerter Web UI Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is required to exploit this vulnerability. The specific flaw exists within the web-based user interface. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28291.	N/A	More Details
CVE-2026-24020	Rejected reason: Not used	N/A	More Details
CVE-2026-0780	ALGO 8180 IP Audio Alerter Web UI Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is required to exploit this vulnerability. The specific flaw exists within the web-based user interface. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28289.	N/A	More Details
CVE-2026-0779	ALGO 8180 IP Audio Alerter Ping Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is required to exploit this vulnerability. The specific flaw exists within the web-based user interface. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-25568.	N/A	More Details
CVE-2026-0778	Enel X JuiceBox 40 Telnet Service Missing Authentication Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Enel X JuiceBox 40 charging stations. Authentication is not required to exploit this vulnerability. The specific flaw exists within the telnet service, which listens on TCP port 2000 by default. The issue results from the lack of authentication prior to allowing remote connections. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-23285.	N/A	More Details
CVE-2026-0775	npm cli Incorrect Permission Assignment Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of npm cli. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of modules. The application loads modules from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of a target user. Was ZDI-CAN-25430.	N/A	More Details

CVE-2026-0793	ALGO 8180 IP Audio Alerter InformaCast Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the InformaCast functionality. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28302.	N/A	More Details
CVE-2026-0774	WatchYourLAN Configuration Page Argument Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of WatchYourLAN. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the arpstrs parameter. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-26708.	N/A	More Details
CVE-2026-0773	Upsonic Cloudpickle Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Upsonic. Authentication is not required to exploit this vulnerability. The specific flaw exists within the add_tool endpoint, which listens on TCP port 7541 by default. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-26845.	N/A	More Details
CVE-2026-0772	Langflow Disk Cache Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Langflow. Authentication is required to exploit this vulnerability. The specific flaw exists within the disk cache service. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-27919.	N/A	More Details
CVE-2026-0771	Langflow PythonFunction Code Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Langflow. Attack vectors and exploitability will vary depending on the configuration of the product. The specific flaw exists within the handling of Python function components. Depending upon product configuration, an attacker may be able to introduce custom Python code into a workflow. An attacker can leverage this vulnerability to execute code in the context of the application. Was ZDI-CAN-27497.	N/A	More Details
CVE-2026-0770	Langflow exec_globals Inclusion of Functionality from Untrusted Control Sphere Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Langflow. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the exec_globals parameter provided to the validate endpoint. The issue results from the inclusion of a resource from an untrusted control sphere. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27325.	N/A	More Details
CVE-2026-0769	Langflow eval_custom_component_code Eval Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Langflow. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of eval_custom_component_code function. The issue results from the lack of proper validation of a user-supplied string before using it to execute python code. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26972.	N/A	More Details
CVE-2026-0768	Langflow code Code Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Langflow. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the code parameter provided to the validate endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute	N/A	More Details

	Python code. An attacker can leverage this vulnerability to execute code in the context of root. . Was ZDI-CAN-27322.		
CVE-2026-0767	Open WebUI Cleartext Transmission of Credentials Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of Open WebUI. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of credentials provided to the endpoint. The issue results from transmitting sensitive information in plaintext. An attacker can leverage this vulnerability to disclose transmitted credentials, leading to further compromise. Was ZDI-CAN-28259.	N/A	More Details
CVE-2026-0766	Open WebUI load_tool_module_by_id Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Open WebUI. Authentication is required to exploit this vulnerability. The specific flaw exists within the load_tool_module_by_id function. The issue results from the lack of proper validation of a user-supplied string before using it to execute Python code. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-28257.	N/A	More Details
CVE-2026-0765	Open WebUI PIP install_frontmatter_requirements Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Open WebUI. Authentication is required to exploit this vulnerability. The specific flaw exists within the install_frontmatter_requirements function.The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-28258.	N/A	More Details
CVE-2026-0764	GPT Academic upload Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GPT Academic. Authentication is not required to exploit this vulnerability. The specific flaw exists within the upload endpoint. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27957.	N/A	More Details
CVE-2026-0763	GPT Academic run_in_subprocess_wrapper_func Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GPT Academic. Authentication is not required to exploit this vulnerability. The specific flaw exists within the run_in_subprocess_wrapper_func function. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27958.	N/A	More Details
CVE-2026-0762	GPT Academic stream_daas Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GPT Academic. Interaction with a malicious DAAS server is required to exploit this vulnerability but attack vectors may vary depending on the implementation. The specific flaw exists within the stream_daas function. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27956.	N/A	More Details
CVE-2026-0761	Foundation Agents MetaGPT actionoutput_str_to_mapping Code Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foundation Agents MetaGPT. Authentication is not required to exploit this vulnerability. The specific flaw exists within the actionoutput_str_to_mapping function. The issue results from the lack of proper validation of a user-supplied string before using it to execute Python code. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-28124.	N/A	More Details
	ALGO 8180 IP Audio Alerter SIP INVITE Alert-Info Stack-based Buffer Overflow Remote Code		

CVE-2026-0792	Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the Alert-Info header of SIP INVITE requests. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28301.	N/A	More Details
CVE-2026-0794	ALGO 8180 IP Audio Alerter SIP Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of SIP calls. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28303.	N/A	More Details
CVE-2025-71150	In the Linux kernel, the following vulnerability has been resolved: ksmbd: Fix refcount leak when invalid session is found on session lookup When a session is found but its state is not SMB2_SESSION_VALID, It indicates that no valid session was found, but it is missing to decrement the reference count acquired by the session lookup, which results in a reference count leak. This patch fixes the issue by explicitly calling ksmbd_user_session_put to release the reference to the session.	N/A	More Details
CVE-2026-0758	mcp-server-siri-shortcuts shortcutName Command Injection Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of mcp-server-siri-shortcuts. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the shortcutName parameter. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the service account. Was ZDI-CAN-27910.	N/A	More Details
CVE-2025-71149	In the Linux kernel, the following vulnerability has been resolved: io_uring/poll: correctly handle io_poll_add() return value on update When the core of io_uring was updated to handle completions consistently and with fixed return codes, the POLL_REMOVE opcode with updates got slightly broken. If a POLL_ADD is pending and then POLL_REMOVE is used to update the events of that request, if that update causes the POLL_ADD to now trigger, then that completion is lost and a CQE is never posted. Additionally, ensure that if an update does cause an existing POLL_ADD to complete, that the completion value isn't always overwritten with -ECANCELED. For that case, whatever io_poll_add() set the value to should just be retained.	N/A	More Details
CVE-2025-71148	In the Linux kernel, the following vulnerability has been resolved: net/handshake: restore destructor on submit failure handshake_req_submit() replaces sk->sk_destruct but never restores it when submission fails before the request is hashed. handshake_sk_destruct() then returns early and the original destructor never runs, leaking the socket. Restore sk_destruct on the error path.	N/A	More Details
CVE-2025-71147	In the Linux kernel, the following vulnerability has been resolved: KEYS: trusted: Fix a memory leak in tpm2_load_cmd 'tpm2_load_cmd' allocates a tempoary blob indirectly via 'tpm2_key_decode' but it is not freed in the failure paths. Address this by wrapping the blob into with a cleanup helper.	N/A	More Details
CVE-2025-71146	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conncount: fix leaked ct in error paths There are some situations where ct might be leaked as error paths are skipping the refcounted check and return immediately. In order to solve it make sure that the check is always called.	N/A	More Details
CVE-2025-68027	Incorrect Privilege Assignment vulnerability in Themefic Hydra Booking hydra-booking allows Privilege Escalation.This issue affects Hydra Booking: from n/a through <= 1.1.32.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: usb: phy: isp1301: fix		

CVE-2025-71145	non-OF device reference imbalance A recent change fixing a device reference leak in a UDC driver introduced a potential use-after-free in the non-OF case as the isp1301_get_client() helper only increases the reference count for the returned I2C device in the OF case. Increment the reference count also for non-OF so that the caller can decrement it unconditionally. Note that this is inherently racy just as using the returned I2C device is since nothing is preventing the PHY driver from being unbound while in use.	N/A	More Details
CVE-2025-68030	Server-Side Request Forgery (SSRF) vulnerability in WP Messiah Frontis Blocks frontis-blocks allows Server Side Request Forgery.This issue affects Frontis Blocks: from n/a through <= 1.1.5.	N/A	More Details
CVE-2025-68034	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CleverReach® CleverReach® WP cleverreach-wp allows SQL Injection.This issue affects CleverReach® WP: from n/a through <= 1.5.22.	N/A	More Details
CVE-2026-0757	MCP Manager for Claude Desktop execute-command Command Injection Sandbox Escape Vulnerability. This vulnerability allows remote attackers to bypass the sandbox on affected installations of MCP Manager for Claude Desktop. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of MCP config objects. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to escape the sandbox and execute arbitrary code in the context of the current process at medium integrity. Was ZDI-CAN-27810.	N/A	More Details
CVE-2025-68035	Insertion of Sensitive Information Into Sent Data vulnerability in tabbyai Tabby Checkout tabby-checkout allows Retrieve Embedded Sensitive Data.This issue affects Tabby Checkout: from n/a through <= 5.8.4.	N/A	More Details
CVE-2025-68039	Missing Authorization vulnerability in Chris Simmons WP BackItUp wp-backitup allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP BackItUp: from n/a through <= 2.0.0.	N/A	More Details
CVE-2025-68041	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codisto Omnichannel for WooCommerce codistoconnect allows Stored XSS.This issue affects Omnichannel for WooCommerce: from n/a through <= 1.3.65.	N/A	More Details
CVE-2025-68046	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in ThemeHunk Contact Form & Lead Form Elementor Builder lead-form-builder allows Retrieve Embedded Sensitive Data.This issue affects Contact Form & Lead Form Elementor Builder: from n/a through <= 2.0.1.	N/A	More Details
CVE-2025-68047	Deserialization of Untrusted Data vulnerability in Arraytics Eventin wp-event-solution allows Object Injection.This issue affects Eventin: from n/a through <= 4.1.1.	N/A	More Details
CVE-2025-68057	Missing Authorization vulnerability in e-plugins Hospital Doctor Directory hospital-doctor-directory allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Hospital Doctor Directory: from n/a through <= 1.3.9.	N/A	More Details
CVE-2026-0795	ALGO 8180 IP Audio Alerter Web UI Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is required to exploit this vulnerability. The specific flaw exists within the web-based user interface. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28321.	N/A	More Details
CVE-2025-68058	Missing Authorization vulnerability in e-plugins Institutions Directory institutions-directory allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Institutions Directory: from n/a through <= 1.3..4.	N/A	More Details
CVE-2026-24342	Rejected reason: Not used	N/A	More Details

