SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 21 January 2026

Generated on 21 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-2026-22686	Enclave is a secure JavaScript sandbox designed for safe AI agent code execution. Prior to 2.7.0, there is a critical sandbox escape vulnerability in enclave-vm that allows untrusted, sandboxed JavaScript code to execute arbitrary code in the host Node.js runtime. When a tool invocation fails, enclave-vm exposes a host-side Error object to sandboxed code. This Error object retains its host realm prototype chain, which can be traversed to reach the host Function constructor. An attacker can intentionally trigger a host error, then climb the prototype chain. Using the host Function constructor, arbitrary JavaScript can be compiled and executed in the host context, fully bypassing the sandbox and granting access to sensitive resources such as process.env, filesystem, and network. This breaks enclave-vm's core security guarantee of isolating untrusted code. This vulnerability is fixed in 2.7.0.	10.0	More Details
CVE-2026-21962	Vulnerability in the Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in product of Oracle Fusion Middleware (component: Weblogic Server Proxy Plug-in for Apache HTTP Server, Weblogic Server Proxy Plug-in for IIS). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in. While the vulnerability is in Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle HTTP Server, Oracle Weblogic	10.0	More Details

	Server Proxy Plug-in accessible data as well as unauthorized access to critical data or complete access to all Oracle HTTP Server, Oracle Weblogic Server Proxy Plug-in accessible data. Note: Affected version for Weblogic Server Proxy Plug-in for IIS is 12.2.1.4.0 only. CVSS 3.1 Base Score 10.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N).		
CVE-2026-23550	Incorrect Privilege Assignment vulnerability in Modular DS allows Privilege Escalation.This issue affects Modular DS: from n/a through 2.5.1.	10.0	More Details
CVE-2025-61937	The vulnerability, if exploited, could allow an unauthenticated miscreant to achieve remote code execution under OS system privileges of “taoimr” service, potentially resulting in complete compromise of the model application server.	10.0	More Details
CVE-2026-23800	Incorrect Privilege Assignment vulnerability in Modular DS modular-connector allows Privilege Escalation.This issue affects Modular DS: from 2.5.2 before 2.6.0.	10.0	More Details
CVE-2026-22907	An attacker may gain unauthorized access to the host filesystem, potentially allowing them to read and modify system data.	9.9	More Details
CVE-2026-22844	A Command Injection vulnerability in Zoom Node Multimedia Routers (MMRs) before version 5.2.1716.0 may allow a meeting participant to conduct remote code execution of the MMR via network access.	9.9	More Details
CVE-2026-22797	An issue was discovered in OpenStack keystonemiddleware 10.5 through 10.7 before 10.7.2, 10.8 and 10.9 before 10.9.1, and 10.10 through 10.12 before 10.12.1. The external_oauth2_token middleware fails to sanitize incoming authentication headers before processing OAuth 2.0 tokens. By sending forged identity headers such as X-Is-Admin-Project, X-Roles, or X-User-Id, an authenticated attacker may escalate privileges or impersonate other users. All deployments using the external_oauth2_token middleware are affected.	9.9	More Details
CVE-2026-23836	HotCRP is conference review software. A problem introduced in April 2024 in version 3.1 led to inadequately sanitized code generation for HotCRP formulas which allowed users to trigger the execution of arbitrary PHP code. The problem is patched in release version 3.2.	9.9	More Details
CVE-2025-60021	Remote command injection vulnerability in heap profiler builtin service in Apache bRPC ((all versions < 1.15.0)) on all platforms allows attacker to inject remote command. Root Cause: The bRPC heap profiler built-in service (/pprof/heap) does not validate the user-provided extra_options parameter and executes it as a command-line argument. Attackers can execute remote commands using the extra_options parameter.. Affected scenarios: Use the built-in bRPC heap profiler service to perform jemalloc memory profiling. How to Fix: we provide two methods, you can choose one of them: 1. Upgrade bRPC to version 1.15.0. 2. Apply this patch (https://github.com/apache/brpc/pull/3101) manually.	9.8	More Details
CVE-2026-1021	Police Statistics Database System developed by Gotac has an Arbitrary File Upload vulnerability, allowing unauthenticated remote attacker to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	9.8	More Details
CVE-2025-62581	Delta Electronics DIAView has multiple vulnerabilities.	9.8	More Details
CVE-2026-	Police Statistics Database System developed by Gotac has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to read,	9.8	More Details

1019	modify, and delete database contents by using a specific functionality.		
CVE-2025-62582	Delta Electronics DIAView has multiple vulnerabilities.	9.8	More Details
CVE-2025-14237	Buffer overflow in XPS font parse processing on Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *: Satera LBP670C Series/Satera MF750C Series firmware v06.02 and earlier sold in Japan.Color imageCLASS LBP630C/Color imageCLASS MF650C Series/imageCLASS LBP230 Series/imageCLASS X LBP1238 II/imageCLASS MF450 Series/imageCLASS X MF1238 II/imageCLASS X MF1643i II/imageCLASS X MF1643iF II firmware v06.02 and earlier sold in US.i-SENSYS LBP630C Series/i-SENSYS MF650C Series/i-SENSYS LBP230 Series/1238P II/1238Pr II/i-SENSYS MF450 Series/i-SENSYS MF550 Series/1238i II/1238iF II/imageRUNNER 1643i II/imageRUNNER 1643iF II firmware v06.02 and earlier sold in Europe.	9.8	More Details
CVE-2025-14236	Buffer overflow in Address Book attribute tag processing on Small Office Multifunction Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *: Satera LBP670C Series/Satera MF750C Series firmware v06.02 and earlier sold in Japan.Color imageCLASS LBP630C/Color imageCLASS MF650C Series/imageCLASS LBP230 Series/imageCLASS X LBP1238 II/imageCLASS MF450 Series/imageCLASS X MF1238 II/imageCLASS X MF1643i II/imageCLASS X MF1643iF II firmware v06.02 and earlier sold in US.i-SENSYS LBP630C Series/i-SENSYS MF650C Series/i-SENSYS LBP230 Series/1238P II/1238Pr II/i-SENSYS MF450 Series/i-SENSYS MF550 Series/1238i II/1238iF II/imageRUNNER 1643i II/imageRUNNER 1643iF II firmware v06.02 and earlier sold in Europe.	9.8	More Details
CVE-2025-14301	The Integration Opvius AI for WooCommerce plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.3.0. This is due to the `process_table_bulk_actions()` function processing user-supplied file paths without authentication checks, nonce verification, or path validation. This makes it possible for unauthenticated attackers to delete or download arbitrary files on the server via the `wsaw-log[]` POST parameter, which can be leveraged to delete critical files like `wp-config.php` or read sensitive configuration files.	9.8	More Details
CVE-2026-23744	MCPJam inspector is the local-first development platform for MCP servers. Versions 1.4.2 and earlier are vulnerable to remote code execution (RCE) vulnerability, which allows an attacker to send a crafted HTTP request that triggers the installation of an MCP server, leading to RCE. Since MCPJam inspector by default listens on 0.0.0.0 instead of 127.0.0.1, an attacker can trigger the RCE remotely via a simple HTTP request. Version 1.4.3 contains a patch.	9.8	More Details
CVE-2026-1162	A flaw has been found in UTT HiPER 810 1.7.4-141218. The impacted element is the function strcpy of the file /goform/setSysAdm. This manipulation of the argument passwd1 causes buffer overflow. Remote exploitation of the attack is possible. The exploit has been published and may be used.	9.8	More Details
CVE-2025-15403	The RegistrationMagic plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 6.0.7.1. This is due to the 'add_menu' function is accessible via the 'rm_user_exists' AJAX action and allows arbitrary updates to the 'admin_order' setting. This makes it possible for unauthenticated attackers to injecting an empty slug into the order parameter, and manipulate the plugin's menu generation logic, and when the admin menu is subsequently built, the plugin adds 'manage_options' capability for the target role. Note: The vulnerability can only be exploited unauthenticated, but further privilege escalation requires at least a subscriber user.	9.8	More Details

CVE-2025-10484	The Registration & Login with Mobile Phone Number for WooCommerce plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.3.1. This is due to the plugin not properly verifying a users identity prior to authenticating them via the fma_lwp_set_session_php_fun() function. This makes it possible for unauthenticated attackers to authenticate as any user on the site, including administrators, without a valid password.	9.8	More Details
CVE-2026-0610	SQL Injection vulnerability in remote-sessions in Devolutions Server.This issue affects Devolutions Server 2025.3.1 through 2025.3.12	9.8	More Details
CVE-2025-14233	Invalid free in CPCA file deletion processing on Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *: Satera LBP670C Series/Satera MF750C Series firmware v06.02 and earlier sold in Japan.Color imageCLASS LBP630C/Color imageCLASS MF650C Series/imageCLASS LBP230 Series/imageCLASS X LBP1238 II/imageCLASS MF450 Series/imageCLASS X MF1238 II/imageCLASS X MF1643i II/imageCLASS X MF1643iF II firmware v06.02 and earlier sold in US.i-SENSYS LBP630C Series/i-SENSYS MF650C Series/i-SENSYS LBP230 Series/1238P II/1238Pr II/i-SENSYS MF450 Series/i-SENSYS MF550 Series/1238i II/1238iF II/imageRUNNER 1643i II/imageRUNNER 1643iF II firmware v06.02 and earlier sold in Europe.	9.8	More Details
CVE-2026-23837	MyTube is a self-hosted downloader and player for several video websites. A vulnerability present in version 1.7.65 and poetntially earlier versions allows unauthenticated users to bypass the mandatory authentication check in the roleBasedAuthMiddleware. By simply not providing an authentication cookie (making req.user undefined), a request is incorrectly passed through to downstream handlers. All users running MyTube with loginEnabled: true are impacted. This flaw allows an attacker to access and modify application settings via /api/settings, change administrative and visitor passwords, and access other protected routes that rely on this specific middleware. The problem is patched in v1.7.66. MyTube maintainers recommend all users upgrade to at least version v1.7.64 immediately to secure their instances. The fix ensures that the middleware explicitly blocks requests if a user is not authenticated, rather than defaulting to next(). Those who cannot upgrade immediately can mitigate risk by restricting network access by usi a firewall or reverse proxy (like Nginx) to restrict access to the /api/ endpoints to trusted IP addresses only or, if they are comfortable editing the source code, manually patch by locating roleBasedAuthMiddleware and ensuring that the logic defaults to an error (401 Unauthorized) when req.user is undefined, instead of calling next().	9.8	More Details
CVE-2026-0905	Insufficient policy enforcement in Network in Google Chrome prior to 144.0.7559.59 allowed an attack who obtained a network log file to potentially obtain potentially sensitive information via a network log file. (Chromium security severity: Medium)	9.8	More Details
CVE-2026-0906	Incorrect security UI in Google Chrome on Android prior to 144.0.7559.59 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Low)	9.8	More Details
CVE-2026-0907	Incorrect security UI in Split View in Google Chrome prior to 144.0.7559.59 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	9.8	More Details
CVE-2026-1221	PrismX MX100 AP controller developed by BROWAN COMMUNICATIONS has a Use of Hard-coded Credentials vulnerability, allowing unauthenticated remote attackers to log in to the database using hardcoded database credentials stored in the firmware.	9.8	More Details

CVE-2025-14533	The Advanced Custom Fields: Extended plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 0.9.2.1. This is due to the 'insert_user' function not restricting the roles with which a user can register. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site. Note: The vulnerability can only be exploited if 'role' is mapped to the custom field.	9.8	More Details
CVE-2025-56005	An undocumented and unsafe feature in the PLY (Python Lex-Yacc) library 3.11 allows Remote Code Execution (RCE) via the `picklefile` parameter in the `yacc()` function. This parameter accepts a `.pkl` file that is deserialized with `pickle.load()` without validation. Because `pickle` allows execution of embedded code via `__reduce__()`, an attacker can achieve code execution by passing a malicious pickle file. The parameter is not mentioned in official documentation or the GitHub repository, yet it is active in the PyPI version. This introduces a stealthy backdoor and persistence risk.	9.8	More Details
CVE-2025-14234	Buffer overflow in CPCA list processing on Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *: Satera LBP670C Series/Satera MF750C Series firmware v06.02 and earlier sold in Japan.Color imageCLASS LBP630C/Color imageCLASS MF650C Series/imageCLASS LBP230 Series/imageCLASS X LBP1238 II/imageCLASS MF450 Series/imageCLASS X MF1238 II/imageCLASS X MF1643i II/imageCLASS X MF1643iF II firmware v06.02 and earlier sold in US.i-SENSYS LBP630C Series/i-SENSYS MF650C Series/i-SENSYS LBP230 Series/1238P II/1238Pr II/i-SENSYS MF450 Series/i-SENSYS MF550 Series/1238i II/1238iF II/imageRUNNER 1643i II/imageRUNNER 1643iF II firmware v06.02 and earlier sold in Europe.	9.8	More Details
CVE-2025-14235	Buffer overflow in XPS font fpgm data processing on Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *: Satera LBP670C Series/Satera MF750C Series firmware v06.02 and earlier sold in Japan.Color imageCLASS LBP630C/Color imageCLASS MF650C Series/imageCLASS LBP230 Series/imageCLASS X LBP1238 II/imageCLASS MF450 Series/imageCLASS X MF1238 II/imageCLASS X MF1643i II/imageCLASS X MF1643iF II firmware v06.02 and earlier sold in US.i-SENSYS LBP630C Series/i-SENSYS MF650C Series/i-SENSYS LBP230 Series/1238P II/1238Pr II/i-SENSYS MF450 Series/i-SENSYS MF550 Series/1238i II/1238iF II/imageRUNNER 1643i II/imageRUNNER 1643iF II firmware v06.02 and earlier sold in Europe.	9.8	More Details
CVE-2025-14232	Buffer overflow in XML processing of XPS file in Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *: Satera LBP670C Series/Satera MF750C Series firmware v06.02 and earlier sold in Japan.Color imageCLASS LBP630C/Color imageCLASS MF650C Series/imageCLASS LBP230 Series/imageCLASS X LBP1238 II/imageCLASS MF450 Series/imageCLASS X MF1238 II/imageCLASS X MF1643i II/imageCLASS X MF1643iF II firmware v06.02 and earlier sold in US.i-SENSYS LBP630C Series/i-SENSYS MF650C Series/i-SENSYS LBP230 Series/1238P II/1238Pr II/i-SENSYS MF450 Series/i-SENSYS MF550 Series/1238i II/1238iF II/imageRUNNER 1643i II/imageRUNNER 1643iF II firmware v06.02 and earlier sold in Europe.	9.8	More Details
CVE-2021-47781	Cmder Console Emulator 1.3.18 contains a buffer overflow vulnerability that allows attackers to trigger a denial of service condition through a maliciously crafted .cmd file. Attackers can create a specially constructed .cmd file with repeated characters to overwhelm the console emulator's buffer and crash the application.	9.8	More Details
	The News and Blog Designer Bundle plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.1 via the template parameter.		