CVE-2026-24341	Rejected reason: Not used	N/A	More Details
CVE-2026-24340	Rejected reason: Not used	N/A	More Details
CVE-2026-24339	Rejected reason: Not used	N/A	More Details
CVE-2026-24338	Rejected reason: Not used	N/A	More Details
CVE-2026-24337	Rejected reason: Not used	N/A	More Details
CVE-2026-24336	Rejected reason: Not used	N/A	More Details
CVE-2026-24335	Rejected reason: Not used	N/A	More Details
CVE-2026-24334	Rejected reason: Not used	N/A	More Details
CVE-2025-68059	Missing Authorization vulnerability in e-plugins Hotel Listing hotel-listing allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Hotel Listing: from n/a through <= 1.4.2.	N/A	More Details
CVE-2025-68072	Missing Authorization vulnerability in Merv Barrett Easy Property Listings easy-property-listings allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Easy Property Listings: from n/a through <= 3.5.17.	N/A	More Details
CVE-2025-68507	Missing Authorization vulnerability in Icegram Icegram icegram allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Icegram: from n/a through <= 3.1.35.	N/A	More Details
CVE-2026-0796	ALGO 8180 IP Audio Alerter Web UI Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is required to exploit this vulnerability. The specific flaw exists within the web-based user interface. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28322.	N/A	More Details
CVE-2025-67958	Missing Authorization vulnerability in Taxcloud TaxCloud for WooCommerce simple-sales-tax allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects TaxCloud for WooCommerce: from n/a through <= 8.3.8.	N/A	More Details
CVE-2025-67956	Missing Authorization vulnerability in wpeverest User Registration user-registration allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects User Registration: from n/a through <= 4.4.6.	N/A	More Details
CVE-2025-69060	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes uReach ureach allows PHP Local File Inclusion.This issue affects uReach: from n/a through <= 1.3.3.	N/A	More Details

CVE-2024-53248	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2025-69056	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins Hotel Listing hotel-listing allows Reflected XSS.This issue affects Hotel Listing: from n/a through <= 1.4.0.	N/A	More Details
CVE-2025-69057	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Edge-Themes Eldon eldon allows PHP Local File Inclusion.This issue affects Eldon: from n/a through <= 1.0.	N/A	More Details
CVE-2024-53252	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2024-53251	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2024-53250	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2024-53249	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2025-69058	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes PartyMaker partymaker allows PHP Local File Inclusion.This issue affects PartyMaker: from n/a through <= 1.1.15.	N/A	More Details
CVE-2025-67955	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in TangibleWP MyHome Core myhome-core allows PHP Local File Inclusion.This issue affects MyHome Core: from n/a through <= 4.1.0.	N/A	More Details
CVE-2024-45743	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2024-45742	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2024-45730	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2024-45729	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2024-45728	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2024-45727	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2025-69055	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in SeaTheme BM Content Builder bm-builder allows Path Traversal.This issue affects BM Content Builder: from n/a through <= 3.16.3.	N/A	More Details

CVE-2025-69044	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in goalthemes Vango vango allows PHP Local File Inclusion.This issue affects Vango: from n/a through <= 1.3.3.	N/A	More Details
CVE-2026-1225	ACE vulnerability in configuration file processing by QOS.CH logback-core up to and including version 1.5.24 in Java applications, allows an attacker to instantiate classes already present on the class path by compromising an existing logback configuration file. The instantiation of a potentially malicious Java class requires that said class is present on the user's class-path. In addition, the attacker must have write access to a configuration file. However, after successful instantiation, the instance is very likely to be discarded with no further ado.	N/A	More Details
CVE-2025-69038	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in goalthemes Hyori hyori allows PHP Local File Inclusion.This issue affects Hyori: from n/a through <= 1.3.6.	N/A	More Details
CVE-2026-24649	Rejected reason: Not used	N/A	More Details
CVE-2026-24648	Rejected reason: Not used	N/A	More Details
CVE-2026-24647	Rejected reason: Not used	N/A	More Details
CVE-2026-24646	Rejected reason: Not used	N/A	More Details
CVE-2026-24645	Rejected reason: Not used	N/A	More Details
CVE-2026-24644	Rejected reason: Not used	N/A	More Details
CVE-2026-24643	Rejected reason: Not used	N/A	More Details
CVE-2026-24642	Rejected reason: Not used	N/A	More Details
CVE-2025-67683	Quick.Cart is vulnerable to reflected XSS via the sSort parameter. An attacker can craft a malicious URL which, when opened, results in arbitrary JavaScript execution in the victim’s browser. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.7 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-67684	Quick.Cart is vulnerable to Local File Inclusion and Path Traversal issues in the theme selection mechanism. Quick.Cart allows a privileged user to upload arbitrary file contents while only validating the filename extension. This allows an attacker to include and execute uploaded PHP code, resulting in Remote Code Execution on the server. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.7 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
	Storing Passwords in a Recoverable Format vulnerability in Automated Logic WebCTRL on		

CVE-2025-14295	Windows, Carrier i-Vu on Windows. Storing Passwords in a Recoverable Format vulnerability (CWE-257) in the Web session management component allows an attacker to access stored passwords in a recoverable format which makes them subject to password reuse attacks by malicious users.This issue affects WebCTRL: from 6.0 through 9.0; i-Vu: from 6.0 through 9.0.	N/A	More Details
CVE-2025-12738	Neo4j Enterprise edition versions prior to 2025.11.2 and 5.26.17 are vulnerable to a potential information disclosure by an attacker who has some legitimate access to the database. The vulnerability allows attacker without read access to a property to infer information about its value by trying to enumerate all possible values through observing error messages of SET property. We recommend upgrading to 2025.11.2 or 5.26.17 and above, where the issues is fixed.	N/A	More Details
CVE-2025-15523	MacOS version of Inkscape bundles a Python interpreter that inherits the Transparency, Consent, and Control (TCC) permissions granted by the user to the main application bundle. An attacker with local user access can invoke this interpreter with arbitrary commands or scripts, leveraging the application's previously granted TCC permissions to access user's files in privacy-protected folders without triggering user prompts. Accessing other resources beyond previously granted TCC permissions will prompt the user for approval in the name of Inkscape, potentially disguising attacker's malicious intent. This issue has been fixed in 1.4.3 version of Inkscape.	N/A	More Details
CVE-2024-45726	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2025-69059	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes DiveIt diveit allows PHP Local File Inclusion.This issue affects DiveIt: from n/a through <= 1.4.3.	N/A	More Details
CVE-2024-45725	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2026-23004	In the Linux kernel, the following vulnerability has been resolved: dst: fix races in rt6_uncached_list_del() and rt_del_uncached_list() syzbot was able to crash the kernel in rt6_uncached_list_flush_dev() in an interesting way [1] Crash happens in list_del_init()/INIT_LIST_HEAD() while writing list->prev, while the prior write on list->next went well. static inline void INIT_LIST_HEAD(struct list_head *list) { WRITE_ONCE(list->next, list); // This went well WRITE_ONCE(list->prev, list); // Crash, @list has been freed. } Issue here is that rt6_uncached_list_del() did not attempt to lock ul->lock, as list_empty(&rt->dst.rt_uncached) returned true because the WRITE_ONCE(list->next, list) happened on the other CPU. We might use list_del_init_careful() and list_empty_careful(), or make sure rt6_uncached_list_del() always grabs the spinlock whenever rt->dst.rt_uncached_list has been set. A similar fix is neeed for IPv4. [1] BUG: KASAN: slab-use-after-free in INIT_LIST_HEAD include/linux/list.h:46 [inline] BUG: KASAN: slab-use-after-free in list_del_init include/linux/list.h:296 [inline] BUG: KASAN: slab-use-after-free in rt6_uncached_list_flush_dev net/ipv6/route.c:191 [inline] BUG: KASAN: slab-use-after-free in rt6_disable_ip+0x633/0x730 net/ipv6/route.c:5020 Write of size 8 at addr ffff8880294cfa78 by task kworker/u8:14/3450 CPU: 0 UID: 0 PID: 3450 Comm: kworker/u8:14 Tainted: G L syzkaller #0 PREEMPT_{RT,(full)} Tainted: [L]=SOFTLOCKUP Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/25/2025 Workqueue: netns cleanup_net Call Trace: <TASK> dump_stack_lvl+0xe8/0x150 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xca/0x240 mm/kasan/report.c:482 kasan_report+0x118/0x150 mm/kasan/report.c:595 INIT_LIST_HEAD include/linux/list.h:46 [inline] list_del_init include/linux/list.h:296 [inline] rt6_uncached_list_flush_dev net/ipv6/route.c:191 [inline] rt6_disable_ip+0x633/0x730 net/ipv6/route.c:5020 addrconf_ifdown+0x143/0x18a0 net/ipv6/addrconf.c:3853 addrconf_notify+0x1bc/0x1050 net/ipv6/addrconf.c:-1 notifier_call_chain+0x19d/0x3a0 kernel/notifier.c:85 call_netdevice_notifiers_extack net/core/dev.c:2268 [inline] call_netdevice_notifiers net/core/dev.c:2282 [inline] netif_close_many+0x29c/0x410 net/core/dev.c:1785 unregister_netdevice_many_notify+0xb50/0x2330 net/core/dev.c:12353 ops_exit_rtnl_list net/core/net_namespace.c:187 [inline]	N/A	More Details

	ops_undo_list+0x3dc/0x990 net/core/net_namespace.c:248 cleanup_net+0x4de/0x7b0 net/core/net_namespace.c:696 process_one_work kernel/workqueue.c:3257 [inline] process_scheduled_works+0xad1/0x1770 kernel/workqueue.c:3340 worker_thread+0x8a0/0xda0 kernel/workqueue.c:3421 kthread+0x711/0x8a0 kernel/kthread.c:463 ret_from_fork+0x510/0xa50 arch/x86/kernel/process.c:158 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:246 </TASK> Allocated by task 803: kasan_save_stack mm/kasan/common.c:57 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:78 unpoison_slab_object mm/kasan/common.c:340 [inline] __kasan_slab_alloc+0x6c/0x80 mm/kasan/common.c:366 kasan_slab_alloc include/linux/kasan.h:253 [inline] slab_post_alloc_hook mm/slub.c:4953 [inline] slab_alloc_node mm/slub.c:5263 [inline] kmem_cache_alloc_noprof+0x18d/0x6c0 mm/slub.c:5270 dst_alloc+0x105/0x170 net/core/dst.c:89 ip6_dst_alloc net/ipv6/route.c:342 [inline] icmp6_dst_alloc+0x75/0x460 net/ipv6/route.c:3333 mld_sendpack+0x683/0xe60 net/ipv6/mcast.c:1844 mld_send_cr net/ipv6/mcast.c:2154 [inline] mld_ifc_work+0x83e/0xd60 net/ipv6/mcast.c:2693 process_one_work kernel/workqueue.c:3257 [inline] process_scheduled_works+0xad1/0x1770 kernel/workqueue.c:3340 worker_thread+0x8a0/0xda0 kernel/workqueue.c:3421 kthread+0x711/0x8a0 kernel/kthread.c:463 ret_from_fork+0x510/0xa50 arch/x86/kernel/process.c:158 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entr ---truncated---		
CVE-2023-22928	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2023-22929	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2023-22930	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2023-22944	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2023-32718	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2026-23013	In the Linux kernel, the following vulnerability has been resolved: net: octeon_ep_vf: fix free_irq dev_id mismatch in IRQ rollback octep_vf_request_irqs() requests MSI-X queue IRQs with dev_id set to ioq_vector. If request_irq() fails part-way, the rollback loop calls free_irq() with dev_id set to 'oct', which does not match the original dev_id and may leave the irqaction registered. This can keep IRQ handlers alive while ioq_vector is later freed during unwind/teardown, leading to a use-after-free or crash when an interrupt fires. Fix the error path to free IRQs with the same ioq_vector dev_id used during request_irq().	N/A	More Details
CVE-2026-23012	In the Linux kernel, the following vulnerability has been resolved: mm/damon/core: remove call_control in inactive contexts If damon_call() is executed against a DAMON context that is not running, the function returns error while keeping the damon_call_control object linked to the context's call_controls list. Let's suppose the object is deallocated after the damon_call(), and yet another damon_call() is executed against the same context. The function tries to add the new damon_call_control object to the call_controls list, which still has the pointer to the previous damon_call_control object, which is deallocated. As a result, use-after-free happens. This can actually be triggered using the DAMON sysfs interface. It is not easily exploitable since it requires the sysfs write permission and making a definitely weird file writes, though. Please refer to the report for more details about the issue reproduction steps. Fix the issue by making two changes. Firstly, move the final kdamond_call() for cancelling all existing damon_call() requests from terminating DAMON context to be done before the ctx->kdamond reset. This makes any code that sees NULL	N/A	More Details