CVE-2025-14502	This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	9.8	More Details
CVE-2025-70968	FreeImage 3.18.0 contains a Use After Free in PluginTARGA.cpp;loadRLE().	9.8	More Details
CVE-2026-22852	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, a malicious RDP server can trigger a heap-buffer-overflow write in the FreeRDP client when processing Audio Input (AUDIN) format lists. audin_process_formats reuses callback->formats_count across multiple MSG_SNDIN_FORMATS PDUs and writes past the newly allocated formats array, causing memory corruption and a crash. This vulnerability is fixed in 3.20.1.	9.8	More Details
CVE-2026-22853	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, RDPEAR's NDR array reader does not perform bounds checking on the on-wire element count and can write past the heap buffer allocated from hints, causing a heap buffer overflow in ndr_read_uint8Array. This vulnerability is fixed in 3.20.1.	9.8	More Details
CVE-2026-22854	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, a heap-buffer-overflow occurs in drive read when a server-controlled read length is used to read file data into an IRP output stream buffer without a hard upper bound, allowing an oversized read to overwrite heap memory. This vulnerability is fixed in 3.20.1.	9.8	More Details
CVE-2026-22857	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, a heap use-after-free occurs in irp_thread_func because the IRP is freed by irp->Complete() and then accessed again on the error path. This vulnerability is fixed in 3.20.1.	9.8	More Details
CVE-2021-47753	phpKF CMS 3.00 Beta y6 contains an unauthenticated file upload vulnerability that allows remote attackers to execute arbitrary code by bypassing file extension checks. Attackers can upload a PHP file disguised as a PNG, rename it, and execute system commands through a crafted web shell parameter.	9.8	More Details
CVE-2021-47755	Oliver Library Server v5 contains a file download vulnerability that allows unauthenticated attackers to access arbitrary system files through unsanitized input in the FileServlet endpoint. Attackers can exploit the vulnerability by manipulating the 'fileName' parameter to download sensitive files from the server's filesystem.	9.8	More Details
CVE-2025-14231	Buffer overflow in print job processing by WSD on Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *: Satera LBP670C Series/Satera MF750C Series firmware v06.02 and earlier sold in Japan.Color imageCLASS LBP630C/Color imageCLASS MF650C Series/imageCLASS LBP230 Series/imageCLASS X LBP1238 II/imageCLASS MF450 Series/imageCLASS X MF1238 II/imageCLASS X MF1643i II/imageCLASS X MF1643iF II firmware v06.02 and earlier sold in US.i-SENSYS LBP630C Series/i-SENSYS MF650C Series/i-SENSYS LBP230 Series/1238P II/1238Pr II/i-SENSYS MF450 Series/i-SENSYS MF550 Series/1238i II/1238iF II/imageRUNNER 1643i II/imageRUNNER 1643iF II firmware v06.02 and earlier sold in Europe.	9.8	More Details
CVE-2021-47772	10-Strike Network Inventory Explorer Pro 9.31 contains a buffer overflow vulnerability in the text file import functionality that allows remote code execution. Attackers can craft a malicious text file with carefully constructed payload to trigger a reverse shell and execute arbitrary code on the target system.	9.8	More Details

CVE-2021-47774	Kingdia CD Extractor 3.0.2 contains a buffer overflow vulnerability in the registration name field that allows attackers to execute arbitrary code. Attackers can craft a malicious payload exceeding 256 bytes to overwrite Structured Exception Handler and gain remote code execution through a bind shell.	9.8	More Details
CVE-2021-47760	TestLink versions 1.16 through 1.19 contain an unauthenticated file download vulnerability in the attachmentdownload.php endpoint. Attackers can download arbitrary files by iterating file IDs through the 'id' parameter with 'skipCheck=1' to bypass access controls.	9.8	More Details
CVE-2021-47819	ProjeQtOr Project Management 9.1.4 contains a file upload vulnerability that allows guest users to upload malicious PHP files with arbitrary code execution capabilities. Attackers can upload a PHP script through the profile attachment section and execute system commands by accessing the uploaded file with a specially crafted request parameter.	9.8	More Details
CVE-2025-70892	Phpgurukul Cyber Cafe Management System v1.0 contains a SQL Injection vulnerability in the user management module. The application fails to properly validate user-supplied input in the username parameter of the add-users.php endpoint.	9.8	More Details
CVE-2021-47798	NoteBurner 2.35 contains a buffer overflow vulnerability in the license code input field that allows attackers to crash the application. Attackers can generate a 6000-byte payload and paste it into the 'Name' and 'Code' fields to trigger an application crash.	9.8	More Details
CVE-2021-47796	Denver SHC-150 Smart Wifi Camera contains a hardcoded telnet credential vulnerability that allows unauthenticated attackers to access a Linux shell. Attackers can connect to port 23 using the default credential to execute arbitrary commands on the camera's operating system.	9.8	More Details
CVE-2021-47785	Ether MP3 CD Burner 1.3.8 contains a buffer overflow vulnerability in the registration name field that allows remote code execution. Attackers can craft a malicious payload to overwrite SEH handlers and execute a bind shell on port 3110 by exploiting improper input validation.	9.8	More Details
CVE-2026-21969	Vulnerability in the Oracle Agile Product Lifecycle Management for Process product of Oracle Supply Chain (component: Supplier Portal). The supported version that is affected is 6.2.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile Product Lifecycle Management for Process. Successful attacks of this vulnerability can result in takeover of Oracle Agile Product Lifecycle Management for Process. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2025-62193	Sites running NOAA PMEL Live Access Server (LAS) are vulnerable to remote code execution via specially crafted requests that include PyFerret expressions. By leveraging a SPAWN command, a remote, unauthenticated attacker can execute arbitrary OS commands. Fixed in a version of 'gov.noaa.pmel.tmap.las.filter.RequestInputFilter.java' from 2025-09-24.	9.8	More Details
CVE-2025-67079	File upload vulnerability in Omnispace Agora Project before 25.10 allowing attackers to execute code through the MSL engine of the Imagick library via crafted PDF file to the file upload and thumbnail functions.	9.8	More Details
CVE-2025-53912	An arbitrary file read vulnerability exists in the encapsulatedDoc functionality of MedDream PACS Premium 7.3.6.870. A specially crafted HTTP request can lead to an arbitrary file read. An attacker can send http request to trigger this vulnerability.	9.6	More Details

CVE-2026-23523	Dive is an open-source MCP Host Desktop Application that enables integration with function-calling LLMs. Prior to 0.13.0, crafted deeplink can install an attacker-controlled MCP server configuration without sufficient user confirmation and can lead to arbitrary local command execution on the victim’s machine. This vulnerability is fixed in 0.13.0.	9.6	More Details
CVE-2025-67822	A vulnerability in the Provisioning Manager component of Mitel MiVoice MX-ONE 7.3 (7.3.0.0.50) through 7.8 SP1 (7.8.1.0.14) could allow an unauthenticated attacker to conduct an authentication bypass attack due to improper authentication mechanisms. A successful exploit could allow an attacker to gain unauthorized access to user or admin accounts in the system.	9.4	More Details
CVE-2026-23839	Movary is a web application to track, rate and explore your movie watch history. Due to insufficient input validation, attackers can trigger cross-site scripting payloads in versions prior to 0.70.0. The vulnerable parameter is `?categoryUpdated=`. Version 0.70.0 fixes the issue.	9.3	More Details
CVE-2026-23840	Movary is a web application to track, rate and explore your movie watch history. Due to insufficient input validation, attackers can trigger cross-site scripting payloads in versions prior to 0.70.0. The vulnerable parameter is `?categoryDeleted=`. Version 0.70.0 fixes the issue.	9.3	More Details
CVE-2026-23841	Movary is a web application to track, rate and explore your movie watch history. Due to insufficient input validation, attackers can trigger cross-site scripting payloads in versions prior to 0.70.0. The vulnerable parameter is `?categoryCreated=`. Version 0.70.0 fixes the issue.	9.3	More Details
CVE-2026-22908	Uploading unvalidated container images may allow remote attackers to gain full access to the system, potentially compromising its integrity and confidentiality.	9.1	More Details
CVE-2026-23722	WeGIA is a Web Manager for Charitable Institutions. Prior to 3.6.2, a Reflected Cross-Site Scripting (XSS) vulnerability was discovered in the WeGIA system, specifically within the html/memorando/insere_despacho.php file. The application fails to properly sanitize or encode user-supplied input via the id_memorando GET parameter before reflecting it into the HTML source (likely inside a <script> block or an attribute). This allows unauthenticated attackers to inject arbitrary JavaScript or HTML into the context of the user's browser session. This vulnerability is fixed in 3.6.2.	9.1	More Details
CVE-2026-22858	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, global-buffer-overflow was observed in FreeRDP's Base64 decoding path. The root cause appears to be implementation-defined char signedness: on Arm/AArch64 builds, plain char is treated as unsigned, so the guard c <= 0 can be optimized into a simple c != 0 check. As a result, non-ASCII bytes (e.g., 0x80-0xFF) may bypass the intended range restriction and be used as an index into a global lookup table, causing out-of-bounds access. This vulnerability is fixed in 3.20.1.	9.1	More Details
CVE-2026-22855	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, a heap out-of-bounds read occurs in the smartcard SetAttrib path when cbAttrLen does not match the actual NDR buffer length. This vulnerability is fixed in 3.20.1.	9.1	More Details
CVE-2026-22859	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, the URBDRC client does not perform bounds checking on server-supplied MSUSB_INTERFACE_DESCRIPTOR values and uses them as indices in libusb_udev_complete_msconfig_setup, causing an out-of-bounds read. This vulnerability is fixed in 3.20.1.	9.1	More Details
	Arcane provides modern docker management. Prior to 1.13.0, Arcane has a		

CVE-2026-23520	command injection in the updater service. Arcane's updater service supported lifecycle labels com.getarcaneapp.arcane.lifecycle.pre-update and com.getarcaneapp.arcane.lifecycle.post-update that allowed defining a command to run before or after a container update. The label value is passed directly to /bin/sh -c without sanitization or validation. Because any authenticated user (not limited to administrators) can create projects through the API, an attacker can create a project that specifies one of these lifecycle labels with a malicious command. When an administrator later triggers a container update (either manually or via scheduled update checks), Arcane reads the lifecycle label and executes its value as a shell command inside the container. This vulnerability is fixed in 1.13.0.	9.0	More Details
CVE-2026-1009	A stored cross-site scripting (XSS) vulnerability exists in the Altium Forum due to missing server-side input sanitization in forum post content. An authenticated attacker can inject arbitrary JavaScript into forum posts, which is stored and executed when other users view the affected post. Successful exploitation allows the attacker's payload to execute in the context of the victim's authenticated Altium 365 session, enabling unauthorized access to workspace data, including design files and workspace settings. Exploitation requires user interaction to view a malicious forum post.	9.0	More Details
CVE-2026-1181	A stored cross-site scripting (XSS) vulnerability exists in the Altium Forum due to missing server-side input sanitization in forum post content. An authenticated attacker can inject arbitrary JavaScript into forum posts, which is stored and executed when other users view the affected post. Successful exploitation allows the attacker's payload to execute in the context of the victim's authenticated Altium 365 session, enabling unauthorized access to workspace data, including design files and workspace settings. Exploitation requires user interaction to view a malicious forum post.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-23527	H3 is a minimal H(TTP) framework built for high performance and portability. Prior to 1.15.5, there is a critical HTTP Request Smuggling vulnerability. readRawBody is doing a strict case-sensitive check for the Transfer-Encoding header. It explicitly looks for "chunked", but per the RFC, this header should be case-insensitive. This vulnerability is fixed in 1.15.5.	8.9	More Details
CVE-2026-0908	Use after free in ANGLE in Google Chrome prior to 144.0.7559.59 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2025-15347	The Creator LMS – The LMS for Creators, Coaches, and Trainers plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check in the get_items_permissions_check function in all versions up to, and including, 1.1.12. This makes it possible for authenticated attackers, with contributor level access and above, to update arbitrary WordPress options.	8.8	More Details
CVE-2026-1155	A vulnerability was found in Totolink LR350 9.3.5u.6369_B20220309. Affected by this vulnerability is the function setWiFiEasyGuestCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ssid results in buffer overflow. The attack may be performed from remote. The exploit has been made public and could be used.	8.8	More Details
CVE-	A vulnerability was determined in Totolink LR350 9.3.5u.6369_B20220309. Affected by this issue is the function setWiFiBasicCfg of the file /cgi-bin/cstecgi.cgi. This		More

2026-1156	manipulation of the argument ssid causes buffer overflow. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	8.8	Details
CVE-2026-1157	A vulnerability was identified in Totolink LR350 9.3.5u.6369_B20220309. This affects the function setWiFiEasyCfg of the file /cgi-bin/cstecgi.cgi. Such manipulation of the argument ssid leads to buffer overflow. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2025-12957	The All-in-One Video Gallery plugin for WordPress is vulnerable to arbitrary file upload in all versions up to, and including, 4.5.7. This is due to insufficient file type validation detecting VTT files, allowing double extension files to bypass sanitization while being accepted as a valid VTT file. This makes it possible for authenticated attackers, with author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2025-33015	IBM Concert 1.0.0 through 2.1.0 is vulnerable to malicious file upload by not validating the content of the file uploaded to the web interface.	8.8	More Details
CVE-2021-47788	WebsiteBaker 2.13.0 contains an authenticated remote code execution vulnerability that allows users with language editing permissions to execute arbitrary code. Attackers can exploit the language installation endpoint by manipulating language installation parameters to achieve remote code execution on the server.	8.8	More Details
CVE-2026-1158	A security flaw has been discovered in Totolink LR350 9.3.5u.6369_B20220309. This vulnerability affects 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 can be initiated remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2025-13062	The Supreme Modules Lite plugin for WordPress is vulnerable to arbitrary file upload in all versions up to, and including, 2.5.62. This is due to insufficient file type validation detecting JSON files, allowing double extension files to bypass sanitization while being accepted as a valid JSON file. This makes it possible for authenticated attackers, with author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2025-65118	The vulnerability, if exploited, could allow an authenticated miscreant (OS Standard User) to trick Process Optimization services into loading arbitrary code and escalate privileges to OS System, potentially resulting in complete compromise of the Model Application Server.	8.8	More Details
CVE-2026-23742	Skipper is an HTTP router and reverse proxy for service composition. The default skipper configuration before 0.23.0 was -lua-sources=inline,file. The problem starts if untrusted users can create lua filters, because of -lua-sources=inline , for example through a Kubernetes Ingress resource. The configuration inline allows these user to create a script that is able to read the filesystem accessible to the skipper process and if the user has access to read the logs, they an read skipper secrets. This vulnerability is fixed in 0.23.0.	8.8	More Details
CVE-2026-0902	Inappropriate implementation in V8 in Google Chrome prior to 144.0.7559.59 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-0900	Inappropriate implementation in V8 in Google Chrome prior to 144.0.7559.59 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-	Out of bounds memory access in V8 in Google Chrome prior to 144.0.7559.59 allowed a remote attacker to potentially exploit object corruption via a crafted HTML	8.8	More

0899	page. (Chromium security severity: High)		Details
CVE-2021-47794	ZesleCP 3.1.9 contains an authenticated remote code execution vulnerability that allows attackers to create malicious FTP accounts with shell injection payloads. Attackers can exploit the FTP account creation endpoint by injecting a reverse shell command that establishes a network connection to a specified listening host.	8.8	More Details
CVE-2026-23950	node-tar,a Tar for Node.js, has a race condition vulnerability in versions up to and including 7.5.3. This is due to an incomplete handling of Unicode path collisions in the `path-reservations` system. On case-insensitive or normalization-insensitive filesystems (such as macOS APFS, In which it has been tested), the library fails to lock colliding paths (e.g., `ß` and `ss`), allowing them to be processed in parallel. This bypasses the library's internal concurrency safeguards and permits Symlink Poisoning attacks via race conditions. The library uses a `PathReservations` system to ensure that metadata checks and file operations for the same path are serialized. This prevents race conditions where one entry might clobber another concurrently. This is a Race Condition which enables Arbitrary File Overwrite. This vulnerability affects users and systems using node-tar on macOS (APFS/HFS+). Because of using `NFD` Unicode normalization (in which `ß` and `ss` are different), conflicting paths do not have their order properly preserved under filesystems that ignore Unicode normalization (e.g., APFS (in which `ß` causes an inode collision with `ss`)). This enables an attacker to circumvent internal parallelization locks (`PathReservations`) using conflicting filenames within a malicious tar archive. The patch in version 7.5.4 updates `path-reservations.js` to use a normalization form that matches the target filesystem's behavior (e.g., `NFKD`), followed by first `toLocaleLowerCase('en')` and then `toLocaleUpperCase('en')`. As a workaround, users who cannot upgrade promptly, and who are programmatically using `node-tar` to extract arbitrary tarball data should filter out all `SymbolicLink` entries (as npm does) to defend against arbitrary file writes via this file system entry name collision issue.	8.8	More Details
CVE-2026-23492	Pimcore is an Open Source Data & Experience Management Platform. Prior to 12.3.1 and 11.5.14, an incomplete SQL injection patch in the Admin Search Find API allows an authenticated attacker to perform blind SQL injection. Although CVE-2023-30848 attempted to mitigate SQL injection by removing SQL comments (--) and catching syntax errors, the fix is insufficient. Attackers can still inject SQL payloads that do not rely on comments and infer database information via blind techniques. This vulnerability affects the admin interface and can lead to database information disclosure. This vulnerability is fixed in 12.3.1 and 11.5.14.	8.8	More Details
CVE-2025-64691	The vulnerability, if exploited, could allow an authenticated miscreant (OS standard user) to tamper with TCL Macro scripts and escalate privileges to OS system, potentially resulting in complete compromise of the model application server.	8.8	More Details
CVE-2026-1139	A vulnerability has been found in UTT 进取 520W 1.7.7-180627. This vulnerability affects the function strcpy of the file /goform/ConfigExceptMSN. The manipulation leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-70893	A time-based blind SQL Injection vulnerability exists in PHPGurukul Cyber Cafe Management System v1.0 within the adminprofile.php endpoint. The application fails to properly sanitize user-supplied input provided via the adminname parameter, allowing authenticated attackers to inject arbitrary SQL expressions.	8.8	More Details
CVE-2021-47757	Chikitsa Patient Management System 2.0.2 contains an authenticated remote code execution vulnerability in the backup restoration functionality. Authenticated attackers can upload a modified backup zip file with a malicious PHP shell to execute arbitrary system commands on the server.	8.8	More Details

CVE-2021-47758	Chikitsa Patient Management System 2.0.2 contains an authenticated remote code execution vulnerability that allows attackers to upload malicious PHP plugins through the module upload functionality. Authenticated attackers can generate and upload a ZIP plugin with a PHP backdoor that enables arbitrary command execution on the server through a weaponized PHP script.	8.8	More Details
CVE-2026-1143	A weakness has been identified in TOTOLINK A3700R 9.1.2u.5822_B20200513. This affects the function setWiFiEasyGuestCfg of the file /cgi-bin/cstecgi.cgi. Executing a manipulation of the argument ssid can lead to buffer overflow. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2025-67077	File upload vulnerability in Omnispace Agora Project before 25.10 allowing authenticated, or under certain conditions also guest users, via the UploadTmpFile action.	8.8	More Details
CVE-2025-61973	A local privilege escalation vulnerability exists during the installation of Epic Games Store via the Microsoft Store. A low-privilege user can replace a DLL file during the installation process, which may result in unintended elevation of privileges.	8.8	More Details
CVE-2026-1140	A vulnerability was found in UTT 进取 520W 1.7.7-180627. This issue affects the function strcpy of the file /goform/ConfigExceptAli. The manipulation results in buffer overflow. It is possible to launch the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2021-47816	Thecus N4800Eco NAS Server Control Panel contains a command injection vulnerability that allows authenticated attackers to execute arbitrary system commands through user management endpoints. Attackers can inject commands via username and batch user creation parameters to execute shell commands with administrative privileges.	8.8	More Details
CVE-2026-1138	A flaw has been found in UTT 进取 520W 1.7.7-180627. This affects the function strcpy of the file /goform/ConfigExceptQQ. Executing a manipulation can lead to buffer overflow. The attack may be performed from remote. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-1137	A vulnerability was detected in UTT 进取 520W 1.7.7-180627. Affected by this issue is the function strcpy of the file /goform/formWebAuthGlobalConfig. Performing a manipulation results in buffer overflow. The attack is possible to be carried out remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-0695	In ConnectWise PSA versions older than 2026.1, Time Entry notes stored in the Time Entry Audit Trail may be rendered without applying output encoding to certain content. Under specific conditions, this may allow stored script code to execute in the context of a user’s browser when the affected content is displayed.	8.7	More Details
CVE-2026-23625	OpenProject is an open-source, web-based project management software. Versions 16.3.0 through 16.6.4 are affected by a stored cross-site scripting vulnerability in the Roadmap view. OpenProject’s roadmap view renders the “Related work packages” list for each version. When a version contains work packages from a different project (e.g., a subproject), the helper link_to_work_package prepends package.project.to_s to the link and returns the entire string with .html_safe. Because project names are user-controlled and no escaping happens before calling html_safe, any HTML placed in a subproject name is injected verbatim into the page. The underlying issue is mitigated in versions 16.6.5 and 17.0.0 by setting a `X-Content-Type-Options: nosniff` header, which was in place until a refactoring move to Rails standard content-security policy, which did not properly apply this header in	8.7	More Details

	the new configuration since OpenProject 16.3.0. Those who cannot upgrade their installations should ensure that they add a X-Content-Type-Options: nosniff header in their proxying web application server.		
CVE-2026-22867	LaSuite Doc is a collaborative note taking, wiki and documentation platform. From 3.8.0 to 4.3.0, a Stored Cross-Site Scripting (XSS) vulnerability exists in the Interlinking feature. When a user creates a link to another document within the editor, the URL of that link is not validated. An attacker with document editing privileges can inject a malicious javascript: URL that executes arbitrary code when other users click on the link. This vulnerability is fixed in 4.4.0.	8.7	More Details
CVE-2026-21967	Vulnerability in the Oracle Hospitality OPERA 5 product of Oracle Hospitality Applications (component: Opera Servlet). Supported versions that are affected are 5.6.19.23, 5.6.25.17, 5.6.26.10 and 5.6.27.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality OPERA 5 accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality OPERA 5. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L).	8.6	More Details
CVE-2026-23493	Pimcore is an Open Source Data & Experience Management Platform. Prior to 12.3.1 and 11.5.14, the http_error_log file stores the $_COOKIE and $_SERVER variables, which means sensitive information such as database passwords, cookie session data, and other details can be accessed or recovered through the Pimcore backend. This vulnerability is fixed in 12.3.1 and 11.5.14.	8.6	More Details
CVE-2026-0532	External Control of File Name or Path (CWE-73) combined with Server-Side Request Forgery (CWE-918) can allow an attacker to cause arbitrary file disclosure through a specially crafted credentials JSON payload in the Google Gemini connector configuration. This requires an attacker to have authenticated access with privileges sufficient to create or modify connectors (Alerts & Connectors: All). The server processes a configuration without proper validation, allowing for arbitrary network requests and for arbitrary file reads.	8.6	More Details
CVE-2026-23949	jaraco.context, an open-source software package that provides some useful decorators and context managers, has a Zip Slip path traversal vulnerability in the `jaraco.context.tarball()` function starting in version 5.2.0 and prior to version 6.1.0. The vulnerability may allow attackers to extract files outside the intended extraction directory when malicious tar archives are processed. The strip_first_component filter splits the path on the first `/` and extracts the second component, while allowing `../` sequences. Paths like `dummy_dir/../../etc/passwd` become `../../etc/passwd`. Note that this suffers from a nested tarball attack as well with multi-level tar files such as `dummy_dir/inner.tar.gz`, where the inner.tar.gz includes a traversal `dummy_dir/../../config/.env` that also gets translated to `../../config/.env`. Version 6.1.0 contains a patch for the issue.	8.6	More Details
CVE-2026-23512	SumatraPDF is a multi-format reader for Windows. In 3.5.2 and earlier, there is a Untrusted Search Path vulnerability when Advanced Options setting is trigger. The application executes notepad.exe without specifying an absolute path when using the Advanced Options setting. On Windows, this allows execution of a malicious notepad.exe placed in the application's installation directory, leading to arbitrary code execution.	8.6	More Details
	Using string formatting and exception handling, an attacker may bypass n8n's python-task-executor sandbox restrictions and run arbitrary unrestricted Python code in the underlying operating system. The vulnerability can be exploited via the		

CVE-2026-0863	Code block by an authenticated user with basic permissions and can lead to a full n8n instance takeover on instances operating under "Internal" execution mode. If the instance is operating under the "External" execution mode (ex. n8n's official Docker image) - arbitrary code execution occurs inside a Sidecar container and not the main node, which significantly reduces the vulnerability impact.	8.5	More Details
CVE-2025-61943	The vulnerability, if exploited, could allow an authenticated miscreant (Process Optimization Standard User) to tamper with queries in Captive Historian and achieve code execution under SQL Server administrative privileges, potentially resulting in complete compromise of the SQL Server.	8.4	More Details
CVE-2026-22037	The @fastify/express plugin adds full Express compatibility to Fastify. A security vulnerability exists in @fastify/express prior to version 4.0.3 where middleware registered with a specific path prefix can be bypassed using URL-encoded characters (e.g., `/%61dmin` instead of `/admin`). While the middleware engine fails to match the encoded path and skips execution, the underlying Fastify router correctly decodes the path and matches the route handler, allowing attackers to access protected endpoints without the middleware constraints. The vulnerability is caused by how @fastify/express matches requests against registered middleware paths. This vulnerability is similar to, but differs from, CVE-2026-22031 because this is a different npm module with its own code. Version 4.0.3 of @fastify/express contains a patch fort the issue.	8.4	More Details
CVE-2026-22031	@fastify/middie is the plugin that adds middleware support on steroids to Fastify. A security vulnerability exists in @fastify/middie prior to version 9.1.0 where middleware registered with a specific path prefix can be bypassed using URL-encoded characters (e.g., `/%61dmin` instead of `/admin`). While the middleware engine fails to match the encoded path and skips execution, the underlying Fastify router correctly decodes the path and matches the route handler, allowing attackers to access protected endpoints without the middleware constraints. Version 9.1.0 fixes the issue.	8.4	More Details
CVE-2025-68957	Multi-thread race condition vulnerability in the card framework module. Impact: Successful exploitation of this vulnerability may affect availability.	8.4	More Details
CVE-2025-12985	IBM Licensing Operator incorrectly assigns privileges to security critical files which could allow a local root escalation inside a container running the IBM Licensing Operator image.	8.4	More Details
CVE-2025-14115	IBM Sterling Connect:Direct for UNIX Container 6.3.0.0 through 6.3.0.6 Interim Fix 016, and 6.4.0.0 through 6.4.0.3 Interim Fix 019 IBM® Sterling Connect:Direct for UNIX contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.	8.4	More Details
CVE-2021-47775	YouTube Video Grabber, now referred to as YouTube Downloader, 1.9.9.1 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting the Structured Exception Handler. Attackers can craft a malicious payload of 712 bytes with SEH manipulation to trigger a bind shell connection on a specified local port.	8.4	More Details
CVE-2021-47756	Laravel Valet versions 1.1.4 to 2.0.3 contain a local privilege escalation vulnerability that allows users to modify the valet command with root privileges. Attackers can edit the symlinked valet command to execute arbitrary code with root permissions without additional authentication.	8.4	More Details
CVE-	An insecure authentication mechanism in the safe_exec.sh startup script of Blurams Flare Camera version 24.1114.151.929 and earlier allows an attacker with physical		

2025-65397	access to the device to execute arbitrary commands with root privileges, if file /opt/images/public_key.der is not present in the file system. The vulnerability can be triggered by providing a maliciously crafted auth.ini file on the device's SD card.	8.4	More Details
CVE-2025-68960	Multi-thread race condition vulnerability in the video framework module. Impact: Successful exploitation of this vulnerability may affect availability.	8.4	More Details
CVE-2026-0861	Passing too large an alignment to the memalign suite of functions (memalign, posix_memalign, aligned_alloc) in the GNU C Library version 2.30 to 2.42 may result in an integer overflow, which could consequently result in a heap corruption. Note that the attacker must have control over both, the size as well as the alignment arguments of the memalign function to be able to exploit this. The size parameter must be close enough to PTRDIFF_MAX so as to overflow size_t along with the large alignment argument. This limits the malicious inputs for the alignment for memalign to the range [1<<62+ 1, 1<<63] and exactly 1<<63 for posix_memalign and aligned_alloc. Typically the alignment argument passed to such functions is a known constrained quantity (e.g. page size, block size, struct sizes) and is not attacker controlled, because of which this may not be easily exploitable in practice. An application bug could potentially result in the input alignment being too large, e.g. due to a different buffer overflow or integer overflow in the application or its dependent libraries, but that is again an uncommon usage pattern given typical sources of alignments.	8.4	More Details
CVE-2026-0713	A security vulnerability in the /apis/dashboard.grafana.app/* endpoints allows authenticated users to bypass dashboard and folder permissions. The vulnerability affects all API versions (v0alpha1, v1alpha1, v2alpha1). Impact: - Viewers can view all dashboards/folders regardless of permissions - Editors can view/edit/delete all dashboards/folders regardless of permissions - Editors can create dashboards in any folder regardless of permissions - Anonymous users with viewer/editor roles are similarly affected Organization isolation boundaries remain intact. The vulnerability only affects dashboard access and does not grant access to datasources.	8.3	More Details
CVE-2026-22643	In Grafana, an excessively long dashboard title or panel name will cause Chromium browsers to become unresponsive due to Improper Input Validation vulnerability in Grafana. This issue affects Grafana: before 11.6.2 and is fixed in 11.6.2 and higher.	8.3	More Details
CVE-2026-22638	A cross-site scripting (XSS) vulnerability exists in Grafana caused by combining a client path traversal and open redirect. This allows attackers to redirect users to a website that hosts a frontend plugin that will execute arbitrary JavaScript. This vulnerability does not require editor permissions and if anonymous access is enabled, the XSS will work. If the Grafana Image Renderer plugin is installed, it is possible to exploit the open redirect to achieve a full read SSRF. The default Content-Security-Policy (CSP) in Grafana will block the XSS though the `connect-src` directive.	8.3	More Details
CVE-2026-22850	Koko Analytics is an open-source analytics plugin for WordPress. Versions prior to 2.1.3 are vulnerable to arbitrary SQL execution through unescaped analytics export/import and permissive admin SQL import. Unauthenticated visitors can submit arbitrary path (`pa`) and referrer (`r`) values to the public tracking endpoint in src/Resources/functions/collect.php, which stores those strings verbatim in the analytics tables. The admin export logic in src/Admin/Data_Export.php writes these stored values directly into SQL INSERT statements without escaping. A crafted path such as "),('999','x');DROP TABLE wp_users;-- breaks out of the value list. When an administrator later imports that export file, the import handler in src/Admin/Data_Import.php reads the uploaded SQL with file_get_contents, performs only a superficial header check, splits on semicolons, and executes each statement via $wpdb->query with no validation of table names or statement types.	8.3	More Details