	ctx->kdamond can safely assume the context may not access damon_call() requests anymore. Secondly, let damon_call() to cleanup the damon_call_control objects that were added to the already-terminated DAMON context, before returning the error.		
CVE-2026-23011	In the Linux kernel, the following vulnerability has been resolved: ipv4: ip_gre: make ipgre_header() robust Analog to commit db5b4e39c4e6 ("ip6_gre: make ip6gre_header() robust") Over the years, syzbot found many ways to crash the kernel in ipgre_header() [1]. This involves team or bonding drivers ability to dynamically change their dev->needed_headroom and/or dev->hard_header_len In this particular crash mld_newpack() allocated an skb with a too small reserve/headroom, and by the time mld_sendpack() was called, syzbot managed to attach an ipgre device. [1] skbuff: skb_under_panic: text:ffffffff89ea3cb7 len:2030915468 put:2030915372 head:ffff888058b43000 data:ffff887fdfa6e194 tail:0x120 end:0x6c0 dev:team0 kernel BUG at net/core/skbuff.c:213 ! Oops: invalid opcode: 0000 [#1] SMP KASAN PTI CPU: 1 UID: 0 PID: 1322 Comm: kworker/1:9 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/25/2025 Workqueue: mld mld_ifc_work RIP: 0010:skb_panic+0x157/0x160 net/core/skbuff.c:213 Call Trace: <TASK> skb_under_panic net/core/skbuff.c:223 [inline] skb_push+0xc3/0xe0 net/core/skbuff.c:2641 ipgre_header+0x67/0x290 net/ipv4/ip_gre.c:897 dev_hard_header include/linux/netdevice.h:3436 [inline] neigh_connected_output+0x286/0x460 net/core/neighbour.c:1618 NF_HOOK_COND include/linux/netfilter.h:307 [inline] ip6_output+0x340/0x550 net/ipv6/ip6_output.c:247 NF_HOOK+0x9e/0x380 include/linux/netfilter.h:318 mld_sendpack+0x8d4/0xe60 net/ipv6/mcast.c:1855 mld_send_cr net/ipv6/mcast.c:2154 [inline] mld_ifc_work+0x83e/0xd60 net/ipv6/mcast.c:2693 process_one_work kernel/workqueue.c:3257 [inline] process_scheduled_works+0xad1/0x1770 kernel/workqueue.c:3340 worker_thread+0x8a0/0xda0 kernel/workqueue.c:3421 kthread+0x711/0x8a0 kernel/kthread.c:463 ret_from_fork+0x510/0xa50 arch/x86/kernel/process.c:158 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:246	N/A	More Details
CVE-2026-23010	In the Linux kernel, the following vulnerability has been resolved: ipv6: Fix use-after-free in inet6_addr_del(). syzbot reported use-after-free of inet6_ifaddr in inet6_addr_del(). [0] The cited commit accidentally moved ipv6_del_addr() for mngtmpaddr before reading its ifp->flags for temporary addresses in inet6_addr_del(). Let's move ipv6_del_addr() down to fix the UAF. [0]: BUG: KASAN: slab-use-after-free in inet6_addr_del.constprop.0+0x67a/0x6b0 net/ipv6/addrconf.c:3117 Read of size 4 at addr ffff88807b89c86c by task syz.3.1618/9593 CPU: 0 UID: 0 PID: 9593 Comm: syz.3.1618 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/25/2025 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x116/0x1f0 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xcd/0x630 mm/kasan/report.c:482 kasan_report+0xe0/0x110 mm/kasan/report.c:595 inet6_addr_del.constprop.0+0x67a/0x6b0 net/ipv6/addrconf.c:3117 addrconf_del_ifaddr+0x11e/0x190 net/ipv6/addrconf.c:3181 inet6_ioctl+0x1e5/0x2b0 net/ipv6/af_inet6.c:582 sock_do_ioctl+0x118/0x280 net/socket.c:1254 sock_ioctl+0x227/0x6b0 net/socket.c:1375 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:597 [inline] __se_sys_ioctl fs/ioctl.c:583 [inline] __x64_sys_ioctl+0x18e/0x210 fs/ioctl.c:583 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xcd/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f164cf8f749 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f164de64038 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 00007f164d1e5fa0 RCX: 00007f164cf8f749 RDX: 0000200000000000 RSI: 0000000000008936 RDI: 0000000000000003 RBP: 00007f164d013f91 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007f164d1e6038 R14: 00007f164d1e5fa0 R15: 00007ffde15c8288 </TASK> Allocated by task 9593: kasan_save_stack+0x33/0x60 mm/kasan/common.c:56 kasan_save_track+0x14/0x30 mm/kasan/common.c:77 poison_kmalloc_redzone mm/kasan/common.c:397 [inline] __kasan_kmalloc+0xaa/0xb0 mm/kasan/common.c:414 kmalloc_noprof include/linux/slab.h:957 [inline] kzalloc_noprof include/linux/slab.h:1094 [inline]	N/A	More Details

	ipv6_add_addr+0x4e3/0x2010 net/ipv6/addrconf.c:1120 inet6_addr_add+0x256/0x9b0 net/ipv6/addrconf.c:3050 addrconf_add_ifaddr+0x1fc/0x450 net/ipv6/addrconf.c:3160 inet6_ioctl+0x103/0x2b0 net/ipv6/af_inet6.c:580 sock_do_ioctl+0x118/0x280 net/socket.c:1254 sock_ioctl+0x227/0x6b0 net/socket.c:1375 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:597 [inline] __se_sys_ioctl fs/ioctl.c:583 [inline] __x64_sys_ioctl+0x18e/0x210 fs/ioctl.c:583 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xcd/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 6099: kasan_save_stack+0x33/0x60 mm/kasan/common.c:56 kasan_save_track+0x14/0x30 mm/kasan/common.c:77 kasan_save_free_info+0x3b/0x60 mm/kasan/generic.c:584 poison_slab_object mm/kasan/common.c:252 [inline] __kasan_slab_free+0x5f/0x80 mm/kasan/common.c:284 kasan_slab_free include/linux/kasan.h:234 [inline] slab_free_hook mm/slub.c:2540 [inline] slab_free_freelist_hook mm/slub.c:2569 [inline] slab_free_bulk mm/slub.c:6696 [inline] kmem_cache_free_bulk mm/slub.c:7383 [inline] kmem_cache_free_bulk+0x2bf/0x680 mm/slub.c:7362 kfree_bulk include/linux/slab.h:830 [inline] kvfree_rcu_bulk+0x1b7/0x1e0 mm/slab_common.c:1523 kvfree_rcu_drain_ready mm/slab_common.c:1728 [inline] kfree_rcu_monitor+0x1d0/0x2f0 mm/slab_common.c:1801 process_one_work+0x9ba/0x1b20 kernel/workqueue.c:3257 process_scheduled_works kernel/workqu ---truncated---		
CVE-2026-23009	In the Linux kernel, the following vulnerability has been resolved: xhci: sideband: don't dereference freed ring when removing sideband endpoint xhci_sideband_remove_endpoint() incorrecly assumes that the endpoint is running and has a valid transfer ring. Lianqin reported a crash during suspend/wake-up stress testing, and found the cause to be dereferencing a non-existing transfer ring 'ep->ring' during xhci_sideband_remove_endpoint(). The endpoint and its ring may be in unknown state if this function is called after xHCI was reinitialized in resume (lost power), or if device is being re-enumerated, disconnected or endpoint already dropped. Fix this by both removing unnecessary ring access, and by checking ep->ring exists before dereferencing it. Also make sure endpoint is running before attempting to stop it. Remove the xhci_initialize_ring_info() call during sideband endpoint removal as is it only initializes ring structure enqueue, dequeue and cycle state values to their starting values without changing actual hardware enqueue, dequeue and cycle state. Leaving them out of sync is worse than leaving it as it is. The endpoint will get freed in after this in most usecases. If the (audio) class driver want's to reuse the endpoint after offload then it is up to the class driver to ensure endpoint is properly set up.	N/A	More Details
CVE-2026-23008	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Fix KMS with 3D on HW version 10 HW version 10 does not have GB Surfaces so there is no backing buffer for surface backed FBs. This would result in a nullptr dereference and crash the driver causing a black screen.	N/A	More Details
CVE-2026-23007	In the Linux kernel, the following vulnerability has been resolved: block: zero non-PI portion of auto integrity buffer The auto-generated integrity buffer for writes needs to be fully initialized before being passed to the underlying block device, otherwise the uninitialized memory can be read back by userspace or anyone with physical access to the storage device. If protection information is generated, that portion of the integrity buffer is already initialized. The integrity data is also zeroed if PI generation is disabled via sysfs or the PI tuple size is 0. However, this misses the case where PI is generated and the PI tuple size is nonzero, but the metadata size is larger than the PI tuple. In this case, the remainder ("opaque") of the metadata is left uninitialized. Generalize the BLK_INTEGRITY_CSUM_NONE check to cover any case when the metadata is larger than just the PI tuple.	N/A	More Details
CVE-2026-23006	In the Linux kernel, the following vulnerability has been resolved: ASoC: tlv320adcx140: fix null pointer The "snd_soc_component" in "adcx140_priv" was only used once but never set. It was only used for reaching "dev" which is already present in "adcx140_priv".	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: x86/fpu: Clear XSTATE_BV[i] in guest XSAVE state whenever XFD[i]=1 When loading guest XSAVE state via KVM_SET_XSAVE, and when updating XFD in response to a guest WRMSR, clear XFD-disabled features in the saved (or to be restored) XSTATE_BV to ensure KVM doesn't		