	Additionally, any authenticated user with manage_koko_analytics can upload an arbitrary .sql file and have it executed in the same permissive way. Combined, attacker-controlled input flows from the tracking endpoint into exported SQL and through the import execution sink, or directly via malicious uploads, enabling arbitrary SQL execution. In a worst-case scenario, attackers can achieve arbitrary SQL execution on the WordPress database, allowing deletion of core tables (e.g., wp_users), insertion of backdoor administrator accounts, or other destructive/privilege-escalating actions. Version 2.1.3 patches the issue.		
CVE-2025-70298	GPAC v2.4.0 was discovered to contain an out-of-bounds read in the oggdmx_parse_tags function.	8.2	More Details
CVE-2021-47811	Grocery Crud 1.6.4 contains a SQL injection vulnerability in the order_by parameter that allows remote attackers to manipulate database queries. Attackers can inject malicious SQL code through the order_by[] parameter in POST requests to the ajax_list endpoint to potentially extract or modify database information.	8.2	More Details
CVE-2021-47777	Build Smart ERP 21.0817 contains an unauthenticated SQL injection vulnerability in the 'eidValue' parameter of the login validation endpoint. Attackers can inject stacked SQL queries using payloads like ';WAITFOR DELAY '0:0:3'-- to manipulate database queries and potentially extract or modify database information.	8.2	More Details
CVE-2021-47782	Odine Solutions GateKeeper 1.0 contains a SQL injection vulnerability in the trafficCycle API endpoint that allows remote attackers to inject malicious database queries. Attackers can exploit the vulnerability by sending crafted payloads to the /rass/api/v1/trafficCycle/ endpoint to manipulate PostgreSQL database queries and potentially extract sensitive information.	8.2	More Details
CVE-2021-47801	Vianeos OctoPUS 5 contains a time-based blind SQL injection vulnerability in the 'login_user' parameter during authentication requests. Attackers can exploit this vulnerability by crafting malicious POST requests with specially constructed SQL payloads that trigger database sleep functions to extract information.	8.2	More Details
CVE-2021-47763	Aimeos 2021.10 LTS contains a SQL injection vulnerability in the json api 'sort' parameter that allows attackers to inject malicious database queries. Attackers can manipulate the sort parameter to reveal table and column names by sending crafted GET requests to the jsonapi/review endpoint.	8.2	More Details
CVE-2025-67823	A vulnerability in the Multimedia Email component of Mitel MiContact Center Business through 10.2.0.10 and Mitel CX through 1.1.0.1 could allow an unauthenticated attacker to conduct a Cross-Site Scripting (XSS) attack due to insufficient input validation. A successful exploit requires user interaction where the email channel is enabled. This could allow an attacker to execute arbitrary scripts in the victim's browser or desktop client application.	8.2	More Details
CVE-2025-14844	The Membership Plugin – Restrict Content plugin for WordPress is vulnerable to Missing Authentication in all versions up to, and including, 3.2.16 via the 'rcp_stripe_create_setup_intent_for_saved_card' function due to missing capability check. Additionally, the plugin does not check a user-controlled key, which makes it possible for unauthenticated attackers to leak Stripe SetupIntent client_secret values for any membership.	8.2	More Details
CVE-2026-21987	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2	8.2	More Details

	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).		
CVE-2026-21988	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2026-21990	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2026-21956	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2026-21955	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2026-21973	Vulnerability in the Oracle FLEXCUBE Investor Servicing product of Oracle Financial Services Applications (component: Security Management System). Supported versions that are affected are 14.5.0.15.0, 14.7.0.8.0 and 14.8.0.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized access to critical data or complete access to all Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2025-14510	Incorrect Implementation of Authentication Algorithm vulnerability in ABB ABB Ability OPTIMAX.This issue affects ABB Ability OPTIMAX: 6.1, 6.2, from 6.3.0 before 6.3.1-251120, from 6.4.0 before 6.4.1-251120.	8.1	More Details
	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization		

CVE-2026-21989	(component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data as well as unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L).	8.1	More Details
CVE-2026-23876	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-13 and 6.9.13-38, a heap buffer overflow vulnerability in the XBM image decoder (ReadXBMImage) allows an attacker to write controlled data past the allocated heap buffer when processing a maliciously crafted image file. Any operation that reads or identifies an image can trigger the overflow, making it exploitable via common image upload and processing pipelines. Versions 7.1.2-13 and 6.9.13-38 fix the issue.	8.1	More Details
CVE-2026-23846	Tugtainer is a self-hosted app for automating updates of Docker containers. In versions prior to 1.16.1, the password authentication mechanism transmits passwords via URL query parameters instead of the HTTP request body. This causes passwords to be logged in server access logs and potentially exposed through browser history, Referer headers, and proxy logs. Version 1.16.1 patches the issue.	8.1	More Details
CVE-2025-64729	The vulnerability, if exploited, could allow an authenticated miscreant (OS Standard User) to tamper with Process Optimization project files, embed code, and escalate their privileges to the identity of a victim user who subsequently interacts with the project files.	8.1	More Details
CVE-2026-22864	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Before 2.5.6, a prior patch aimed to block spawning Windows batch/shell files by returning an error when a spawned path’s extension matched .bat or .cmd. That check performs a case-sensitive comparison against lowercase literals and therefore can be bypassed when the extension uses alternate casing (for example .BAT, .Bat, etc.). This vulnerability is fixed in 2.5.6.	8.1	More Details
CVE-2025-62291	In the eap-mschapv2 plugin (client-side) in strongSwan before 6.0.3, a malicious EAP-MSCHAPv2 server can send a crafted message of size 6 through 8, and cause an integer underflow that potentially results in a heap-based buffer overflow.	8.1	More Details
CVE-2026-22856	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, a race in the serial channel IRP thread tracking allows a heap use-after-free when one thread removes an entry from serial->IrpThreads while another reads it. This vulnerability is fixed in 3.20.1.	8.1	More Details
CVE-2025-14977	The Dokan: AI Powered WooCommerce Multivendor Marketplace Solution – Build Your Own Amazon, eBay, Etsy plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 4.2.4 via the `/wp-json/dokan/v1/settings` REST API endpoint due to missing validation on a user-controlled key. This makes it possible for authenticated attackers, with customer-level permissions and above, to read or modify other vendors' store settings including sensitive payment information (PayPal email, bank account details, routing numbers, IBAN, SWIFT codes), phone numbers, and addresses, and change PayPal email addresses to attacker-controlled addresses, enabling financial theft when the marketplace processes payouts.	8.1	More Details
	The Nexter Extension – Site Enhancements Toolkit plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 4.4.6 via		

CVE-2026-0726	deserialization of untrusted input in the 'nxt_unserialize_replace' function. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	8.1	More Details
CVE-2025-66292	DPanel is an open source server management panel written in Go. Prior to 1.9.2, DPanel has an arbitrary file deletion vulnerability in the /api/common/attach/delete interface. Authenticated users can delete arbitrary files on the server via path traversal. When a user logs into the administrative backend, this interface can be used to delete files. The vulnerability lies in the Delete function within the app/common/http/controller/attach.go file. The path parameter submitted by the user is directly passed to storage.Local{}.GetSaveRealPath and subsequently to os.Remove without proper sanitization or checking for path traversal characters (../). And the helper function in common/service/storage/local.go uses filepath.Join, which resolves ../ but does not enforce a chroot/jail. This vulnerability is fixed in 1.9.2.	8.1	More Details
CVE-2026-1010	A stored cross-site scripting (XSS) vulnerability exists in the Altium Workflow Engine due to missing server-side input sanitization in workflow form submission APIs. A regular authenticated user can inject arbitrary JavaScript into workflow data. When an administrator views the affected workflow, the injected payload executes in the administrator’s browser context, allowing privilege escalation, including creation of new administrator accounts, session token theft, and execution of administrative actions.	8.0	More Details
CVE-2026-20960	Improper authorization in Microsoft Power Apps allows an authorized attacker to execute code over a network.	8.0	More Details
CVE-2025-68958	Multi-thread race condition vulnerability in the card framework module. Impact: Successful exploitation of this vulnerability may affect availability.	8.0	More Details
CVE-2025-68956	Multi-thread race condition vulnerability in the card framework module. Impact: Successful exploitation of this vulnerability may affect availability.	8.0	More Details
CVE-2025-68955	Multi-thread race condition vulnerability in the card framework module. Impact: Successful exploitation of this vulnerability may affect availability.	8.0	More Details
CVE-2026-23535	wlc is a Weblate command-line client using Weblate's REST API. Prior to 1.17.2, the multi-translation download could write to an arbitrary location when instructed by a crafted server. This vulnerability is fixed in 1.17.2.	8.0	More Details
CVE-2025-0647	In certain Arm CPUs, a CPP RCTX instruction executed on one Processing Element (PE) may inhibit TLB invalidation when a TLBI is issued to the PE, either by the same PE or another PE in the shareability domain. In this case, the PE may retain stale TLB entries which should have been invalidated by the TLBI.	7.9	More Details
CVE-2021-47803	iFunbox 4.2 contains an unquoted service path vulnerability in the Apple Mobile Device Service that allows local attackers to execute code with elevated privileges. Attackers can insert a malicious executable into the unquoted service path to run with LocalSystem privileges when the service restarts.	7.8	More Details
CVE-2021-	Wise Care 365 5.6.7.568 contains an unquoted service path vulnerability in the WiseBootAssistant service running with LocalSystem privileges. Attackers can exploit this by inserting a malicious executable in the service path, which will	7.8	More Details

47804	execute with elevated system privileges when the service restarts.		
CVE-2021-47805	Disk Savvy 13.6.14 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 path in service binaries to inject malicious executables that will be run with elevated LocalSystem privileges.	7.8	More Details
CVE-2021-47806	Dup Scout 13.5.28 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 path in 'C:\Program Files\Dup Scout Server\bin\dupscts.exe' to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2021-47807	Sync Breeze 13.6.18 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 path in service binaries located in 'Program Files' directories to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2021-47809	Disk Sorter Enterprise 13.6.12 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 path in 'C:\Program Files\Disk Sorter Enterprise\bin\disksrs.exe' to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2021-47792	Remote Mouse 4.002 contains an unquoted service path vulnerability that allows local attackers to execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted service path in the RemoteMouseService to inject malicious executables and gain administrative access.	7.8	More Details
CVE-2021-47790	Active WebCam 11.5 contains an unquoted service path vulnerability that allows local attackers to execute arbitrary code with elevated system privileges. Attackers can exploit the misconfigured service path by placing malicious executables in specific directory locations to gain administrative access.	7.8	More Details
CVE-2025-33233	NVIDIA Merlin Transformers4Rec for all platforms contains a vulnerability where an attacker could cause code injection. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2025-33206	NVIDIA NSIGHT Graphics for Linux contains a vulnerability where an attacker could cause command injection. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and denial of service.	7.8	More Details
CVE-2021-47780	Macro Expert 4.7 contains an unquoted service path vulnerability that allows local users to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the improperly configured service path to inject malicious executables that will be run with LocalSystem permissions during service startup.	7.8	More Details
CVE-2020-36930	SysGauge Server 7.9.18 contains an unquoted service path vulnerability in its binary path configuration that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in 'C:\Program Files\SysGauge Server\bin\sysgaus.exe' to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2020-36929	Brother BRPrint Auditor 3.0.7 contains an unquoted service path vulnerability in its Windows service configurations that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted file paths in BrAuSvc and BRPA_Agent services to inject malicious executables and escalate privileges on the system.	7.8	More Details
CVE-	Brother BRAgent 1.38 contains an unquoted service path vulnerability in the WBA_Agent_Client service running with LocalSystem privileges. Attackers can		More

2020-36928	exploit the unquoted path in C:\Program Files (x86)\Brother\BRAgent\ to inject and execute malicious code with elevated system permissions.	7.8	Details
CVE-2020-36927	DiskPulse Enterprise 13.6.14 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 path in 'C:\Program Files\Disk Pulse Enterprise\bin\diskpls.exe' to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2025-68968	Double free vulnerability in the multi-mode input module. Impact: Successful exploitation of this vulnerability may affect the input function.	7.8	More Details
CVE-2025-13455	A vulnerability was reported in ThinkPlus configuration software that could allow a local authenticated user to bypass ThinkPlus device authentication and enroll an untrusted fingerprint.	7.8	More Details
CVE-2021-47773	Dynojet Power Core 2.3.0 contains an unquoted service path vulnerability in the DJ.UpdateService that allows local authenticated users to potentially execute code with elevated privileges. Attackers can exploit the unquoted binary path by placing malicious executables in the service's file path to gain Local System access.	7.8	More Details
CVE-2021-47767	10-Strike Network Inventory Explorer Pro 9.31 contains an unquoted service path vulnerability in the srvInventoryWebServer service running with LocalSystem privileges. Attackers can exploit the unquoted path by placing malicious executables in potential path segments to achieve privilege escalation and execute code with system-level permissions.	7.8	More Details
CVE-2021-47762	HTTPDebuggerPro 9.11 contains an unquoted service path vulnerability that allows local attackers to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted binary path in the service configuration to inject malicious executables and gain elevated access to the system.	7.8	More Details
CVE-2021-47761	MilleGPG5 5.7.2 contains a local privilege escalation vulnerability that allows authenticated users to modify service executable files in the MariaDB bin directory. Attackers can replace the mysqld.exe with a malicious executable, which will execute with system privileges when the computer restarts.	7.8	More Details
CVE-2025-12053	The drivers in the tool packages use RTL_QUERY_REGISTRY_DIRECT flag to read a registry value to which an untrusted user-mode application may be able to cause a buffer overflow.	7.8	More Details
CVE-2025-12052	The drivers in the tool packages use RTL_QUERY_REGISTRY_DIRECT flag to read a registry value to which an untrusted user-mode application may be able to cause a buffer overflow.	7.8	More Details
CVE-2021-47810	WibuKey Runtime 6.51 contains an unquoted service path vulnerability in the WkSvW32.exe service that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in 'C:\PROGRAM FILES (X86)\WIBUKEY\SERVER\WkSvW32.exe' to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2021-47787	TotalAV 5.15.69 contains an unquoted service path vulnerability in multiple system services running with LocalSystem privileges. Attackers can place malicious executables in specific unquoted path segments to potentially gain SYSTEM-level access by exploiting the service path configuration.	7.8	More Details
CVE-2025-12050	The drivers in the tool packages use RTL_QUERY_REGISTRY_DIRECT flag to read a registry value to which an untrusted user-mode application may be able to cause a buffer overflow.	7.8	More Details

CVE-2021-47832	Sandboxie Plus 0.7.4 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 path during system startup or reboot to inject and run malicious executables with LocalSystem permissions.	7.8	More Details
CVE-2021-47822	DiskBoss Service 12.2.18 contains an unquoted service path vulnerability in its binary path configuration that allows local attackers to execute code with elevated privileges. Attackers can exploit the unquoted path by placing malicious executables in potential path locations to gain system-level access during service startup.	7.8	More Details
CVE-2021-47823	Acer ePowerSvc 6.0.3008.0 contains an unquoted service path vulnerability that allows local users to potentially execute code with elevated system privileges. Attackers can exploit the unquoted path in the service configuration to inject malicious code that would execute with LocalSystem permissions during service startup.	7.8	More Details
CVE-2024-44238	The issue was addressed with improved bounds checks. This issue is fixed in iOS 18.1 and iPadOS 18.1. An app may be able to corrupt coprocessor memory.	7.8	More Details
CVE-2025-68921	SteelSeries Nahimic 3 1.10.7 allows Directory traversal.	7.8	More Details
CVE-2021-47826	Acer Backup Manager 3.0.0.99 contains an unquoted service path vulnerability in the NTI IScheduleSvc service that allows local users to potentially execute arbitrary code. Attackers can exploit the unquoted path in C:\Program Files (x86)\NTI\Acer Backup Manager\ to inject malicious executables that would run with elevated LocalSystem privileges.	7.8	More Details
CVE-2025-12051	The drivers in the tool packages use RTL_QUERY_REGISTRY_DIRECT flag to read a registry value to which an untrusted user-mode application may be able to cause a buffer overflow.	7.8	More Details
CVE-2021-47828	BOOTP Turbo 2.0.0.1253 contains an unquoted service path vulnerability in its Windows service configuration. Attackers can exploit the unquoted path to execute arbitrary code with elevated LocalSystem privileges during system startup or reboot.	7.8	More Details
CVE-2021-47829	DHCP Broadband 4.1.0.1503 contains an unquoted service path vulnerability in its service configuration that allows local attackers to execute code with elevated privileges. Attackers can exploit the unquoted path in 'C:\Program Files\DHCP Broadband 4\dhcpt.exe' to inject malicious code that will execute during service startup with LocalSystem permissions.	7.8	More Details
CVE-2026-0975	Delta Electronics DIAView has Command Injection vulnerability.	7.8	More Details
CVE-2021-47825	Acer Updater Service 1.2.3500.0 contains an unquoted service path vulnerability that allows local users to execute code with elevated system privileges. Attackers can exploit the unquoted path in C:\Program Files\Acer\Acer Updater\ to inject malicious executables that will run with LocalSystem permissions during service startup.	7.8	More Details
CVE-2021-47845	Spy Emergency 25.0.650 contains an unquoted service path vulnerability in its Windows service configurations that allows local attackers to execute code with elevated privileges. Attackers can exploit the unquoted file paths in SpyEmergencyHealth.exe and SpyEmergencySrv.exe to inject malicious code during system startup or service restart.	7.8	More Details

CVE-2021-47847	Disk Sorter Server 13.6.12 contains an unquoted service path vulnerability in its binary path configuration that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in 'C:\Program Files\Disk Sorter Server\bin\disksrs.exe' to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2021-47833	WifiHotSpot 1.0.0.0 contains an unquoted service path vulnerability in its WifiHotSpotService.exe that allows local attackers to execute code with elevated privileges. Attackers can exploit the unquoted path during system startup or reboot to inject and run malicious executables with LocalSystem permissions.	7.8	More Details
CVE-2025-48647	In cpm_fwtp_msg_handler of cpm/google/lib/tracepoint/cpm_fwtp_ipc.c, there is a possible memory overwrite due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-23529	Kafka Connect BigQuery Connector is an implementation of a sink connector from Apache Kafka to Google BigQuery. Prior to 2.11.0, there is an arbitrary file read in Google BigQuery Sink connector. Aiven's Google BigQuery Kafka Connect Sink connector requires Google Cloud credential configurations for authentication to BigQuery services. During connector configuration, users can supply credential JSON files that are processed by Google authentication libraries. The service fails to validate externally-sourced credential configurations before passing them to the authentication libraries. An attacker can exploit this by providing a malicious credential configuration containing crafted credential_source.file paths or credential_source.url endpoints, resulting in arbitrary file reads or SSRF attacks.	7.7	More Details
CVE-2025-11224	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.10 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2 that could have allowed an authenticated user to execute stored cross-site scripting through improper input validation in the Kubernetes proxy functionality.	7.7	More Details
CVE-2026-23477	Rocket.Chat is an open-source, secure, fully customizable communications platform. In Rocket.Chat versions up to 6.12.0, the API endpoint GET /api/v1/oauth-apps.get is exposed to any authenticated user, regardless of their role or permissions. This endpoint returns an OAuth application, as long as the user knows its ID, including potentially sensitive fields such as client_id and client_secret. This vulnerability is fixed in 6.12.0.	7.7	More Details
CVE-2026-1007	Incorrect Authorization vulnerability in virtual gateway component in Devolutions Server allows attackers to bypass deny IP rules.This issue affects Server: from 2025.3.1 through 2025.3.12.	7.6	More Details
CVE-2026-1008	A stored cross-site scripting (XSS) vulnerability exists in the user profile text fields of Altium 365. Insufficient server-side input sanitization allows authenticated users to inject arbitrary HTML and JavaScript payloads using whitespace-based attribute parsing bypass techniques. The injected payload is persisted and executed when other users view the affected profile page, potentially allowing session token theft, phishing attacks, or malicious redirects. Exploitation requires an authenticated account and user interaction to view the crafted profile.	7.6	More Details
CVE-2026-0712	An open redirect vulnerability has been identified in Grafana OSS that can be exploited to achieve XSS attacks. The vulnerability was introduced in Grafana v11.5.0. The open redirect can be chained with path traversal vulnerabilities to achieve XSS. Fixed in versions 12.0.2+security-01, 11.6.3+security-01, 11.5.6+security-01, 11.4.6+security-01 and 11.3.8+security-01	7.6	More Details
CVE-	Svelte devalue is a JavaScript library that serializes values into strings when JSON.stringify isn't sufficient for the job. From 5.1.0 to 5.6.1, certain inputs can cause devalue.parse to consume excessive CPU time and/or memory, potentially		

2026-22775	leading to denial of service in systems that parse input from untrusted sources. This affects applications using devalue.parse on externally-supplied data. The root cause is the ArrayBuffer hydration expecting base64 encoded strings as input, but not checking the assumption before decoding the input. This vulnerability is fixed in 5.6.2.	7.5	More Details
CVE-2024-48077	An issue in nanomq v0.22.7 allows attackers to cause a Denial of Service (DoS) via a crafted request. The number of data packets received in the recv-q queue of the Nanomq process continues to increase, causing the nanomq broker to fall into a deadlock and be unable to provide normal services.	7.5	More Details
CVE-2025-70744	Tenda AX-1806 v1.0.0.1 was discovered to contain a stack overflow in the cloneType parameter of the sub_65B5C function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-71019	Tenda AX-1806 v1.0.0.1 was discovered to contain a stack overflow in the wanSpeed parameter of the sub_65B5C function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-70307	A stack overflow in the dump_ttxt_sample function of GPAC v2.4.0 allows attackers to cause a Denial of Service (DoS) via a crafted packet.	7.5	More Details
CVE-2026-21982	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	7.5	More Details
CVE-2026-21983	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details
CVE-2026-23490	pyasn1 is a generic ASN.1 library for Python. Prior to 0.6.2, a Denial-of-Service issue has been found that leads to memory exhaustion from malformed RELATIVE-OID with excessive continuation octets. This vulnerability is fixed in 0.6.2.	7.5	More Details
CVE-2025-60003	A Buffer Over-read vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). When an affected device receives a BGP update with a set of specific optional transitive attributes over an established peering session, rpd will crash and restart when attempting to advertise the received information to another peer. This issue can only happen if one or both of the BGP peers of the receiving session are non-4-byte-AS capable as determined from the advertised capabilities during BGP session establishment. Junos OS and Junos OS Evolved default behavior is 4-byte-AS capable unless this has been specifically disabled by configuring: [protocols bgp ... disable-4byte-as] Established BGP sessions can be checked by executing: show bgp neighbor <IP address> | match "4 byte AS" This issue affects: Junos OS: * all versions before 22.4R3-S8, * 23.2 versions before 23.2R2-S5, * 23.4 versions before 23.4R2-S6, * 24.2 versions before 24.2R2-S2, * 24.4 versions before 24.4R2; Junos OS Evolved: * all versions	7.5	More Details

	before 22.4R3-S8-EVO, * 23.2 versions before 23.2R2-S5-EVO, * 23.4 versions before 23.4R2-S6-EVO, * 24.2 versions before 24.2R2-S2-EVO, * 24.4 versions before 24.4R2-EVO.		
CVE-2026-22774	Svelte devalue is a JavaScript library that serializes values into strings when JSON.stringify isn't sufficient for the job. From 5.3.0 to 5.6.1, certain inputs can cause devalue.parse to consume excessive CPU time and/or memory, potentially leading to denial of service in systems that parse input from untrusted sources. This affects applications using devalue.parse on externally-supplied data. The root cause is the typed array hydration expecting an ArrayBuffer as input, but not checking the assumption before creating the typed array. This vulnerability is fixed in 5.6.2.	7.5	More Details
CVE-2021-47752	AWebServer GhostBuilding 18 contains a denial of service vulnerability that allows remote attackers to overwhelm the server by sending multiple concurrent HTTP requests. Attackers can generate high-volume requests to multiple endpoints including /mysqladmin to potentially crash or render the service unresponsive.	7.5	More Details
CVE-2026-22265	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. Prior to 8.2.8.2, command injection vulnerability exists in the log viewing functionality that allows authenticated users to execute arbitrary system commands. The vulnerability is in app/modules/roxywi/logs.py line 87, where the grep parameter is used twice - once sanitized and once raw. This vulnerability is fixed in 8.2.8.2.	7.5	More Details
CVE-2025-70656	Tenda AX-1806 v1.0.0.1 was discovered to contain a stack overflow in the mac parameter of the sub_65B5C function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-70308	An out-of-bounds read in the GSF demuxer filter component of GPAC v2.4.0 allows attackers to cause a Denial of Service (DoS) via a crafted .gsf file.	7.5	More Details
CVE-2025-70304	A buffer overflow in the vobsub_get_subpic_duration() function of GPAC v2.4.0 allows attackers to cause a Denial of Service (DoS) via a crafted packet.	7.5	More Details
CVE-2026-21984	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details
CVE-2025-66417	GLPI is a free asset and IT management software package. From 11.0.0, < 11.0.3, an unauthenticated user can perform a SQL injection through the inventory endpoint. This vulnerability is fixed in 11.0.3.	7.5	More Details
CVE-2021-47824	iDailyDiary 4.30 contains a denial of service vulnerability that allows attackers to crash the application by overflowing the preferences tab name field. Attackers can paste a 2,000,000 character buffer into the default diary tab name to trigger an application crash.	7.5	More Details
CVE-2026-	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may		More

21957	significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	Details
CVE-2025-67076	Directory traversal vulnerability in Omnispace Agora Project before 25.10 allowing unauthenticated attackers to read files on the system via the misc controller and the ExternalGetFile action. Only files with an extension can be read.	7.5	More Details
CVE-2025-64516	GLPI is a free asset and IT management software package. Prior to 10.0.21 and 11.0.3, an unauthorized user can access GLPI documents attached to any item (ticket, asset, ...). If the public FAQ is enabled, this unauthorized access can be performed by an anonymous user. This vulnerability is fixed in 10.0.21 and 11.0.3.	7.5	More Details
CVE-2025-68924	In Umbraco UmbracoForms through 8.13.16, an authenticated attacker can supply a malicious WSDL (aka Webservice) URL as a data source for remote code execution.	7.5	More Details
CVE-2021-47784	Cyberfox Web Browser 52.9.1 contains a denial of service vulnerability that allows attackers to crash the application by overflowing the search bar with excessive data. Attackers can generate a 9,000,000 byte payload and paste it into the search bar to trigger an application crash.	7.5	More Details
CVE-2021-47831	Sandboxie 5.49.7 contains a denial of service vulnerability that allows attackers to crash the application by overflowing the container folder input field. Attackers can paste a large buffer of repeated characters into the Sandbox container folder setting to trigger an application crash.	7.5	More Details
CVE-2021-47821	RarmaRadio 2.72.8 contains a denial of service vulnerability that allows attackers to crash the application by overflowing network configuration fields with large character buffers. Attackers can generate a 100,000 character buffer and paste it into multiple network settings fields to trigger application instability and potential crash.	7.5	More Details
CVE-2021-47812	GravCMS 1.10.7 contains an unauthenticated vulnerability that allows remote attackers to write arbitrary YAML configuration and execute PHP code through the scheduler endpoint. Attackers can exploit the admin-nonce parameter to inject base64-encoded payloads and create malicious custom jobs with system command execution.	7.5	More Details
CVE-2026-21905	A Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in the SIP application layer gateway (ALG) of Juniper Networks Junos OS on SRX Series and MX Series with MX-SPC3 or MS-MPC allows an unauthenticated network-based attacker sending specific SIP messages over TCP to crash the flow management process, leading to a Denial of Service (DoS). On SRX Series, and MX Series with MX-SPC3 or MS-MPC service cards, receipt of multiple SIP messages causes the SIP headers to be parsed incorrectly, eventually causing a continuous loop and leading to a watchdog timer expiration, crashing the flowd process on SRX Series and MX Series with MX-SPC3, or mspmand process on MX Series with MS-MPC. This issue only occurs over TCP. SIP messages sent over UDP cannot trigger this issue. This issue affects Junos OS on SRX Series and MX Series with MX-SPC3 and MS-MPC: * all versions before 21.2R3-S10, * from 21.4 before 21.4R3-S12, * from 22.4 before 22.4R3-S8, * from 23.2 before 23.2R2-S5, * from 23.4 before 23.4R2-S6, * from 24.2 before 24.2R2-S3, * from 24.4 before 24.4R2-S1, * from 25.2 before 25.2R1-S1, 25.2R2.	7.5	More Details
CVE-2021-	Leawo Prof. Media 11.0.0.1 contains a denial of service vulnerability that allows attackers to crash the application by supplying an oversized payload in the activation keycode field. Attackers can generate a 6000-byte buffer of repeated		More

47797	characters to trigger an application crash when pasted into the registration interface.	7.5	Details
CVE-2021-47786	Redragon Gaming Mouse driver contains a kernel-level vulnerability that allows attackers to trigger a denial of service by sending malformed IOCTL requests. Attackers can send a crafted 2000-byte buffer with specific byte patterns to the REDRAGON_MOUSE device to crash the kernel driver.	7.5	More Details
CVE-2025-14478	The Demo Importer Plus plugin for WordPress is vulnerable to XML External Entity Injection (XXE) in all versions up to, and including, 2.0.9 via the SVG file upload functionality. This makes it possible for authenticated attackers, with Author-level access and above, to achieve code execution in vulnerable configurations. This only impacts sites on versions of PHP older than 8.0.	7.5	More Details
CVE-2025-68438	In Apache Airflow versions before 3.1.6, when rendered template fields in a Dag exceed [core] max_templated_field_length, sensitive values could be exposed in cleartext in the Rendered Templates UI. This occurred because serialization of those fields used a secrets masker instance that did not include user-registered mask_secret() patterns, so secrets were not reliably masked before truncation and display. Users are recommended to upgrade to 3.1.6 or later, which fixes this issue	7.5	More Details
CVE-2021-47789	Yenkee Hornet Gaming Mouse driver GM312Fltr.sys contains a buffer overrun vulnerability that allows attackers to crash the system by sending oversized input. Attackers can exploit the driver by sending a 2000-byte buffer through DeviceIoControl to trigger a kernel-level system crash.	7.5	More Details
CVE-2025-29847	A vulnerability in Apache Linkis. Problem Description When using the JDBC engine and da When using the JDBC engine and data source functionality, if the URL parameter configured on the frontend has undergone multiple rounds of URL encoding, it may bypass the system's checks. This bypass can trigger a vulnerability that allows unauthorized access to system files via JDBC parameters. Scope of Impact This issue affects Apache Linkis: from 1.3.0 through 1.7.0. Severity level moderate Solution Continuously check if the connection information contains the "%" character; if it does, perform URL decoding. Users are recommended to upgrade to version 1.8.0, which fixes the issue. More questions about this vulnerability can be discussed here: https://lists.apache.org/list?dev@linkis.apache.org:2025-9:cve	7.5	More Details
CVE-2021-47791	SmartFTP Client 10.0.2909.0 contains multiple denial of service vulnerabilities that allow attackers to crash the application through specific input manipulation. Attackers can trigger crashes by entering malformed paths, using invalid IP addresses, or clearing connection history in the client's interface.	7.5	More Details
CVE-2021-47793	Telegram Desktop 2.9.2 contains a denial of service vulnerability that allows attackers to crash the application by sending an oversized message payload. Attackers can generate a 9 million byte buffer and paste it into the messaging interface to trigger an application crash.	7.5	More Details
CVE-2026-1023	Statistics Database System developed by Gotac has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to directly exploit a specific functionality to query database contents.	7.5	More Details
CVE-2026-	An Improper Handling of Exceptional Conditions vulnerability in the packet forwarding engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated network-based attacker sending a specific ICMP packet through a GRE tunnel to cause the PFE to crash and restart. When PowerMode IPsec (PMI) and GRE performance acceleration are enabled and the device receives a specific ICMP packet, a crash occurs in the SRX PFE, resulting in traffic loss. PMI is enabled by default, and GRE performance acceleration can be enabled by running the	7.5	More