CVE-2026-23005	attempt to load state for features that are disabled via the guest's XFD. Because the kernel executes XRSTOR with the guest's XFD, saving XSTATE_BV[i]=1 with XFD[i]=1 will cause XRSTOR to #NM and panic the kernel. E.g. if fpu_update_guest_xfd() sets XFD without clearing XSTATE_BV: ------------[cut here]------------ WARNING: arch/x86/kernel/traps.c:1524 at exc_device_not_available+0x101/0x110, CPU#29: amx_test/848 Modules linked in: kvm_intel kvm irqbypass CPU: 29 UID: 1000 PID: 848 Comm: amx_test Not tainted 6.19.0-rc2-ffa07f7fd437-x86_amx_nm_xfd_non_init-vm #171 NONE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 0.0.0 02/06/2015 RIP: 0010:exc_device_not_available+0x101/0x110 Call Trace: <TASK> asm_exc_device_not_available+0x1a/0x20 RIP: 0010:restore_fpregs_from_fpstate+0x36/0x90 switch_fpu_return+0x4a/0xb0 kvm_arch_vcpu_ioctl_run+0x1245/0x1e40 [kvm] kvm_vcpu_ioctl+0x2c3/0x8f0 [kvm] __x64_sys_ioctl+0x8f/0xd0 do_syscall_64+0x62/0x940 entry_SYSCALL_64_after_hwframe+0x4b/0x53 </TASK> ---[end trace 0000000000000000]--- This can happen if the guest executes WRMSR(MSR_IA32_XFD) to set XFD[18] = 1, and a host IRQ triggers kernel_fpu_begin() prior to the vmexit handler's call to fpu_update_guest_xfd(). and if userspace stuffs XSTATE_BV[i]=1 via KVM_SET_XSAVE: ------------[cut here]------------ WARNING: arch/x86/kernel/traps.c:1524 at exc_device_not_available+0x101/0x110, CPU#14: amx_test/867 Modules linked in: kvm_intel kvm irqbypass CPU: 14 UID: 1000 PID: 867 Comm: amx_test Not tainted 6.19.0-rc2-2dace9faccd6-x86_amx_nm_xfd_non_init-vm #168 NONE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 0.0.0 02/06/2015 RIP: 0010:exc_device_not_available+0x101/0x110 Call Trace: <TASK> asm_exc_device_not_available+0x1a/0x20 RIP: 0010:restore_fpregs_from_fpstate+0x36/0x90 fpu_swap_kvm_fpstate+0x6b/0x120 kvm_load_guest_fpu+0x30/0x80 [kvm] kvm_arch_vcpu_ioctl_run+0x85/0x1e40 [kvm] kvm_vcpu_ioctl+0x2c3/0x8f0 [kvm] __x64_sys_ioctl+0x8f/0xd0 do_syscall_64+0x62/0x940 entry_SYSCALL_64_after_hwframe+0x4b/0x53 </TASK> ---[end trace 0000000000000000]--- The new behavior is consistent with the AMX architecture. Per Intel's SDM, XSAVE saves XSTATE_BV as '0' for components that are disabled via XFD (and non-compacted XSAVE saves the initial configuration of the state component): If XSAVE, XSAVEC, XSAVEOPT, or XSAVES is saving the state component i, the instruction does not generate #NM when XCR0[i] = IA32_XFD[i] = 1; instead, it operates as if XINUSE[i] = 0 (and the state component was in its initial state): it saves bit i of XSTATE_BV field of the XSAVE header as 0; in addition, XSAVE saves the initial configuration of the state component (the other instructions do not save state component i). Alternatively, KVM could always do XRSTOR with XFD=0, e.g. by using a constant XFD based on the set of enabled features when XSAVEing for a struct fpu_guest. However, having XSTATE_BV[i]=1 for XFD-disabled features can only happen in the above interrupt case, or in similar scenarios involving preemption on preemptible kernels, because fpu_swap_kvm_fpstate()'s call to save_fpregs_to_fpstate() saves the outgoing FPU state with the current XFD; and that is (on all but the first WRMSR to XFD) the guest XFD. Therefore, XFD can only go out of sync with XSTATE_BV in the above interrupt case, or in similar scenarios involving preemption on preemptible kernels, and it we can consider it (de facto) part of KVM ABI that KVM_GET_XSAVE returns XSTATE_BV[i]=0 for XFD-disabled features. [Move clea ---truncated---	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: ip6_tunnel: use skb_vlan_inet_prepare() in __ip6_tnl_rcv() Blamed commit did not take care of VLAN encapsulations as spotted by syzbot [1]. Use skb_vlan_inet_prepare() instead of pskb_inet_may_pull(). [1] BUG: KMSAN: uninit-value in __INET_ECN_decapsulate include/net/inet_ecn.h:253 [inline] BUG: KMSAN: uninit-value in INET_ECN_decapsulate include/net/inet_ecn.h:275 [inline] BUG: KMSAN: uninit-value in IP6_ECN_decapsulate+0x7a8/0x1fa0 include/net/inet_ecn.h:321 __INET_ECN_decapsulate include/net/inet_ecn.h:253 [inline] INET_ECN_decapsulate include/net/inet_ecn.h:275 [inline] IP6_ECN_decapsulate+0x7a8/0x1fa0 include/net/inet_ecn.h:321 ip6ip6_dscp_ecn_decapsulate+0x16f/0x1b0 net/ipv6/ip6_tunnel.c:729 __ip6_tnl_rcv+0xed9/0x1b50 net/ipv6/ip6_tunnel.c:860 ip6_tnl_rcv+0xc3/0x100 net/ipv6/ip6_tunnel.c:903 gre_rcv+0x1529/0x1b90 net/ipv6/ip6_gre.c:-1 ip6_protocol_deliver_rcu+0x1c89/0x2c60 net/ipv6/ip6_input.c:438 ip6_input_finish+0x1f4/0x4a0 net/ipv6/ip6_input.c:489 NF_HOOK		

CVE-2026-23003	include/linux/netfilter.h:318 [inline] ip6_input+0x9c/0x330 net/ipv6/ip6_input.c:500 ip6_mc_input+0x7ca/0xc10 net/ipv6/ip6_input.c:590 dst_input include/net/dst.h:474 [inline] ip6_rcv_finish+0x958/0x990 net/ipv6/ip6_input.c:79 NF_HOOK include/linux/netfilter.h:318 [inline] ipv6_rcv+0xf1/0x3c0 net/ipv6/ip6_input.c:311 __netif_receive_skb_one_core net/core/dev.c:6139 [inline] __netif_receive_skb+0x1df/0xac0 net/core/dev.c:6252 netif_receive_skb_internal net/core/dev.c:6338 [inline] netif_receive_skb+0x57/0x630 net/core/dev.c:6397 tun_rx_batched+0x1df/0x980 drivers/net/tun.c:1485 tun_get_user+0x5c0e/0x6c60 drivers/net/tun.c:1953 tun_chr_write_iter+0x3e9/0x5c0 drivers/net/tun.c:1999 new_sync_write fs/read_write.c:593 [inline] vfs_write+0xbe2/0x15d0 fs/read_write.c:686 ksys_write fs/read_write.c:738 [inline] __do_sys_write fs/read_write.c:749 [inline] __se_sys_write fs/read_write.c:746 [inline] __x64_sys_write+0x1fb/0x4d0 fs/read_write.c:746 x64_sys_call+0x30ab/0x3e70 arch/x86/include/generated/asm/syscalls_64.h:2 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xd3/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:4960 [inline] slab_alloc_node mm/slub.c:5263 [inline] kmem_cache_alloc_node_noprof+0x9e7/0x17a0 mm/slub.c:5315 kmalloc_reserve+0x13c/0x4b0 net/core/skbuff.c:586 __alloc_skb+0x805/0x1040 net/core/skbuff.c:690 alloc_skb include/linux/skbuff.h:1383 [inline] alloc_skb_with_frags+0xc5/0xa60 net/core/skbuff.c:6712 sock_alloc_send_pskb+0xacc/0xc60 net/core/sock.c:2995 tun_alloc_skb drivers/net/tun.c:1461 [inline] tun_get_user+0x1142/0x6c60 drivers/net/tun.c:1794 tun_chr_write_iter+0x3e9/0x5c0 drivers/net/tun.c:1999 new_sync_write fs/read_write.c:593 [inline] vfs_write+0xbe2/0x15d0 fs/read_write.c:686 ksys_write fs/read_write.c:738 [inline] __do_sys_write fs/read_write.c:749 [inline] __se_sys_write fs/read_write.c:746 [inline] __x64_sys_write+0x1fb/0x4d0 fs/read_write.c:746 x64_sys_call+0x30ab/0x3e70 arch/x86/include/generated/asm/syscalls_64.h:2 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xd3/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f CPU: 0 UID: 0 PID: 6465 Comm: syz.0.17 Not tainted syzkaller #0 PREEMPT(none) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/25/2025	N/A	More Details
CVE-2024-45724	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2026-23002	In the Linux kernel, the following vulnerability has been resolved: lib/buildid: use __kernel_read() for sleepable context Prevent a "BUG: unable to handle kernel NULL pointer dereference in filemap_read_folio". For the sleepable context, convert freader to use __kernel_read() instead of direct page cache access via read_cache_folio(). This simplifies the faultable code path by using the standard kernel file reading interface which handles all the complexity of reading file data. At the moment we are not changing the code for non-sleepable context which uses filemap_get_folio() and only succeeds if the target folios are already in memory and up-to-date. The reason is to keep the patch simple and easier to backport to stable kernels. Syzbot repro does not crash the kernel anymore and the selftests run successfully. In the follow up we will make __kernel_read() with IOCB_NOWAIT work for non-sleepable contexts. In addition, I would like to replace the secretmem check with a more generic approach and will add fstest for the buildid code.	N/A	More Details
CVE-2026-23001	In the Linux kernel, the following vulnerability has been resolved: macvlan: fix possible UAF in macvlan_forward_source() Add RCU protection on (struct macvlan_source_entry)->vlan. Whenever macvlan_hash_del_source() is called, we must clear entry->vlan pointer before RCU grace period starts. This allows macvlan_forward_source() to skip over entries queued for freeing. Note that macvlan_dev are already RCU protected, as they are embedded in a standard netdev (netdev_priv(ndev)). https: //lore.kernel.org/netdev/695fb1e8.050a0220.1c677c.039f.GAE@google.com/T/#u	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix crash on profile change rollback failure mlx5e_netdev_change_profile can fail to attach a new profile and can fail to rollback to old profile, in such case, we could end up with a dangling netdev with a fully reset netdev_priv. A retry to change profile, e.g. another attempt to call		

CVE-2026-23000	mlx5e_netdev_change_profile via switchdev mode change, will crash trying to access the now NULL priv->mdev. This fix allows mlx5e_netdev_change_profile() to handle previous failures and an empty priv, by not assuming priv is valid. Pass netdev and mdev to all flows requiring mlx5e_netdev_change_profile() and avoid passing priv. In mlx5e_netdev_change_profile() check if current priv is valid, and if not, just attach the new profile without trying to access the old one. This fixes the following oops, when enabling switchdev mode for the 2nd time after first time failure: ## Enabling switchdev mode first time: mlx5_core 0012:03:00.1: E-Switch: Supported tc chains and prios offload 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: mlx5e_netdev_change_profile: failed to rollback to orig profile, -12 ^^^^^^^^ mlx5_core 0000:00:03.0: E-Switch: Disable: mode(LEGACY), nvfs(0), necvfs(0), active vports(0) ## retry: Enabling switchdev mode 2nd time: mlx5_core 0000:00:03.0: E-Switch: Supported tc chains and prios offload BUG: kernel NULL pointer dereference, address: 0000000000000038 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] SMP NOPTI CPU: 13 UID: 0 PID: 520 Comm: devlink Not tainted 6.18.0-rc4+ #91 PREEMPT(voluntary) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 RIP: 0010:mlx5e_detach_netdev+0x3c/0x90 Code: 50 00 00 f0 80 4f 78 02 48 8b bf e8 07 00 00 48 85 ff 74 16 48 8b 73 78 48 d1 ee 83 e6 01 83 f6 01 40 0f b6 f6 e8 c4 42 00 00 <48> 8b 45 38 48 85 c0 74 08 48 89 df e8 cc 47 40 1e 48 8b bb f0 07 RSP: 0018:ffffc90000673890 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffff8881036a89c0 RCX: 0000000000000000 RDX: ffff888113f63800 RSI: ffffffff822fe720 RDI: 0000000000000000 RBP: 0000000000000000 R08: 0000000000002dcd R09: 0000000000000000 R10: ffffc900006738e8 R11: 00000000ffffffff R12: 0000000000000000 R13: 0000000000000000 R14: ffff8881036a89c0 R15: 0000000000000000 FS: 00007fdfb8384740(0000) GS:ffff88856a9d6000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000038 CR3: 0000000112ae0005 CR4: 0000000000370ef0 Call Trace: <TASK> mlx5e_netdev_change_profile+0x45/0xb0 mlx5e_vport_rep_load+0x27b/0x2d0 mlx5_esw_offloads_rep_load+0x72/0xf0 esw_offloads_enable+0x5d0/0x970 mlx5_eswitch_enable_locked+0x349/0x430 ? is_mp_supported+0x57/0xb0 mlx5_devlink_eswitch_mode_set+0x26b/0x430 devlink_nl_eswitch_set_doit+0x6f/0xf0 genl_family_rcv_msg_doit+0xe8/0x140 genl_rcv_msg+0x18b/0x290 ? __pfx_devlink_nl_pre_doit+0x10/0x10 ? __pfx_devlink_nl_eswitch_set_doit+0x10/0x10 ? __pfx_devlink_nl_post_doit+0x10/0x10 ? __pfx_genl_rcv_msg+0x10/0x10 netlink_rcv_skb+0x52/0x100 genl_rcv+0x28/0x40 netlink_unicast+0x282/0x3e0 ? __alloc_skb+0xd6/0x190 netlink_sendmsg+0x1f7/0x430 __sys_sendto+0x213/0x220 ? __sys_recvmsg+0x6a/0xd0 __x64_sys_sendto+0x24/0x30 do_syscall_64+0x50/0x1f0 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7fdfb8495047	N/A	More Details
CVE-2026-22999	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_qfq: do not free existing class in qfq_change_class() Fixes qfq_change_class() error case. cl->qdisc and cl should only be freed if a new class and qdisc were allocated, or we risk various UAF.	N/A	More Details
CVE-2026-22998	In the Linux kernel, the following vulnerability has been resolved: nvme-tcp: fix NULL pointer dereferences in nvmet_tcp_build_pdu_iovec Commit efa56305908b ("nvmet-tcp: Fix a kernel panic when host sends an invalid H2C PDU length") added ttag bounds checking and data_offset validation in nvmet_tcp_handle_h2c_data_pdu(), but it did not validate whether the command's data structures (cmd->req.sg and cmd->iov) have been properly initialized before processing H2C_DATA PDUs. The nvmet_tcp_build_pdu_iovec() function dereferences these pointers without NULL checks. This can be triggered by sending H2C_DATA PDU immediately after the ICREQ/ICRESP handshake, before sending a CONNECT command or NVMe write command. Attack vectors that trigger NULL pointer dereferences: 1. H2C_DATA PDU sent before CONNECT → both pointers NULL 2. H2C_DATA PDU for READ command → cmd->req.sg allocated, cmd->iov NULL 3. H2C_DATA PDU for uninitialized command slot → both pointers NULL The fix validates both cmd->req.sg and cmd->iov before calling nvmet_tcp_build_pdu_iovec(). Both checks are required because: - Uninitialized commands: both NULL - READ commands: cmd->req.sg allocated, cmd->iov	N/A	More Details

	NULL - WRITE commands: both allocated		
CVE-2026-22997	In the Linux kernel, the following vulnerability has been resolved: net: can: j1939: j1939_xtp_rx_rts_session_active(): deactivate session upon receiving the second rts Since j1939_session_deactivate_activate_next() in j1939_tp_rxtimer() is called only when the timer is enabled, we need to call j1939_session_deactivate_activate_next() if we cancelled the timer. Otherwise, refcount for j1939_session leaks, which will later appear as | unregister_netdevice: waiting for vcan0 to become free. Usage count = 2. problem.	N/A	More Details
CVE-2026-22996	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Don't store mlx5e_priv in mlx5e_dev devlink priv mlx5e_priv is an unstable structure that can be memset(0) if profile attaching fails, mlx5e_priv in mlx5e_dev devlink private is used to reference the netdev and mdev associated with that struct. Instead, store netdev directly into mlx5e_dev and get mdev from the containing mlx5_adev aux device structure. 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: 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: 0000000000000520 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] SMP NOPTI CPU: 3 UID: 0 PID: 521 Comm: devlink Not tainted 6.18.0-rc5+ #117 PREEMPT(voluntary) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 RIP: 0010:mlx5e_remove+0x68/0x130 RSP: 0018:ffffc900034838f0 EFLAGS: 00010246 RAX: ffff88810283c380 RBX: ffff888101874400 RCX: ffffffff826ffc45 RDX: 0000000000000000 RSI: 0000000000000001 RDI: 0000000000000000 RBP: ffff888102d789c0 R08: ffff8881007137f0 R09: ffff888100264e10 R10: ffffc90003483898 R11: ffffc900034838a0 R12: ffff888100d261a0 R13: ffff888100d261a0 R14: ffff8881018749a0 R15: ffff888101874400 FS: 00007f8565fea740(0000) GS:ffff88856a759000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000520 CR3: 000000010b11a004 CR4: 0000000000370ef0 Call Trace: <TASK> 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-2025-71163	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: fix device leaks on compat bind and unbind Make sure to drop the reference taken when looking up the idxd device as part of the compat bind and unbind sysfs interface.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: dmaengine: tegra-adma: Fix use-after-free A use-after-free bug exists in the Tegra ADMA driver when audio streams are terminated, particularly during XRUN conditions. The issue occurs when the DMA buffer is freed by tegra_adma_terminate_all() before the vchan completion tasklet finishes accessing it. The race condition follows this sequence: 1. DMA transfer completes, triggering an interrupt that schedules the completion tasklet (tasklet has not executed yet) 2. Audio playback stops, calling tegra_adma_terminate_all() which frees the DMA buffer memory via kfree() 3. The scheduled tasklet finally executes, calling vchan_complete() which attempts to access the already-freed memory Since tasklets can execute at any time after being scheduled, there is no guarantee that the buffer will remain valid when vchan_complete() runs. Fix this by properly synchronizing the virtual channel completion: - Calling vchan_terminate_vdesc() in tegra_adma_stop() to mark the descriptors as terminated instead of freeing the descriptor. - Add the callback tegra_adma_synchronize() that calls vchan_synchronize() which kills any pending tasklets and frees any terminated		

CVE-2025-71162	descriptors. Crash logs: [337.427523] BUG: KASAN: use-after-free in vchan_complete+0x124/0x3b0 [337.427544] Read of size 8 at addr ffff000132055428 by task swapper/0/0 [337.427562] Call trace: [337.427564] dump_backtrace+0x0/0x320 [337.427571] show_stack+0x20/0x30 [337.427575] dump_stack_lvl+0x68/0x84 [337.427584] print_address_description.constprop.0+0x74/0x2b8 [337.427590] kasan_report+0x1f4/0x210 [337.427598] __asan_load8+0xa0/0xd0 [337.427603] vchan_complete+0x124/0x3b0 [337.427609] tasklet_action_common.constprop.0+0x190/0x1d0 [337.427617] tasklet_action+0x30/0x40 [337.427623] __do_softirq+0x1a0/0x5c4 [337.427628] irq_exit+0x110/0x140 [337.427633] handle_domain_irq+0xa4/0xe0 [337.427640] gic_handle_irq+0x64/0x160 [337.427644] call_on_irq_stack+0x20/0x4c [337.427649] do_interrupt_handler+0x7c/0x90 [337.427654] el1_interrupt+0x30/0x80 [337.427659] el1h_64_irq_handler+0x18/0x30 [337.427663] el1h_64_irq+0x7c/0x80 [337.427667] cpuidle_enter_state+0xe4/0x540 [337.427674] cpuidle_enter+0x54/0x80 [337.427679] do_idle+0x2e0/0x380 [337.427685] cpu_startup_entry+0x2c/0x70 [337.427690] rest_init+0x114/0x130 [337.427695] arch_call_rest_init+0x18/0x24 [337.427702] start_kernel+0x380/0x3b4 [337.427706] __primary_switched+0xc0/0xc8	N/A	More Details
CVE-2023-32719	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2023-32720	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2024-22166	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2024-36988	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. The CVE was never used.	N/A	More Details
CVE-2026-0760	Foundation Agents MetaGPT deserialize_message Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foundation Agents MetaGPT. Authentication is not required to exploit this vulnerability. The specific flaw exists within the deserialize_message function. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-28121.	N/A	More Details
CVE-2025-64097	NervesHub is a web service that allows users to manage over-the-air (OTA) firmware updates of devices in the field. A vulnerability present starting in version 1.0.0 and prior to version 2.3.0 allowed attackers to brute-force user API tokens due to the predictable format of previously issued tokens. Tokens included user-identifiable components and were not cryptographically secure, making them susceptible to guessing or enumeration. The vulnerability could have allowed unauthorized access to user accounts or API actions protected by these tokens. A fix is available in version 2.3.0 of NervesHub. This version introduces strong, cryptographically-random tokens using `:crypto.strong_rand_bytes/1`, hashing of tokens before database storage to prevent misuse even if the database is compromised, and context-aware token storage to distinguish between session and API tokens. There are no practical workarounds for this issue other than upgrading. In sensitive environments, as a temporary mitigation, firewalling access to the NervesHub server can help limit exposure until an upgrade is possible.	N/A	More Details
CVE-2023-7335	EduSoho versions prior to 22.4.7 contain an arbitrary file read vulnerability in the classroom-course-statistics export functionality. A remote, unauthenticated attacker can supply crafted path traversal sequences in the fileNames[] parameter to read arbitrary files from the server filesystem, including application configuration files such as config/parameters.yml that may contain secrets and database credentials. Exploitation evidence was observed by the Shadowserver Foundation on 2026-01-19 (UTC).	N/A	More Details