21906	configuration command shown below. PMI is a mode of operation that provides IPsec performance improvements using Vector Packet Processing. Note that PMI with GRE performance acceleration is only supported on specific SRX platforms. This issue affects Junos OS on the SRX Series: * all versions before 21.4R3-S12, * from 22.4 before 22.4R3-S8, * from 23.2 before 23.2R2-S5, * from 23.4 before 23.4R2-S5, * from 24.2 before 24.2R2-S3, * from 24.4 before 24.4R2-S1, * from 25.2 before 25.2R1-S1, 25.2R2.		Details
CVE-2026-1022	Statistics Database System developed by Gotac has an Arbitrary File Read vulnerability, allowing unauthenticated remote attackers to exploit Relative Path Traversal to download arbitrary system files.	7.5	More Details
CVE-2026-1018	Police Statistics Database System developed by Gotac has an Arbitrary File Read vulnerability, allowing Unauthenticated remote attacker to exploit Absolute Path Traversal to download arbitrary system files.	7.5	More Details
CVE-2025-61684	Quicly, an IETF QUIC protocol implementation, is susceptible to a denial-of-service attack prior to commit d9d3df6a8530a102b57d840e39b0311ce5c9e14e. A remote attacker can exploit these bugs to trigger an assertion failure that crashes process using Quicly. Commit d9d3df6a8530a102b57d840e39b0311ce5c9e14e fixes the issue.	7.5	More Details
CVE-2025-68616	WeasyPrint helps web developers to create PDF documents. Prior to version 68.0, a server-side request forgery (SSRF) protection bypass exists in WeasyPrint's `default_url_fetcher`. The vulnerability allows attackers to access internal network resources (such as `localhost` services or cloud metadata endpoints) even when a developer has implemented a custom `url_fetcher` to block such access. This occurs because the underlying `urllib` library follows HTTP redirects automatically without re-validating the new destination against the developer's security policy. Version 68.0 contains a patch for the issue.	7.5	More Details
CVE-2026-23842	ChatterBot is a machine learning, conversational dialog engine for creating chat bots. ChatterBot versions up to 1.2.10 are vulnerable to a denial-of-service condition caused by improper database session and connection pool management. Concurrent invocations of the get_response() method can exhaust the underlying SQLAlchemy connection pool, resulting in persistent service unavailability and requiring a manual restart to recover. Version 1.2.11 fixes the issue.	7.5	More Details
CVE-2021-47815	Nsauditor 3.2.3 contains a denial of service vulnerability in the registration code input field that allows attackers to crash the application. Attackers can paste a large buffer of 256 repeated characters into the 'Key' field to trigger an application crash.	7.5	More Details
CVE-2021-47814	NBMonitor 1.6.8 contains a denial of service vulnerability that allows attackers to crash the application by overflowing the registration code input field. Attackers can paste a 256-character buffer into the registration key field to trigger an application crash and potential system instability.	7.5	More Details
CVE-2025-68675	In Apache Airflow versions before 3.1.6, the proxies and proxy fields within a Connection may include proxy URLs containing embedded authentication information. These fields were not treated as sensitive by default and therefore were not automatically masked in log output. As a result, when such connections are rendered or printed to logs, proxy credentials embedded in these fields could be exposed. Users are recommended to upgrade to 3.1.6 or later, which fixes this issue	7.5	More Details
CVE-2025-14894	Livewire Filemanager, commonly used in Laravel applications, contains LivewireFilemanagerComponent.php, which does not perform file type and MIME validation, allowing for RCE through upload of a malicious php file that can then be executed via the /storage/ URL if a commonly performed setup process within Laravel applications has been completed.	7.5	More Details

CVE-2026-21926	Vulnerability in the Siebel CRM Deployment product of Oracle Siebel CRM (component: Server Infrastructure). Supported versions that are affected are 17.0-25.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Siebel CRM Deployment. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Siebel CRM Deployment. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2026-0612	The Librarian contains a information leakage vulnerability through the `web_fetch` tool, which can be used to retrieve arbitrary external content provided by an attacker, which can be used to proxy requests through The Librarian infrastructure. The vendor has fixed the vulnerability in all versions of TheLibrarian.	7.5	More Details
CVE-2026-21913	An Incorrect Initialization of Resource vulnerability in the Internal Device Manager (IDM) of Juniper Networks Junos OS on EX4000 models allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). On EX4000 models with 48 ports (EX4000-48T, EX4000-48P, EX4000-48MP) a high volume of traffic destined to the device will cause an FXPC crash and restart, which leads to a complete service outage until the device has automatically restarted. The following reboot reason can be seen in the output of 'show chassis routing-engine' and as a log message: reason=0x4000002 reason_string=0x4000002:watchdog + panic with core dump This issue affects Junos OS on EX4000-48T, EX4000-48P and EX4000-48MP: * 24.4 versions before 24.4R2, * 25.2 versions before 25.2R1-S2, 25.2R2. This issue does not affect versions before 24.4R1 as the first Junos OS version for the EX4000 models was 24.4R1.	7.5	More Details
CVE-2021-47813	Backup Key Recovery 2.2.7 contains a denial of service vulnerability that allows attackers to crash the application by overflowing the registration code input field. Attackers can paste a large buffer of 256 repeated characters into the registration key field to trigger application instability and potential crash.	7.5	More Details
CVE-2021-47818	DupTerminator 1.4.5639.37199 contains a denial of service vulnerability that allows attackers to crash the application by inputting a long character string in the Excluded text box. Attackers can generate a payload of 8000 repeated characters to trigger the application to stop working on Windows 10.	7.5	More Details
CVE-2026-21917	An Improper Validation of Syntactic Correctness of Input vulnerability in the Web-Filtering module of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). If an SRX device configured for UTM Web-Filtering receives a specifically malformed SSL packet, this will cause an FPC crash and restart. This issue affects Junos OS on SRX Series: * 23.2 versions from 23.2R2-S2 before 23.2R2-S5, * 23.4 versions from 23.4R2-S1 before 23.4R2-S5, * 24.2 versions before 24.2R2-S2, * 24.4 versions before 24.4R1-S3, 24.4R2. Earlier versions of Junos are also affected, but no fix is available.	7.5	More Details
CVE-2026-21918	A Double Free vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX and MX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). On all SRX and MX Series platforms, when during TCP session establishment a specific sequence of packets is encountered a double free happens. This causes flowd to crash and the respective FPC to restart. This issue affects Junos OS on SRX and MX Series: * all versions before 22.4R3-S7, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R2.	7.5	More Details
	An Unchecked Return Value vulnerability in the DNS module of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). If an SRX Series device configured for DNS processing,		

CVE-2026-21920	receives a specifically formatted DNS request flowd will crash and restart, which causes a service interruption until the process has recovered. This issue affects Junos OS on SRX Series: * 23.4 versions before 23.4R2-S5, * 24.2 versions before 24.2R2-S1, * 24.4 versions before 24.4R2. This issue does not affect Junos OS versions before 23.4R1.	7.5	More Details
CVE-2026-21945	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17 and 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2026-0915	Calling getnetbyaddr or getnetbyaddr_r with a configured nsswitch.conf that specifies the library's DNS backend for networks and queries for a zero-valued network in the GNU C Library version 2.0 to version 2.42 can leak stack contents to the configured DNS resolver.	7.5	More Details
CVE-2025-71020	Tenda AX-1806 v1.0.0.1 was discovered to contain a stack overflow in the security parameter of the sub_4C408 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-70746	Tenda AX-1806 v1.0.0.1 was discovered to contain a stack overflow in the timeZone parameter of the fromSetSysTime function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2020-36926	SmarterTrack 7922 contains an information disclosure vulnerability in the Chat Management search form that reveals agent identification details. Attackers can access the vulnerable /Management/Chat/frmChatSearch.aspx endpoint to retrieve agents' first and last names along with their unique identifiers.	7.5	More Details
CVE-2026-0943	HarfBuzz::Shaper versions before 0.032 for Perl contains a bundled library with a null pointer dereference vulnerability. Versions before 0.032 contain HarfBuzz 8.4.0 or earlier bundled as hb_src.tar.gz in the source tarball, which is affected by CVE-2026-22693.	7.5	More Details
CVE-2026-0616	TheLibrarians web_fetch tool can be used to retrieve the Adminer interface content, which can then be used to log into the internal TheLibrarian backend system. The vendor has fixed the vulnerability in all affected versions.	7.5	More Details
CVE-2026-0613	The Librarian contains an internal port scanning vulnerability, facilitated by the `web_fetch` tool, which can be used with SSRF-style behavior to perform GET requests to internal IP addresses and services, enabling scanning of the Hertzner cloud environment that TheLibrarian uses. The vendor has fixed the vulnerability in all affected versions.	7.5	More Details
	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: User and User Group). The supported version that is affected is 9.3.6. Easily		

CVE-2026-21940	exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Agile PLM accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2026-21914	An Improper Locking vulnerability in the GTP plugin of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (Dos). If an SRX Series device receives a specifically malformed GPRS Tunnelling Protocol (GTP) Modify Bearer Request message, a lock is acquired and never released. This results in other threads not being able to acquire a lock themselves, causing a watchdog timeout leading to FPC crash and restart. This issue leads to a complete traffic outage until the device has automatically recovered. This issue affects Junos OS on SRX Series: * all versions before 22.4R3-S8, * 23.2 versions before 23.2R2-S5, * 23.4 versions before 23.4R2-S6, * 24.2 versions before 24.2R2-S3, * 24.4 versions before 24.4R2-S2, * 25.2 versions before 25.2R1-S1, 25.2R2.	7.5	More Details
CVE-2021-47827	WebSSH for iOS 14.16.10 contains a denial of service vulnerability in the mashREPL tool that allows attackers to crash the application by pasting malformed input. Attackers can trigger the vulnerability by copying a 300-character buffer of repeated 'A' characters into the mashREPL input field, causing the application to crash.	7.5	More Details
CVE-2026-22910	The device is deployed with weak and publicly known default passwords for certain hidden user levels, increasing the risk of unauthorized access. This represents a high risk to the integrity of the system.	7.5	More Details
CVE-2025-70747	Tenda AX-1806 v1.0.0.1 was discovered to contain a stack overflow in the serviceName parameter of the sub_65A28 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-9142	A local user can trigger Harmony SASE Windows client to write or delete files outside the intended certificate working directory.	7.5	More Details
CVE-2025-14770	The Shipping Rate By Cities plugin for WordPress is vulnerable to SQL Injection via the 'city' parameter in all versions up to, and including, 2.0.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2025-12166	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin plugin for WordPress is vulnerable to blind SQL Injection via the `order` and `append_where_sql` parameters in all versions up to, and including, 1.6.9.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-22909	Certain system functions may be accessed without proper authorization, allowing attackers to start, stop, or delete installed applications, potentially disrupting system operations.	7.5	More Details
CVE-2025-71021	Tenda AX-1806 v1.0.0.1 was discovered to contain a stack overflow in the serverName parameter of the sub_65A28 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-15032	Missing about:blank indicator in custom-sized new windows in Dia before 1.9.0 on macOS could allow an attacker to spoof a trusted domain in the window title and mislead users about the current site.	7.4	More Details

CVE-2025-59960	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Juniper DHCP service (jdhcpd) of Juniper Networks Junos OS and Junos OS Evolved allows a DHCP client in one subnet to exhaust the address pools of other subnets, leading to a Denial of Service (DoS) on the downstream DHCP server. By default, the DHCP relay agent inserts its own Option 82 information when forwarding client requests, optionally replacing any Option 82 information provided by the client. When a specific DHCP DISCOVER is received in 'forward-only' mode with Option 82, the device should drop the message unless 'trust-option82' is configured. Instead, the DHCP relay forwards these packets to the DHCP server unmodified, which uses up addresses in the DHCP server's address pool, ultimately leading to address pool exhaustion. This issue affects Junos OS: * all versions before 21.2R3-S10, * from 21.4 before 21.4R3-S12, * all versions of 22.2, * from 22.4 before 22.4R3-S8, * from 23.2 before 23.2R2-S5, * from 23.4 before 23.4R2-S6, * from 24.2 before 24.2R2-S2, * from 24.4 before 24.4R2, * from 25.2 before 25.2R1-S1, 25.2R2. Junos OS Evolved: * all versions before 21.4R3-S12-EVO, * all versions of 22.2-EVO, * from 22.4 before 22.4R3-S8-EVO, * from 23.2 before 23.2R2-S5-EVO, * from 23.4 before 23.4R2-S6-EVO, * from 24.2 before 24.2R2-S2-EVO, * from 24.4 before 24.4R2-EVO, * from 25.2 before 25.2R1-S1-EVO, 25.2R2-EVO.	7.4	More Details
CVE-2025-65117	The vulnerability, if exploited, could allow an authenticated miscreant (Process Optimization Designer User) to embed OLE objects into graphics, and escalate their privileges to the identity of a victim user who subsequently interacts with the graphical elements.	7.4	More Details
CVE-2026-21932	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: AWT, JavaFX). Supported versions that are affected are Oracle Java SE: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17 and 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.4 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N).	7.4	More Details
CVE-2025-11043	An Improper Certificate Validation vulnerability in the OPC-UA client and ANSL over TLS client used in Automation Studio versions before 6.5 could allow an unauthenticated attacker on the network to position themselves to intercept and interfere with data exchanges.	7.4	More Details
CVE-2025-59870	HCL MyXalytics v6.7 is affected by improper management of a static JWT signing secret in the web application, where the secret lacks rotation , introducing a security risk	7.4	More Details
CVE-2026-1192	A vulnerability was determined in Tosei Online Store Management System ネット店舗管理システム 1.01. The affected element is an unknown function of the file /cgi-bin/imode_alldata.php. Executing a manipulation of the argument DevId can lead to command injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this	7.3	More Details

	disclosure but did not respond in any way.		
CVE-2026-1122	A vulnerability was determined in Yonyou KSOA 9.0. This impacts an unknown function of the file /worksheet/work_info.jsp of the component HTTP GET Parameter Handler. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-1179	A vulnerability was detected in Yonyou KSOA 9.0. This affects an unknown part of the file /kmf/user_popedom.jsp of the component HTTP GET Parameter Handler. The manipulation of the argument folderid results in sql injection. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-1105	A vulnerability was identified in EasyCMS up to 1.6. This vulnerability affects unknown code of the file /UserAction.class.php. Such manipulation of the argument _order leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-1119	A flaw has been found in itsourcecode Society Management System 1.0. The affected element is an unknown function of the file /admin/delete_activity.php. Executing a manipulation of the argument activity_id can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-33230	NVIDIA Nsight Systems for Linux contains a vulnerability in the .run installer, where an attacker could cause an OS command injection by supplying a malicious string to the installation path. A successful exploit of this vulnerability might lead to escalation of privileges, code execution, data tampering, denial of service, and information disclosure.	7.3	More Details
CVE-2026-1059	A security vulnerability has been detected in FeMiner wms up to 9cad1f1b179a98b9547fd003c23b07c7594775fa. Affected by this vulnerability is an unknown functionality of the file /src/chkuser.php. The manipulation of the argument Username leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-33229	NVIDIA Nsight Visual Studio for Windows contains a vulnerability in Nsight Monitor where an attacker can execute arbitrary code with the same privileges as the NVIDIA Nsight Visual Studio Edition Monitor application. A successful exploit of this vulnerability may lead to escalation of privileges, code execution, data tampering, denial of service, and information disclosure.	7.3	More Details
CVE-2025-36418	IBM ApplinX 11.1 is vulnerable due to a privilege escalation vulnerability due to improper verification of JWT tokens. An attacker may be able to craft or modify a JSON web token in order to impersonate another user or to elevate their privileges.	7.3	More Details
CVE-2026-1120	A vulnerability has been found in Yonyou KSOA 9.0. The impacted element is an unknown function of the file /worksheet/del_work.jsp of the component HTTP GET Parameter Handler. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
	A flaw has been found in risesoft-y9 Digital-Infrastructure up to 9.6.7. This affects an		