CVE-2025-69037	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in goalthemes Pippo pippo allows PHP Local File Inclusion.This issue affects Pippo: from n/a through <= 1.2.3.	N/A	More Details
CVE-2026-22983	In the Linux kernel, the following vulnerability has been resolved: net: do not write to msg_get_inq in callee NULL pointer dereference fix. msg_get_inq is an input field from caller to callee. Don't set it in the callee, as the caller may not clear it on struct reuse. This is a kernel-internal variant of msghdr only, and the only user does reinitialize the field. So this is not critical for that reason. But it is more robust to avoid the write, and slightly simpler code. And it fixes a bug, see below. Callers set msg_get_inq to request the input queue length to be returned in msg_inq. This is equivalent to but independent from the SO_INQ request to return that same info as a cmsg (tp->recvmsg_inq). To reduce branching in the hot path the second also sets the msg_inq. That is WAI. This is a fix to commit 4d1442979e4a ("af_unix: don't post cmsg for SO_INQ unless explicitly asked for"), which fixed the inverse. Also avoid NULL pointer dereference in unix_stream_read_generic if state->msg is NULL and msg->msg_get_inq is written. A NULL state->msg can happen when splicing as of commit 2b514574f7e8 ("net: af_unix: implement splice for stream af_unix sockets"). Also collapse two branches using a bitwise or.	N/A	More Details
CVE-2025-67946	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in scriptsbundle AdForest adforest allows PHP Local File Inclusion.This issue affects AdForest: from n/a through <= 6.0.11.	N/A	More Details
CVE-2025-67947	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in scriptsbundle AdForest Elementor adforest-elementor allows Reflected XSS.This issue affects AdForest Elementor: from n/a through <= 3.0.11.	N/A	More Details
CVE-2026-22995	In the Linux kernel, the following vulnerability has been resolved: ublk: fix use-after-free in ublk_partition_scan_work A race condition exists between the async partition scan work and device teardown that can lead to a use-after-free of ub->ub_disk: 1. ublk_ctrl_start_dev() schedules partition_scan_work after add_disk() 2. ublk_stop_dev() calls ublk_stop_dev_unlocked() which does: - del_gendisk(ub->ub_disk) - ublk_detach_disk() sets ub->ub_disk = NULL - put_disk() which may free the disk 3. The worker ublk_partition_scan_work() then dereferences ub->ub_disk leading to UAF Fix this by using ublk_get_disk()/ublk_put_disk() in the worker to hold a reference to the disk during the partition scan. The spinlock in ublk_get_disk() synchronizes with ublk_detach_disk() ensuring the worker either gets a valid reference or sees NULL and exits early. Also change flush_work() to cancel_work_sync() to avoid running the partition scan work unnecessarily when the disk is already detached.	N/A	More Details
CVE-2026-22994	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix reference count leak in bpf_prog_test_run_xdp() syzbot is reporting unregister_netdevice: waiting for sit0 to become free. Usage count = 2 problem. A debug printk() patch found that a refcount is obtained at xdp_convert_md_to_buff() from bpf_prog_test_run_xdp(). According to commit ec94670fcb3b ("bpf: Support specifying ingress via xdp_md context in BPF_PROG_TEST_RUN"), the refcount obtained by xdp_convert_md_to_buff() will be released by xdp_convert_buff_to_md(). Therefore, we can consider that the error handling path introduced by commit 1c1949982524 ("bpf: introduce frags support to bpf_prog_test_run_xdp()") forgot to call xdp_convert_buff_to_md().	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: idpf: Fix RSS LUT NULL ptr issue after soft reset During soft reset, the RSS LUT is freed and not restored unless the interface is up. If an ethtool command that accesses the rss lut is attempted immediately after reset, it will result in NULL ptr dereference. Also, there is no need to reset the rss lut if the soft reset does not involve queue count change. After soft reset, set the RSS LUT to default values based on the updated queue count only if the reset was a result of a queue count change and the LUT was not configured by the user. In all other cases, don't touch the LUT. Steps to reproduce: ** Bring the interface down (if up) ifconfig eth1 down ** update the queue count (eg., 27->20) ethtool -L eth1 combined 20 ** display the RSS LUT ethtool -x eth1 [82375.558338] BUG: kernel NULL pointer dereference, address: 0000000000000000 [82375.558373] #PF: supervisor read access in kernel mode [82375.558391] #PF: error_code(0x0000) - not-present page [82375.558408] PGD 0 P4D 0		

2026-22993	[82375.558421] Oops: Oops: 0000 [#1] SMP NOPTI <snip> [82375.558516] RIP: 0010:idpf_get_rxfh+0x108/0x150 [idpf] [82375.558786] Call Trace: [82375.558793] <TASK> [82375.558804] rss_prepare.isra.0+0x187/0x2a0 [82375.558827] rss_prepare_data+0x3a/0x50 [82375.558845] ethnl_default_doit+0x13d/0x3e0 [82375.558863] genl_family_rcv_msg_doit+0x11f/0x180 [82375.558886] genl_rcv_msg+0x1ad/0x2b0 [82375.558902] ? __pfx_ethnl_default_doit+0x10/0x10 [82375.558920] ? __pfx_genl_rcv_msg+0x10/0x10 [82375.558937] netlink_rcv_skb+0x58/0x100 [82375.558957] genl_rcv+0x2c/0x50 [82375.558971] netlink_unicast+0x289/0x3e0 [82375.558988] netlink_sendmsg+0x215/0x440 [82375.559005] __sys_sendto+0x234/0x240 [82375.559555] __x64_sys_sendto+0x28/0x30 [82375.560068] x64_sys_call+0x1909/0x1da0 [82375.560576] do_syscall_64+0x7a/0xfa0 [82375.561076] ? clear_bhb_loop+0x60/0xb0 [82375.561567] entry_SYSCALL_64_after_hwframe+0x76/0x7e <snip>	N/A	More Details
CVE-2026-22992	In the Linux kernel, the following vulnerability has been resolved: libceph: return the handler error from mon_handle_auth_done() Currently any error from ceph_auth_handle_reply_done() is propagated via finish_auth() but isn't returned from mon_handle_auth_done(). This results in higher layers learning that (despite the monitor considering us to be successfully authenticated) something went wrong in the authentication phase and reacting accordingly, but msgr2 still trying to proceed with establishing the session in the background. In the case of secure mode this can trigger a WARN in setup_crypto() and later lead to a NULL pointer dereference inside of prepare_auth_signature().	N/A	More Details
CVE-2026-22991	In the Linux kernel, the following vulnerability has been resolved: libceph: make free_choose_arg_map() resilient to partial allocation free_choose_arg_map() may dereference a NULL pointer if its caller fails after a partial allocation. For example, in decode_choose_args(), if allocation of arg_map->args fails, execution jumps to the fail label and free_choose_arg_map() is called. Since arg_map->size is updated to a non-zero value before memory allocation, free_choose_arg_map() will iterate over arg_map->args and dereference a NULL pointer. To prevent this potential NULL pointer dereference and make free_choose_arg_map() more resilient, add checks for pointers before iterating.	N/A	More Details
CVE-2026-22990	In the Linux kernel, the following vulnerability has been resolved: libceph: replace overzealous BUG_ON in osdmap_apply_incremental() If the osdmap is (maliciously) corrupted such that the incremental osdmap epoch is different from what is expected, there is no need to BUG. Instead, just declare the incremental osdmap to be invalid.	N/A	More Details
CVE-2026-22989	In the Linux kernel, the following vulnerability has been resolved: nfsd: check that server is running in unlock_filesystem If we are trying to unlock the filesystem via an administrative interface and nfsd isn't running, it crashes the server. This happens currently because nfsd4_revoke_states() access state structures (eg., conf_id_hashtbl) that has been freed as a part of the server shutdown. [59.465072] Call trace: [59.465308] nfsd4_revoke_states+0x1b4/0x898 [nfsd] (P) [59.465830] write_unlock_fs+0x258/0x440 [nfsd] [59.466278] nfsctl_transaction_write+0xb0/0x120 [nfsd] [59.466780] vfs_write+0x1f0/0x938 [59.467088] ksys_write+0xfc/0x1f8 [59.467395] __arm64_sys_write+0x74/0xb8 [59.467746] invoke_syscall.constprop.0+0xdc/0x1e8 [59.468177] do_el0_svc+0x154/0x1d8 [59.468489] el0_svc+0x40/0xe0 [59.468767] el0t_64_sync_handler+0xa0/0xe8 [59.469138] el0t_64_sync+0x1ac/0x1b0 Ensure this can't happen by taking the nfsd_mutex and checking that the server is still up, and then holding the mutex across the call to nfsd4_revoke_states().	N/A	More Details
CVE-2026-22988	In the Linux kernel, the following vulnerability has been resolved: arp: do not assume dev_hard_header() does not change skb->head arp_create() is the only dev_hard_header() caller making assumption about skb->head being unchanged. A recent commit broke this assumption. Initialize @arp pointer after dev_hard_header() call.	N/A	More Details
CVE-2026-22987	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_api: avoid dereferencing ERR_PTR in tcf_idrinfo_destroy syzbot reported a crash in tc_act_in_hw() during netns teardown where tcf_idrinfo_destroy() passed an ERR_PTR(-EBUSY) value as a tc_action pointer, leading to an invalid dereference. Guard against ERR_PTR entries when	N/A	More Details

	iterating the action IDR so teardown does not call tc_act_in_hw() on an error pointer.		
CVE-2026-22986	In the Linux kernel, the following vulnerability has been resolved: gpiolib: fix race condition for gdev->srcu If two drivers were calling gpiochip_add_data_with_key(), one may be traversing the srcu-protected list in gpio_name_to_desc(), meanwhile other has just added its gdev in gpiodev_add_to_list_unlocked(). This creates a non-mutexed and non-protected timeframe, when one instance is dereferencing and using &gdev->srcu, before the other has initialized it, resulting in crash: [4.935481] Unable to handle kernel paging request at virtual address ffff800272bcc000 [4.943396] Mem abort info: [4.943400] ESR = 0x0000000096000005 [4.943403] EC = 0x25: DABT (current EL), IL = 32 bits [4.943407] SET = 0, FnV = 0 [4.943410] EA = 0, S1PTW = 0 [4.943413] FSC = 0x05: level 1 translation fault [4.943416] Data abort info: [4.943418] ISV = 0, ISS = 0x00000005, ISS2 = 0x00000000 [4.946220] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [4.955261] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [4.955268] swapper pgtable: 4k pages, 48-bit VAs, pgdp=0000000038e6c000 [4.961449] [ffff800272bcc000] pgd=0000000000000000 [4.969203] , p4d=1000000039739003 [4.979730] , pud=0000000000000000 [4.980210] phandle (CPU): 0x0000005e, phandle (BE): 0x5e000000 for node "reset" [4.991736] Internal error: Oops: 0000000096000005 [#1] PREEMPT SMP ... [5.121359] pc : __srcu_read_lock+0x44/0x98 [5.131091] lr : gpio_name_to_desc+0x60/0x1a0 [5.153671] sp : ffff8000833bb430 [5.298440] [5.298443] Call trace: [5.298445] __srcu_read_lock+0x44/0x98 [5.309484] gpio_name_to_desc+0x60/0x1a0 [5.320692] gpiochip_add_data_with_key+0x488/0xf00 5.946419] ---[end trace 0000000000000000]--- Move initialization code for gdev fields before it is added to gpio_devices, with adjacent initialization code. Adjust goto statements to reflect modified order of operations [Bartosz: fixed a build issue, removed stray newline]	N/A	More Details
CVE-2026-22985	In the Linux kernel, the following vulnerability has been resolved: idpf: Fix RSS LUT NULL pointer crash on early ethtool operations The RSS LUT is not initialized until the interface comes up, causing the following NULL pointer crash when ethtool operations like rxhash on/off are performed before the interface is brought up for the first time. Move RSS LUT initialization from ndo_open to vport creation to ensure LUT is always available. This enables RSS configuration via ethtool before bringing the interface up. Simplify LUT management by maintaining all changes in the driver's soft copy and programming zeros to the indirection table when rxhash is disabled. Defer HW programming until the interface comes up if it is down during rxhash and LUT configuration changes. Steps to reproduce: ** Load idpf driver; interfaces will be created modprobe idpf ** Before bringing the interfaces up, turn rxhash off ethtool -K eth2 rxhash off [89408.371875] BUG: kernel NULL pointer dereference, address: 0000000000000000 [89408.371908] #PF: supervisor read access in kernel mode [89408.371924] #PF: error_code(0x0000) - not-present page [89408.371940] PGD 0 P4D 0 [89408.371953] Oops: Oops: 0000 [#1] SMP NOPTI <snip> [89408.372052] RIP: 0010:memcpy_orig+0x16/0x130 [89408.372310] Call Trace: [89408.372317] <TASK> [89408.372326] ? idpf_set_features+0xfc/0x180 [idpf] [89408.372363] __netdev_update_features+0x295/0xde0 [89408.372384] ethnl_set_features+0x15e/0x460 [89408.372406] genl_family_rcv_msg_doit+0x11f/0x180 [89408.372429] genl_rcv_msg+0x1ad/0x2b0 [89408.372446] ? __pfx_ethnl_set_features+0x10/0x10 [89408.372465] ? __pfx_genl_rcv_msg+0x10/0x10 [89408.372482] netlink_rcv_skb+0x58/0x100 [89408.372502] genl_rcv+0x2c/0x50 [89408.372516] netlink_unicast+0x289/0x3e0 [89408.372533] netlink_sendmsg+0x215/0x440 [89408.372551] __sys_sendto+0x234/0x240 [89408.372571] __x64_sys_sendto+0x28/0x30 [89408.372585] x64_sys_call+0x1909/0x1da0 [89408.372604] do_syscall_64+0x7a/0xfa0 [89408.373140] ? clear_bhb_loop+0x60/0xb0 [89408.373647] entry_SYSCALL_64_after_hwframe+0x76/0x7e [89408.378887] </TASK> <snip>	N/A	More Details
CVE-2026-22984	In the Linux kernel, the following vulnerability has been resolved: libceph: prevent potential out-of-bounds reads in handle_auth_done() Perform an explicit bounds check on payload_len to avoid a possible out-of-bounds access in the callout. [idryomov: changelog]	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: net: mscc: ocelot: Fix crash when adding interface under a lag Commit 15faa1f67ab4 ("lan966x: Fix crash when adding interface under a lag") fixed a similar issue in the lan966x driver caused by a NULL		

2026-22982	pointer dereference. The ocelot_set_aggr_pgids() function in the ocelot driver has similar logic and is susceptible to the same crash. This issue specifically affects the ocelot_vsc7514.c frontend, which leaves unused ports as NULL pointers. The felix_vsc9959.c frontend is unaffected as it uses the DSA framework which registers all ports. Fix this by checking if the port pointer is valid before accessing it.	N/A	More Details
CVE-2025-67944	Improper Control of Generation of Code ('Code Injection') vulnerability in Nelio Software Nelio AB Testing nelio-ab-testing allows Code Injection.This issue affects Nelio AB Testing: from n/a through <= 8.1.8.	N/A	More Details
CVE-2026-22981	In the Linux kernel, the following vulnerability has been resolved: idpf: detach and close netdevs while handling a reset Protect the reset path from callbacks by setting the netdevs to detached state and close any netdevs in UP state until the reset handling has completed. During a reset, the driver will de-allocate resources for the vport, and there is no guarantee that those will recover, which is why the existing vport_ctrl_lock does not provide sufficient protection. idpf_detach_and_close() is called right before reset handling. If the reset handling succeeds, the netdevs state is recovered via call to idpf_attach_and_open(). If the reset handling fails the netdevs remain down. The detach/down calls are protected with RTNL lock to avoid racing with callbacks. On the recovery side the attach can be done without holding the RTNL lock as there are no callbacks expected at that point, due to detach/close always being done first in that flow. The previous logic restoring the netdevs state based on the IDPF_VPORT_UP_REQUESTED flag in the init task is not needed anymore, hence the removal of idpf_set_vport_state(). The IDPF_VPORT_UP_REQUESTED is still being used to restore the state of the netdevs following the reset, but has no use outside of the reset handling flow. idpf_init_hard_reset() is converted to void, since it was used as such and there is no error handling being done based on its return value. Before this change, invoking hard and soft resets simultaneously will cause the driver to lose the vport state: ip -br a <inf> UP echo 1 > /sys/class/net/ens801f0/device/reset& \ ethtool -L ens801f0 combined 8 ip -br a <inf> DOWN ip link set <inf> up ip -br a <inf> DOWN Also in case of a failure in the reset path, the netdev is left exposed to external callbacks, while vport resources are not initialized, leading to a crash on subsequent ifup/down: [408471.398966] idpf 0000:83:00.0: HW reset detected [408471.411744] idpf 0000:83:00.0: Device HW Reset initiated [408472.277901] idpf 0000:83:00.0: The driver was unable to contact the device's firmware. Check that the FW is running. Driver state= 0x2 [408508.125551] BUG: kernel NULL pointer dereference, address: 0000000000000078 [408508.126112] #PF: supervisor read access in kernel mode [408508.126687] #PF: error_code(0x0000) - not-present page [408508.127256] PGD 2aae2f067 P4D 0 [408508.127824] Oops: Oops: 0000 [#1] SMP NOPTI ... [408508.130871] RIP: 0010:idpf_stop+0x39/0x70 [idpf] ... [408508.139193] Call Trace: [408508.139637] <TASK> [408508.140077] __dev_close_many+0xbb/0x260 [408508.140533] __dev_change_flags+0x1cf/0x280 [408508.140987] netif_change_flags+0x26/0x70 [408508.141434] dev_change_flags+0x3d/0xb0 [408508.141878] devinet_ioctl+0x460/0x890 [408508.142321] inet_ioctl+0x18e/0x1d0 [408508.142762] ? _copy_to_user+0x22/0x70 [408508.143207] sock_do_ioctl+0x3d/0xe0 [408508.143652] sock_ioctl+0x10e/0x330 [408508.144091] ? find_held_lock+0x2b/0x80 [408508.144537] __x64_sys_ioctl+0x96/0xe0 [408508.144979] do_syscall_64+0x79/0x3d0 [408508.145415] entry_SYSCALL_64_after_hwframe+0x76/0x7e [408508.145860] RIP: 0033:0x7f3e0bb4caff	N/A	More Details
CVE-2026-22980	In the Linux kernel, the following vulnerability has been resolved: nfsd: provide locking for v4_end_grace Writing to v4_end_grace can race with server shutdown and result in memory being accessed after it was freed - reclaim_str_hashtbl in particularly. We cannot hold nfsd_mutex across the nfsd4_end_grace() call as that is held while client_tracking_op->init() is called and that can wait for an upcall to nfsdcltrack which can write to v4_end_grace, resulting in a deadlock. nfsd4_end_grace() is also called by the landromat work queue and this doesn't require locking as server shutdown will stop the work and wait for it before freeing anything that nfsd4_end_grace() might access. However, we must be sure that writing to v4_end_grace doesn't restart the work item after shutdown has already waited for it. For this we add a new flag protected with nn->client_lock. It is set only while it is safe to make client tracking calls, and v4_end_grace only schedules work while the flag is set with the spinlock held. So this patch adds a nfsd_net field "client_tracking_active" which is set as described. Another field "grace_end_forced", is set when v4_end_grace is written.	N/A	More Details

	After this is set, and providing client_tracking_active is set, the laundromat is scheduled. This "grace_end_forced" field bypasses other checks for whether the grace period has finished. This resolves a race which can result in use-after-free.		
CVE-2026-22979	In the Linux kernel, the following vulnerability has been resolved: net: fix memory leak in skb_segment_list for GRO packets When skb_segment_list() is called during packet forwarding, it handles packets that were aggregated by the GRO engine. Historically, the segmentation logic in skb_segment_list assumes that individual segments are split from a parent SKB and may need to carry their own socket memory accounting. Accordingly, the code transfers truesize from the parent to the newly created segments. Prior to commit ed4cccef64c1 ("gro: fix ownership transfer"), this truesize subtraction in skb_segment_list() was valid because fragments still carry a reference to the original socket. However, commit ed4cccef64c1 ("gro: fix ownership transfer") changed this behavior by ensuring that fraglist entries are explicitly orphaned (skb->sk = NULL) to prevent illegal orphaning later in the stack. This change meant that the entire socket memory charge remained with the head SKB, but the corresponding accounting logic in skb_segment_list() was never updated. As a result, the current code unconditionally adds each fragment's truesize to delta_truesize and subtracts it from the parent SKB. Since the fragments are no longer charged to the socket, this subtraction results in an effective under-count of memory when the head is freed. This causes sk_wmem_alloc to remain non-zero, preventing socket destruction and leading to a persistent memory leak. The leak can be observed via KMEMLEAK when tearing down the networking environment: unreferenced object 0xffff8881e6eb9100 (size 2048): comm "ping", pid 6720, jiffies 4295492526 backtrace: kmem_cache_alloc_noprof+0x5c6/0x800 sk_prot_alloc+0x5b/0x220 sk_alloc+0x35/0xa00 inet6_create.part.0+0x303/0x10d0 __sock_create+0x248/0x640 __sys_socket+0x11b/0x1d0 Since skb_segment_list() is exclusively used for SKB_GSO_FRAGLIST packets constructed by GRO, the truesize adjustment is removed. The call to skb_release_head_state() must be preserved. As documented in commit cf673ed0e057 ("net: fix fraglist segmentation reference count leak"), it is still required to correctly drop references to SKB extensions that may be overwritten during __copy_skb_header().	N/A	More Details
CVE-2026-22978	In the Linux kernel, the following vulnerability has been resolved: wifi: avoid kernel-infoleak from struct iw_point struct iw_point has a 32bit hole on 64bit arches. struct iw_point { void __user *pointer; /* Pointer to the data (in user space) */ __u16 length; /* number of fields or size in bytes */ __u16 flags; /* Optional params */ }; Make sure to zero the structure to avoid disclosing 32bits of kernel data to user space.	N/A	More Details
CVE-2025-71161	In the Linux kernel, the following vulnerability has been resolved: dm-verity: disable recursive forward error correction There are two problems with the recursive correction: 1. It may cause denial-of-service. In fec_read_bufs, there is a loop that has 253 iterations. For each iteration, we may call verity_hash_for_block recursively. There is a limit of 4 nested recursions - that means that there may be at most 253^4 (4 billion) iterations. Red Hat QE team actually created an image that pushes dm-verity to this limit - and this image just makes the udev-worker process get stuck in the 'D' state. 2. It doesn't work. In fec_read_bufs we store data into the variable "fio->bufs", but fio bufs is shared between recursive invocations, if "verity_hash_for_block" invoked correction recursively, it would overwrite partially filled fio->bufs.	N/A	More Details
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: avoid chain re-validation if possible Hamza Mahfooz reports cpu soft lock-ups in nft_chain_validate(): watchdog: BUG: soft lockup - CPU#1 stuck for 27s! [iptables-nft-re:37547] [..] RIP: 0010:nft_chain_validate+0xcb/0x110 [nf_tables] [..] nft_immediate_validate+0x36/0x50 [nf_tables] nft_chain_validate+0xc9/0x110 [nf_tables] nft_immediate_validate+0x36/0x50 [nf_tables] nft_chain_validate+0xc9/0x110 [nf_tables] nft_immediate_validate+0x36/0x50 [nf_tables] nft_chain_validate+0xc9/0x110 [nf_tables] nft_immediate_validate+0x36/0x50 [nf_tables] nft_chain_validate+0xc9/0x110 [nf_tables] nft_immediate_validate+0x36/0x50 [nf_tables] nft_chain_validate+0xc9/0x110 [nf_tables] nft_immediate_validate+0x36/0x50 [nf_tables] nft_chain_validate+0xc9/0x110 [nf_tables] nft_table_validate+0x6b/0xb0 [nf_tables] nf_tables_validate+0x8b/0xa0 [nf_tables] nf_tables_commit+0x1df/0x1eb0 [nf_tables] [..] Currently nf_tables will traverse the entire table (chain graph), starting from the entry points (base chains), exploring all possible	N/A	More Details