CVE-2026-1050	unknown function of the file source-code/src/main/java/net/risesoft/util/Y9PlatformUtil.java of the component REST Authenticate Endpoint. Executing a manipulation can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-1121	A vulnerability was found in Yonyou KSOA 9.0. This affects an unknown function of the file /worksheet/del_workplan.jsp of the component HTTP GET Parameter Handler. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-1178	A security vulnerability has been detected in Yonyou KSOA 9.0. Affected by this issue is some unknown functionality of the file /kmf/select.jsp of the component HTTP GET Parameter Handler. The manipulation of the argument folderid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-1123	A vulnerability was identified in Yonyou KSOA 9.0. Affected is an unknown function of the file /worksheet/work_mod.jsp of the component HTTP GET Parameter Handler. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-1124	A security flaw has been discovered in Yonyou KSOA 9.0. Affected by this vulnerability is an unknown functionality of the file /worksheet/work_report.jsp of the component HTTP GET Parameter Handler. Performing a manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-1125	A weakness has been identified in D-Link DIR-823X 250416. Affected by this issue is the function sub_412E7C of the file /goform/set_wifidog_settings. Executing a manipulation of the argument wd_enable can lead to command injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-1202	A security flaw has been discovered in CRMEB up to 5.6.3. The affected element is the function appleLogin of the file crmeb/app/api/controller/v1/LoginController.php. Performing a manipulation of the argument openId results in improper authentication. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-1177	A weakness has been identified in Yonyou KSOA 9.0. Affected by this vulnerability is an unknown functionality of the file /kmf/save_folder.jsp of the component HTTP GET Parameter Handler. Executing a manipulation of the argument folderid can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-1129	A vulnerability was detected in Yonyou KSOA 9.0. This vulnerability affects unknown code of the file /worksheet/worksadd.jsp of the component HTTP GET Parameter Handler. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
	A flaw has been found in Yonyou KSOA 9.0. This issue affects some unknown		

CVE-2026-1130	processing of the file /worksheet/worksadd_plan.jsp of the component HTTP GET Parameter Handler. This manipulation of the argument ID causes sql injection. It is possible to initiate 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-2026-1131	A vulnerability has been found in Yonyou KSOA 9.0. Impacted is an unknown function of the file /kmc/save_catalog.jsp of the component HTTP GET Parameter Handler. Such manipulation of the argument catalogid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-1132	A vulnerability was found in Yonyou KSOA 9.0. The affected element is an unknown function of the file /kmf/edit_folder.jsp of the component HTTP GET Parameter Handler. Performing a manipulation of the argument folderid results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-1133	A vulnerability was determined in Yonyou KSOA 9.0. The impacted element is an unknown function of the file /kmf/folder.jsp of the component HTTP GET Parameter Handler. Executing a manipulation of the argument folderid can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-23880	OnboardLite is a comprehensive membership lifecycle platform built for student organizations at the University of Central Florida. Versions of the software prior to commit 1d32081a66f21bcf41df1ecb672490b13f6e429f have a stored cross-site scripting vulnerability that can be rendered to an admin when they attempt to migrate a user's discord account in the dashboard. Commit 1d32081a66f21bcf41df1ecb672490b13f6e429f patches the issue.	7.3	More Details
CVE-2026-0615	The Librarian `supervisord` status page can be retrieved by the `web_fetch` tool, which can be used to retrieve running processes within TheLibrarian backend. The vendor has fixed the vulnerability in all affected versions.	7.3	More Details
CVE-2026-1159	A weakness has been identified in itsourcecode Online Frozen Foods Ordering System 1.0. This issue affects some unknown processing of the file /order_online.php. Executing a manipulation of the argument product_name can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-1160	A security vulnerability has been detected in PHPGurukul Directory Management System 1.0. Impacted is an unknown function of the file /index.php of the component Search. The manipulation of the argument searchdata leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-1176	A security flaw has been discovered in itsourcecode School Management System 1.0. Affected is an unknown function of the file /subject/index.php. Performing a manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-	A local information disclosure vulnerability exists in the Ludashi driver before 5.1025 due to a lack of access control in the IOCTL handler. This driver exposes a device interface accessible to a normal user and handles attacker-controlled structures containing the lower 4GB of physical addresses. The handler maps arbitrary physical		

2025-67246	memory via MmMapIoSpace and copies data back to user mode without verifying the caller's privileges or the target address range. This allows unprivileged users to read arbitrary physical memory, potentially exposing kernel data structures, kernel pointers, security tokens, and other sensitive information. This vulnerability can be further exploited to bypass the Kernel Address Space Layout Rules (KASLR) and achieve local privilege escalation.	7.3	More Details
CVE-2025-33228	NVIDIA Nsight Systems contains a vulnerability in the gfx_hotspot recipe, where an attacker could cause an OS command injection by supplying a malicious string to the process_nsys_rep_cli.py script if the script is invoked manually. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	7.3	More Details
CVE-2021-47837	Markdownify 1.2.0 contains a persistent cross-site scripting vulnerability that allows attackers to store malicious payloads within markdown files. Attackers can upload crafted markdown files with embedded scripts that execute when the file is opened, potentially enabling remote code execution.	7.2	More Details
CVE-2026-23723	WeGIA is a web manager for charitable institutions. Prior to 3.6.2, an authenticated SQL Injection vulnerability was identified in the Atendido_ocorrenciaControle endpoint via the id_memorando parameter. This flaw allows for full database exfiltration, exposure of sensitive PII, and potential arbitrary file reads in misconfigured environments. This vulnerability is fixed in 3.6.2.	7.2	More Details
CVE-2021-47840	Moeditor 0.2.0 contains a persistent cross-site scripting vulnerability that allows attackers to store malicious payloads within markdown files. Attackers can upload specially crafted markdown files with embedded JavaScript that execute when opened, potentially enabling remote code execution on the victim's system.	7.2	More Details
CVE-2021-47839	Marky 0.0.1 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts into markdown files. Attackers can upload crafted markdown files with embedded JavaScript payloads that execute when the file is opened, potentially enabling remote code execution.	7.2	More Details
CVE-2021-47838	Markright 1.0 contains a persistent cross-site scripting vulnerability that allows attackers to embed malicious payloads in markdown files. Attackers can upload specially crafted markdown files that execute arbitrary JavaScript when opened, potentially enabling remote code execution on the victim's system.	7.2	More Details
CVE-2025-15266	The GeekyBot — Generate AI Content Without Prompt, Chatbot and Lead Generation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the chat message field in all versions up to, and including, 1.1.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an administrator accesses the Chat History page.	7.2	More Details
CVE-2025-14613	The GetContentFromURL plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.0. This is due to the plugin using wp_remote_get() instead of wp_safe_remote_get() to fetch content from a user-supplied URL in the 'url' parameter of the [gcfu] shortcode. This makes it possible for authenticated attackers, with Contributor-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.	7.2	More Details
CVE-2026-1222	PrismX MX100 AP controller developed by BROWAN COMMUNICATIONS has an Arbitrary File Upload vulnerability, allowing privileged remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	7.2	More Details
	Freeter 1.2.1 contains a persistent cross-site scripting vulnerability that allows		

CVE-2021-47835	attackers to store malicious payloads in custom widget titles and files. Attackers can craft malicious files with embedded scripts that execute when victims interact with the application, potentially enabling remote code execution.	7.2	More Details
CVE-2021-47842	StudyMD 0.3.2 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts into markdown files. Attackers can upload crafted markdown files with embedded JavaScript payloads that execute when the file is opened, potentially enabling remote code execution.	7.2	More Details
CVE-2025-15283	The Name Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name_directory_name' and 'name_directory_description' parameters in all versions up to, and including, 1.30.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-15378	The AJS Footnotes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'note_list_class' and 'popup_display_effect_in' parameters in all versions up to, and including, 1.0 due to missing authorization and nonce verification on settings save, as well as insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to update plugin settings and inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-23498	Shopware is an open commerce platform. From 6.7.0.0 to before 6.7.6.1, a regression of CVE-2023-2017 leads to an array and array crafted PHP Closure not checked being against allow list for the map(...) override. This vulnerability is fixed in 6.7.6.1.	7.2	More Details
CVE-2025-31510	In the portal in LemonLDAP::NG before 2.21.0, cross-site scripting (XSS) allows remote attackers to inject arbitrary web script or HTML (into the login page) via the tab parameter, for Choice authentication.	7.2	More Details
CVE-2025-12007	There is a vulnerability in the Supermicro BMC firmware validation logic at Supermicro MBD-X13SEM-F . An attacker can update the system firmware with a specially crafted image.	7.2	More Details
CVE-2021-47779	Dolibarr ERP-CRM 14.0.2 contains a stored cross-site scripting vulnerability in the ticket creation module that allows low-privilege users to inject malicious scripts. Attackers can craft a specially designed ticket message with embedded JavaScript that triggers when an administrator copies the text, potentially enabling privilege escalation.	7.2	More Details
CVE-2021-47808	Cotonti Siena 0.9.19 contains a stored cross-site scripting vulnerability in the admin configuration panel's site title parameter. Attackers can inject malicious JavaScript code through the 'maintitle' parameter to execute scripts when administrators view the page.	7.2	More Details
CVE-2025-37182	Vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to perform SQL injection attacks. Successful exploitation could allow an attacker to execute arbitrary SQL commands on the underlying database, potentially leading to unauthorized data access or data manipulation.	7.2	More Details
CVE-2021-47843	Tagstoo 2.0.1 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious payloads through files or custom tags. Attackers can execute arbitrary JavaScript code to spawn system processes, access files, and perform remote code execution on the victim's computer.	7.2	More Details
	The NotificationX – FOMO, Live Sales Notification, WooCommerce Sales Popup, GDPR, Social Proof, Announcement Banner & Floating Notification Bar plugin for WordPress is vulnerable to DOM-Based Cross-Site Scripting via the 'nx-preview'		

CVE-2025-15380	POST parameter in all versions up to, and including, 3.2.0. This is due to insufficient input sanitization and output escaping when processing preview data. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute when a user visits a malicious page that auto-submits a form to the vulnerable site.	7.2	More Details
CVE-2025-37183	Vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to perform SQL injection attacks. Successful exploitation could allow an attacker to execute arbitrary SQL commands on the underlying database, potentially leading to unauthorized data access or data manipulation.	7.2	More Details
CVE-2025-12006	There is a vulnerability in the Supermicro BMC firmware validation logic at Supermicro MBD-X12STW-F . An attacker can update the system firmware with a specially crafted image.	7.2	More Details
CVE-2025-37181	Vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to perform SQL injection attacks. Successful exploitation could allow an attacker to execute arbitrary SQL commands on the underlying database, potentially leading to unauthorized data access or data manipulation.	7.2	More Details
CVE-2021-47769	Isshue Shopping Cart 3.5 contains a persistent cross-site scripting vulnerability in title input fields across stock, customer, and invoice modules. Attackers with privileged user accounts can inject malicious scripts that execute on preview, potentially enabling session hijacking and persistent phishing attacks.	7.2	More Details
CVE-2025-14615	The DASHBOARD BUILDER – WordPress plugin for Charts and Graphs plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5.7. This is due to missing nonce validation on the settings handler in dashboardbuilder-admin.php. This makes it possible for unauthenticated attackers to modify the stored SQL query and database credentials used by the [show-dashboardbuilder] shortcode via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. The modified SQL query is subsequently executed on the front-end when the shortcode is rendered, enabling arbitrary SQL injection and data exfiltration through the publicly visible chart output.	7.1	More Details
CVE-2026-23843	teklifolustur_app is a web-based PHP application that allows users to create, manage, and track quotes for their clients. Prior to commit dd082a134a225b8dcd401b6224eead4fb183ea1c, an Insecure Direct Object Reference (IDOR) vulnerability exists in the offer view functionality. Authenticated users can manipulate the offer_id parameter to access offers belonging to other users. The issue is caused by missing authorization checks ensuring that the requested offer belonged to the currently authenticated user. Commit dd082a134a225b8dcd401b6224eead4fb183ea1c contains a patch.	7.1	More Details
CVE-2026-22249	Docmost is an open-source collaborative wiki and documentation software. From 0.21.0 to before 0.24.0, Docmost is vulnerable to Arbitrary File Write via Zip Import Feature (ZipSlip). In apps/server/src/integrations/import/utils/file.utils.ts, there are no validation on filename. This vulnerability is fixed in 0.24.0.	7.1	More Details
CVE-2025-24528	In MIT Kerberos 5 (aka krb5) before 1.22 (with incremental propagation), there is an integer overflow for a large update size to resize() in kdb_log.c. An authenticated attacker can cause an out-of-bounds write and kadmind daemon crash.	7.1	More Details
	A Use After Free vulnerability was identified in the 802.1X authentication daemon (dot1xd) of Juniper Networks Junos OS and Junos OS Evolved that could allow an authenticated, network-adjacent attacker flapping a port to crash the dot1xd		

CVE-2026-21908	process, leading to a Denial of Service (DoS), or potentially execute arbitrary code within the context of the process running as root. The issue is specific to the processing of a change in authorization (CoA) when a port bounce occurs. A pointer is freed but was then referenced later in the same code path. Successful exploitation is outside the attacker's direct control due to the specific timing of the two events required to execute the vulnerable code path. This issue affects systems with 802.1X authentication port-based network access control (PNAC) enabled. This issue affects: Junos OS: * from 23.2R2-S1 before 23.2R2-S5, * from 23.4R2 before 23.4R2-S6, * from 24.2 before 24.2R2-S3, * from 24.4 before 24.4R2-S1, * from 25.2 before 25.2R1-S2, 25.2R2; Junos OS Evolved: * from 23.2R2-S1 before 23.2R2-S5-EVO, * from 23.4R2 before 23.4R2-S6-EVO, * from 24.2 before 24.2R2-S3-EVO, * from 24.4 before 24.4R2-S1-EVO, * from 25.2 before 25.2R1-S2-EVO, 25.2R2-EVO.	7.1	More Details
CVE-2025-36911	In key-based pairing, there is a possible ID due to a logic error in the code. This could lead to remote (proximal/adjacent) information disclosure of user's conversations and location with no additional execution privileges needed. User interaction is not needed for exploitation.	7.1	More Details
CVE-2026-21986	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: This vulnerability applies to Windows VMs only. CVSS 3.1 Base Score 7.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H).	7.1	More Details
CVE-2025-64769	The Process Optimization application suite leverages connection channels/protocols that by-default are not encrypted and could become subject to hijacking or data leakage in certain man-in-the-middle or passive inspection scenarios.	7.1	More Details
CVE-2026-21976	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Oracle Analytics Cloud). Supported versions that are affected are 7.6.0.0.0 and 8.2.0.0.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Business Intelligence Enterprise Edition executes to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	7.1	More Details
CVE-2021-47766	Kmaleon 1.1.0.205 contains an authenticated SQL injection vulnerability in the 'tipocomb' parameter of kmaleonW.php that allows attackers to manipulate database queries. Attackers can exploit this vulnerability using boolean-based, error-based, and time-based blind SQL injection techniques to potentially extract or manipulate database information.	7.1	More Details
CVE-2026-21939	Vulnerability in the SQLcl component of Oracle Database Server. Supported versions that are affected are 23.4.0-23.26.0. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where SQLcl executes to compromise SQLcl. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of SQLcl. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).	7.0	More Details