71160	paths (chain jumps). But there are cases where we could avoid revalidation. Consider: 1 input -> j2 -> j3 2 input -> j2 -> j3 3 input -> j1 -> j2 -> j3 Then the second rule does not need to revalidate j2, and, by extension j3, because this was already checked during validation of the first rule. We need to validate it only for rule 3. This is needed because chain loop detection also ensures we do not exceed the jump stack: Just because we know that j2 is cycle free, its last jump might now exceed the allowed stack size. We also need to update all reachable chains with the new largest observed call depth. Care has to be taken to revalidate even if the chain depth won't be an issue: chain validation also ensures that expressions are not called from invalid base chains. For example, the masquerade expression can only be called from NAT postrouting base chains. Therefore we also need to keep record of the base chain context (type, hooknum) and revalidate if the chain becomes reachable from a different hook location.		
CVE-2025-71159	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix use-after-free warning in btrfs_get_or_create_delayed_node() Previously, btrfs_get_or_create_delayed_node() set the delayed_node's refcount before acquiring the root->delayed_nodes lock. Commit e8513c012de7 ("btrfs: implement ref_tracker for delayed_nodes") moved refcount_set inside the critical section, which means there is no longer a memory barrier between setting the refcount and setting btrfs_inode->delayed_node. Without that barrier, the stores to node->refs and btrfs_inode->delayed_node may become visible out of order. Another thread can then read btrfs_inode->delayed_node and attempt to increment a refcount that hasn't been set yet, leading to a refcounting bug and a use-after-free warning. The fix is to move refcount_set back to where it was to take advantage of the implicit memory barrier provided by lock acquisition. Because the allocations now happen outside of the lock's critical section, they can use GFP_NOFS instead of GFP_ATOMIC.	N/A	More Details
CVE-2025-71158	In the Linux kernel, the following vulnerability has been resolved: gpio: mpsse: ensure worker is torn down When an IRQ worker is running, unplugging the device would cause a crash. The sealevel hardware this driver was written for was not hotpluggable, so I never realized it. This change uses a spinlock to protect a list of workers, which it tears down on disconnect.	N/A	More Details
CVE-2025-67949	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in designingmedia Hostiko hostiko allows Reflected XSS.This issue affects Hostiko: from n/a through < 94.3.6.	N/A	More Details
CVE-2025-67952	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand Tour grandtour allows Reflected XSS.This issue affects Grand Tour: from n/a through < 5.6.2.	N/A	More Details
CVE-2025-67953	Incorrect Privilege Assignment vulnerability in Booking Activities Team Booking Activities booking-activities allows Privilege Escalation.This issue affects Booking Activities: from n/a through <= 1.16.44.	N/A	More Details
CVE-2025-67954	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Dimitri Grassi Salon booking system salon-booking-system allows Retrieve Embedded Sensitive Data.This issue affects Salon booking system: from n/a through <= 10.30.3.	N/A	More Details
CVE-2025-14751	A low-privileged user can bypass account credentials without confirming the user's current authentication state, which may lead to unauthorized privilege escalation.	N/A	More Details
CVE-2025-9289	A Cross-Site Scripting (XSS) vulnerability was identified in a parameter in Omada Controllers due to improper input sanitization. Exploitation requires advanced conditions, such as network positioning or emulating a trusted entity, and user interaction by an authenticated administrator. If successful, an attacker could execute arbitrary JavaScript in the administrator’s browser, potentially exposing sensitive information and compromising confidentiality.	N/A	More Details
CVE-2025-	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in MailerLite MailerLite – WooCommerce integration woo-mailerlite allows SQL Injection.This issue affects MailerLite – WooCommerce integration: from n/a through <=	N/A	More Details

67945	3.1.2.		
CVE-2025-67943	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wphocus My auctions allegro my-auctions-allegro-free-edition allows Reflected XSS.This issue affects My auctions allegro: from n/a through <= 3.6.32.	N/A	More Details
CVE-2025-69036	Deserialization of Untrusted Data vulnerability in strongholdthemes Tech Life CPT techlife-cpt allows Object Injection.This issue affects Tech Life CPT: from n/a through <= 16.4.	N/A	More Details
CVE-2026-24423	SmarterTools SmarterMail versions prior to build 9511 contain an unauthenticated remote code execution vulnerability in the ConnectToHub API method. The attacker could point the SmarterMail to the malicious HTTP server, which serves the malicious OS command. This command will be executed by the vulnerable application.	N/A	More Details
CVE-2025-69035	Deserialization of Untrusted Data vulnerability in strongholdthemes Dental Care CPT dentalcare-cpt allows Object Injection.This issue affects Dental Care CPT: from n/a through <= 20.2.	N/A	More Details
CVE-2026-24402	Rejected reason: GitHub cannot issue a CVE for this Security Advisory because this advisory includes information about more than one vulnerability. According to [rule 4.2.11 of the CVE CNA rules] (https://www.cve.org/ResourcesSupport/AllResources/CNARules#section_4-2_CVE_ID_Assignment): > 4.2.6 CNAs SHOULD assign different CVE IDs to separate Vulnerabilities, as determined using the guidance in [4.1] (https://www.cve.org/ResourcesSupport/AllResources/CNARules#section_4-1_Vulnerability_Determination). > 4.2.11 CNAs SHOULD assign different CVE IDs to different, Independently Fixable Vulnerabilities. You can move forward in one of two ways: - If you agree that this Security Advisory concerns more than one independently fixable vulnerability, split each vulnerability into its own advisory and request one CVE for each vulnerability. - If you do not agree that these vulnerabilities are independently fixable, resubmit the CVE request with a section clarifying how they are dependent and should have the same CVE. Thank you for making the open source ecosystem more secure by fixing and responsibly disclosing these vulnerabilities.	N/A	More Details
CVE-2026-24474	Dioxus Components is a shadcn-style component library for the Dioxus app framework. Prior to commit 41e4242ecb1062d04ae42a5215363c1d9fd4e23a, `use_animated_open` formats a string for `eval` with an `id` that can be user supplied. Commit 41e4242ecb1062d04ae42a5215363c1d9fd4e23a patches the issue.	N/A	More Details
CVE-2026-24139	MyTube is a self-hosted downloader and player for several video websites. Versions 1.7.78 and below do not safeguard against authorization bypass, allowing guest users to download the complete application database. The application fails to properly validate user permissions on the database export endpoint, enabling low-privileged users to access sensitive data they should not have permission to view.	N/A	More Details
CVE-2026-24136	Saleor is an e-commerce platform. Versions 3.2.0 through 3.20.109, 3.21.0-a.0 through 3.21.44 and 3.22.0-a.0 through 3.22.28 have a n Insecure Direct Object Reference (IDOR) vulnerability that allows unauthenticated actors to extract sensitive information in plain text. Orders created before Saleor 3.2.0 could have PIIs exfiltrated. The issue has been patched in Saleor versions: 3.22.29, 3.21.45, and 3.20.110. To workaround, temporarily block non-staff users from fetching order information (the order() GraphQL query) using a WAF.	N/A	More Details
CVE-2026-24128	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Versions 7.0-milestone-2 through 16.10.11, 17.0.0-rc-1 through 17.4.4, and 17.5.0-rc-1 through 17.7.0 contain a reflected Cross-site Scripting (XSS) vulnerability, which allows an attacker to craft a malicious URL and execute arbitrary actions with the same privileges as the victim. If the victim has administrative or programming rights, those rights can be exploited to gain full access to the XWiki installation. This issue has been patched in versions 17.8.0-rc-1, 17.4.5 and 16.10.12. To workaround, the patch can be applied manually, only a single line in templates/logging_macros.vm needs to be changed, no	N/A	More Details

	restart is required.		
CVE-2025-69005	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Search & Go search-and-go allows PHP Local File Inclusion.This issue affects Search & Go: from n/a through <= 2.8.	N/A	More Details
CVE-2026-0991	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-12780	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-66139	Missing Authorization vulnerability in merkulove Audier For Elementor audier-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Audier For Elementor: from n/a through <= 1.0.9.	N/A	More Details
CVE-2025-14750	The web application does not sufficiently verify inputs that are assumed to be immutable but are actually externally controllable. A low-privileged user can modify the parameters and potentially manipulate account-level privileges.	N/A	More Details
CVE-2026-21867	Rejected reason: Reason: This candidate was issued in error.	N/A	More Details
CVE-2025-66141	Missing Authorization vulnerability in merkulove Scroller scroller allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Scroller: from n/a through <= 2.0.2.	N/A	More Details
CVE-2025-66142	Missing Authorization vulnerability in merkulove Comparimager for Elementor comparimager-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Comparimager for Elementor: from n/a through <= 1.0.1.	N/A	More Details
CVE-2026-1299	The email module, specifically the "BytesGenerator" class, didn’t properly quote newlines for email headers when serializing an email message allowing for header injection when an email is serialized. This is only applicable if using "LiteralHeader" writing headers that don't respect email folding rules, the new behavior will reject the incorrectly folded headers in "BytesGenerator".	N/A	More Details
CVE-2025-67942	Missing Authorization vulnerability in peachpayments Peach Payments Gateway wc-peach-payments-gateway allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Peach Payments Gateway: from n/a through <= 3.3.6.	N/A	More Details
CVE-2025-71177	LavaLite CMS versions up to and including 10.1.0 contain a stored cross-site scripting vulnerability in the package creation and search functionality. Authenticated users can supply crafted HTML or JavaScript in the package Name or Description fields that is stored and later rendered without proper output encoding in package search results. When other users view search results that include the malicious package, the injected script executes in their browsers, potentially enabling session hijacking, credential theft, and unauthorized actions in the context of the victim.	N/A	More Details
CVE-2025-66143	Missing Authorization vulnerability in merkulove Crumber crumber-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Crumber: from n/a through <= 1.0.10.	N/A	More Details
CVE-2025-67614	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in foreverpinetree TheNa thena allows Reflected XSS.This issue affects TheNa: from n/a through <= 1.5.5.	N/A	More Details
CVE-2025-67615	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in bslthemes Myour myour allows PHP Local File Inclusion.This issue affects Myour: from n/a through <= 1.5.1.	N/A	More Details
CVE-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote		

2025-67616	File Inclusion') vulnerability in BZOTheme Mella mella allows PHP Local File Inclusion.This issue affects Mella: from n/a through <= 1.2.29.	N/A	More Details
CVE-2025-67617	Deserialization of Untrusted Data vulnerability in themeton Consult Aid consultaid allows Object Injection.This issue affects Consult Aid: from n/a through <= 1.4.3.	N/A	More Details
CVE-2025-67619	Deserialization of Untrusted Data vulnerability in designthemes Kids Heaven kids-world allows Object Injection.This issue affects Kids Heaven: from n/a through <= 3.2.	N/A	More Details
CVE-2025-67620	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CleverSoft Anon anon2x allows Reflected XSS.This issue affects Anon: from n/a through <= 2.2.10.	N/A	More Details
CVE-2025-67626	Cross-Site Request Forgery (CSRF) vulnerability in Angel Costa WP SEO Search wp-seo-search allows Cross Site Request Forgery.This issue affects WP SEO Search: from n/a through <= 1.1.	N/A	More Details
CVE-2025-67923	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetEngine jet-engine allows Reflected XSS.This issue affects JetEngine: from n/a through <= 3.7.7.	N/A	More Details
CVE-2025-67938	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Biagiotti biagiotti allows PHP Local File Inclusion.This issue affects Biagiotti: from n/a through < 3.5.2.	N/A	More Details
CVE-2025-67939	Missing Authorization vulnerability in Tickera Tickera tickera-event-ticketing-system allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tickera: from n/a through <= 3.5.6.2.	N/A	More Details
CVE-2025-67940	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Powerlift powerlift allows PHP Local File Inclusion.This issue affects Powerlift: from n/a through < 3.2.1.	N/A	More Details
CVE-2025-67941	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes The Aisle theaisle allows PHP Local File Inclusion.This issue affects The Aisle: from n/a through < 2.9.1.	N/A	More Details
CVE-2026-0781	ALGO 8180 IP Audio Alerter Web UI Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is required to exploit this vulnerability. The specific flaw exists within the web-based user interface. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-28290.	N/A	More Details