CVE-2025-14435	Mattermost versions 10.11.x <= 10.11.8, 11.1.x <= 11.1.1, 11.0.x <= 11.0.6 fail to prevent infinite re-renders on API errors which allows authenticated users to cause application-level DoS via triggering unbounded component re-render loops.	6.8	More Details
CVE-2026-22718	The VSCode extension for Spring CLI are vulnerable to command injection, resulting in command execution on the users machine.	6.8	More Details
CVE-2025-11044	An Allocation of Resources Without Limits or Throttling vulnerability in the ANSL-Server component of B&R Automation Runtime versions prior to 6.5 and prior to R4.93 could be exploited by an unauthenti-cated attacker on the network to win a race condition, resulting in permanent denial-of-service (DoS) conditions on affected devices.	6.8	More Details
CVE-2025-13453	A potential vulnerability was reported in some ThinkPlus USB drives that could allow a user with physical access to read data stored on the drive.	6.8	More Details
CVE-2026-22637	The built-in XY Chart plugin is vulnerable to a DOM XSS vulnerability. A user with Editor permissions is able to modify such a panel in order to make it execute arbitrary JavaScript.	6.8	More Details
CVE-2026-23626	Kimai is a web-based multi-user time-tracking application. Prior to version 2.46.0, Kimai's export functionality uses a Twig sandbox with an overly permissive security policy (`DefaultPolicy`) that allows arbitrary method calls on objects available in the template context. An authenticated user with export permissions can deploy a malicious Twig template that extracts sensitive information including environment variables, all user password hashes, serialized session tokens, and CSRF tokens. Version 2.46.0 patches this issue.	6.8	More Details
CVE-2025-68969	Multi-thread race condition vulnerability in the thermal management module. Impact: Successful exploitation of this vulnerability may affect availability.	6.8	More Details
CVE-2025-33231	NVIDIA Nsight Systems for Windows contains a vulnerability in the application’s DLL loading mechanism where an attacker could cause an uncontrolled search path element by exploiting insecure DLL search paths. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service and information disclosure.	6.7	More Details
CVE-2025-24531	In OpenSC pam_pkcs11 before 0.6.13, pam_sm_authenticate() wrongly returns PAM_IGNORE in many error situations (such as an error triggered by a smartcard before login), allowing authentication bypass.	6.7	More Details
CVE-2026-23885	Alchemy is an open source content management system engine written in Ruby on Rails. Prior to versions 7.4.12 and 8.0.3, the application uses the Ruby `eval()` function to dynamically execute a string provided by the `resource_handler.engine_name` attribute in `Alchemy::ResourcesHelper#resource_url_proxy`. The vulnerability exists in `app/helpers/alchemy/resources_helper.rb` at line 28. The code explicitly bypasses security linting with `# rubocop:disable Security/Eval`, indicating that the use of a dangerous function was known but not properly mitigated. Since `engine_name` is sourced from module definitions that can be influenced by administrative configurations, it allows an authenticated attacker to escape the Ruby sandbox and execute arbitrary system commands on the host OS. Versions 7.4.12 and 8.0.3 fix the issue by replacing `eval()` with `send()`.	6.6	More Details
	Vulnerability in the Oracle Life Sciences Central Coding product of Oracle Health Sciences Applications (component: Platform). The supported version that is affected is 7.0.1.0. Easily exploitable vulnerability allows unauthenticated attacker with		

CVE-2026-21980	network access via HTTP to compromise Oracle Life Sciences Central Coding. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Life Sciences Central Coding accessible data as well as unauthorized read access to a subset of Oracle Life Sciences Central Coding accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	6.5	More Details
CVE-2026-23646	OpenProject is an open-source, web-based project management software. Users of OpenProject versions prior to 16.6.5 and 17.0.1 have the ability to view and end their active sessions via Account Settings → Sessions. When deleting a session, it was not properly checked if the session belongs to the user. As the ID that is used to identify these session objects use incremental integers, users could iterate requests using `DELETE /my/sessions/:id` and thus unauthenticate other users. Users did not have access to any sensitive information (like browser identifier, IP addresses, etc) of other users that are stored in the session. The problem was patched in OpenProject versions 16.6.5 and 17.0.1. No known workarounds are available as this does not require any permissions or other that can temporarily be disabled.	6.5	More Details
CVE-2026-21911	An Incorrect Calculation vulnerability in the Layer 2 Control Protocol Daemon (l2cpd) of Juniper Networks Junos OS Evolved allows an unauthenticated network-adjacent attacker flapping the management interface to cause the learning of new MACs over label-switched interfaces (LSI) to stop while generating a flood of logs, resulting in high CPU usage. When the issue is seen, the following log message will be generated: op:1 flag:0x6 mac:xx:xx:xx:xx:xx:xx bd:2 ifl:13302 reason:0(REASON_NONE) i-op:6(INTRNL_OP_HW_FORCE_DELETE) status:10 lstatus:10 err:26(GETIFBD_VALIDATE_FAILED) err-reason 4(IFBD_VALIDATE_FAIL_EPOCH_MISMATCH) hw_wr:0x4 ctxsync:0 fwdsync:0 rtt-id:51 p_ifl:0 fwd_nh:0 svlbnh:0 event:- smask:0x100000000 dmask:0x0 mplsmask 0x1 act:0x5800 extf:0x0 pfe-id 0 hw-notif-ifl 13302 programmed-ifl 4294967295 pseudo-vtep underlay-ifl-idx 0 stack:GET_MAC, ALLOCATE_MAC, GET_IFL, GET_IFF, GET_IFBD, STOP, This issue affects Junos OS Evolved: * all versions before 21.4R3-S7-EVO, * from 22.2 before 22.2R3-S4-EVO, * from 22.3 before 22.3R3-S3-EVO, * from 22.4 before 22.4R3-S2-EVO, * from 23.2 before 23.2R2-S1-EVO, * from 23.4 before 23.4R1-S2-EVO, 23.4R2-EVO.	6.5	More Details
CVE-2026-21910	An Improper Check for Unusual or Exceptional Conditions vulnerability in the packet forwarding engine (PFE) of Juniper Networks Junos OS on EX4k Series and QFX5k Series platforms allows an unauthenticated network-adjacent attacker flapping an interface to cause traffic between VXLAN Network Identifiers (VNIs) to drop, leading to a Denial of Service (DoS). On all EX4k and QFX5k platforms, a link flap in an EVPN-VXLAN configuration Link Aggregation Group (LAG) results in Inter-VNI traffic dropping when there are multiple load-balanced next-hop routes for the same destination. This issue is only applicable to systems that support EVPN-VXLAN Virtual Port-Link Aggregation Groups (VPLAG), such as the QFX5110, QFX5120, QFX5200, EX4100, EX4300, EX4400, and EX4650. Service can only be restored by restarting the affected FPC via the 'request chassis fpc restart slot <slot-number>' command. This issue affects Junos OS on EX4k and QFX5k Series: * all versions before 21.4R3-S12, * all versions of 22.2 * from 22.4 before 22.4R3-S8, * from 23.2 before 23.2R2-S5, * from 23.4 before 23.4R2-S5, * from 24.2 before 24.2R2-S3, * from 24.4 before 24.4R2.	6.5	More Details
CVE-2026-0203	An Improper Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS allows an unauthenticated, network-adjacent attacker sending a specifically malformed ICMP packet to cause an FPC to crash and restart, resulting in a Denial of Service (DoS). When an ICMP packet is received with a specifically malformed IP header value, the FPC receiving the packet crashes and restarts. Due to the specific type of malformed packet, adjacent upstream routers would not forward the packet, limiting the attack surface to adjacent networks. This issue only affects ICMPv4. ICMPv6 is not vulnerable to this issue. This issue affects	6.5	More Details

	Junos OS: * all versions before 21.2R3-S9, * from 21.4 before 21.4R3-S10, * from 22.2 before 22.2R3-S7, * from 22.3 before 22.3R3-S4, * from 22.4 before 22.4R3-S5, * from 23.2 before 23.2R2-S3, * from 23.4 before 23.4R2-S3, * from 24.2 before 24.2R1-S2, 24.2R2.		
CVE-2026-21909	A Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated attacker controlling an adjacent IS-IS neighbor to send a specific update packet causing a memory leak. Continued receipt and processing of these packets will exhaust all available memory, crashing rpd and creating a Denial of Service (DoS) condition. Memory usage can be monitored through the use of the 'show task memory detail' command. For example: user@junos> show task memory detail | match ted-infra TED-INFRA-COOKIE 25 1072 28 1184 229 user@junos> show task memory detail | match ted-infra TED-INFRA-COOKIE 31 1360 34 1472 307 This issue affects: Junos OS: * from 23.2 before 23.2R2, * from 23.4 before 23.4R1-S2, 23.4R2, * from 24.1 before 24.1R2; Junos OS Evolved: * from 23.2 before 23.2R2-EVO, * from 23.4 before 23.4R1-S2-EVO, 23.4R2-EVO, * from 24.1 before 24.1R2-EVO. This issue does not affect Junos OS versions before 23.2R1 or Junos OS Evolved versions before 23.2R1-EVO.	6.5	More Details
CVE-2026-21978	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Relationship Pricing). Supported versions that are affected are 14.0.0.0.0-14.8.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2026-21921	A Use After Free vulnerability in the chassis daemon (chassisd) of Juniper Networks Junos OS and Junos OS Evolved allows a network-based attacker authenticated with low privileges to cause a Denial-of-Service (DoS). When telemetry collectors are frequently subscribing and unsubscribing to sensors continuously over a long period of time, telemetry-capable processes like chassisd, rpd or mib2d will crash and restart, which - depending on the process - can cause a complete outage until the system has recovered. This issue affects: Junos OS: * all versions before 22.4R3-S8, * 23.2 versions before 23.2R2-S5, * 23.4 versions before 23.4R2; Junos OS Evolved: * all versions before 22.4R3-S8-EVO, * 23.2 versions before 23.2R2-S5-EVO, * 23.4 versions before 23.4R2-EVO.	6.5	More Details
CVE-2025-12573	The Bookingor WordPress plugin through 1.0.12 exposes authenticated AJAX actions without capability or nonce checks, allowing low-privileged users to delete Bookingor WordPress plugin through 1.0.12 data.	6.5	More Details
CVE-2026-23848	MyTube is a self-hosted downloader and player for several video websites. Prior to version 1.7.71, a rate limiting bypass via `X-Forwarded-For` header spoofing allows unauthenticated attackers to bypass IP-based rate limiting on general API endpoints. Attackers can spoof client IPs by manipulating the `X-Forwarded-For` header, enabling unlimited requests to protected endpoints, including general API endpoints (enabling DoS) and other rate-limited functionality. Version 1.7.71 contains a patch for the issue.	6.5	More Details
CVE-2026-21903	A Stack-based Buffer Overflow vulnerability in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS allows a network-based attacker, authenticated with low privileges to cause a Denial-of-Service (DoS). Subscribing to telemetry sensors at scale causes all FPC connections to drop, resulting in an FPC crash and restart. The issue was not seen when YANG packages for the specific sensors were installed. This issue affects Junos OS: * all versions before 22.4R3-S7, * 23.2 version before 23.2R2-S4, * 23.4 versions before 23.4R2.	6.5	More Details

CVE-2025-59355	A vulnerability. When org.apache.linkis.metadata.util.HiveUtils.decode() fails to perform Base64 decoding, it records the complete input parameter string in the log via logger.error(str + "decode failed", e). If the input parameter contains sensitive information such as Hive Metastore keys, plaintext passwords will be left in the log files when decoding fails, resulting in information leakage. Affected Scope Component: Sensitive fields in hive-site.xml (e.g., javax.jdo.option.ConnectionPassword) or other fields encoded in Base64. Version: Apache Linkis 1.0.0 – 1.7.0 Trigger Conditions The value of the configuration item is an invalid Base64 string. Log files are readable by users other than hive-site.xml administrators. Severity: Low The probability of Base64 decoding failure is low. The leakage is only triggered when logs at the Error level are exposed. Remediation Apache Linkis 1.8.0 and later versions have replaced the log with desensitized content. logger.error("URL decode failed: {}", e.getMessage()); // 不再输出 str Users are recommended to upgrade to version 1.8.0, which fixes the issue.	6.5	More Details
CVE-2025-68671	lakeFS is an open-source tool that transforms object storage into a Git-like repositories. LakeFS's S3 gateway does not validate timestamps in authenticated requests, allowing replay attacks. Prior to 1.75.0, an attacker who captures a valid signed request (e.g., through network interception, logs, or compromised systems) can replay that request until credentials are rotated, even after the request is intended to expire. This vulnerability is fixed in 1.75.0.	6.5	More Details
CVE-2025-13725	The Gutenberg Thim Blocks – Page Builder, Gutenberg Blocks for the Block Editor plugin for WordPress is vulnerable to arbitrary file reads in all versions up to, and including, 1.0.1. This is due to insufficient path validation in the server-side rendering of the thim-blocks/icon block. This makes it possible for authenticated attackers, with Contributor-level access and above, to read the contents of arbitrary files on the server via the 'iconSVG' parameter, which can contain sensitive information such as wp-config.php.	6.5	More Details
CVE-2026-0696	In ConnectWise PSA versions older than 2026.1, certain session cookies were not set with the HttpOnly attribute. In some scenarios, this could allow client-side scripts access to session cookie values.	6.5	More Details
CVE-2026-22770	ImageMagick is free and open-source software used for editing and manipulating digital images. The BilateralBlurImage method will allocate a set of double buffers inside AcquireBilateralTLS. But, in versions prior to 7.1.2-13, the last element in the set is not properly initialized. This will result in a release of an invalid pointer inside DestroyBilateralTLS when the memory allocation fails. Version 7.1.2-13 contains a patch for the issue.	6.5	More Details
CVE-2026-21944	Vulnerability in the Oracle Agile Product Lifecycle Management for Process product of Oracle Supply Chain (component: Product Quality Management). The supported version that is affected is 6.2.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile Product Lifecycle Management for Process. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Agile Product Lifecycle Management for Process accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2025-14242	A flaw was found in vsftpd. This vulnerability allows a denial of service (DoS) via an integer overflow in the ls command parameter parsing, triggered by a remote, authenticated attacker sending a crafted STAT command with a specific byte sequence.	6.5	More Details
CVE-	The Wallet System for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'change_wallet_fund_request_status_callback' function in all versions up to, and		More

2025-14450	including, 2.7.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to manipulate wallet withdrawal requests and arbitrarily increase their wallet balance or decrease other users' balances.	6.5	Details
CVE-2026-21949	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 9.0.0-9.5.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2026-21923	Vulnerability in the Oracle Life Sciences Central Designer product of Oracle Health Sciences Applications (component: Platform). The supported version that is affected is 7.0.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Life Sciences Central Designer. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Life Sciences Central Designer accessible data as well as unauthorized read access to a subset of Oracle Life Sciences Central Designer accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	6.5	More Details
CVE-2026-21950	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 9.0.0-9.5.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2026-0421	A potential vulnerability was reported in the BIOS of L13 Gen 6, L13 Gen 6 2-in-1, L14 Gen 6, and L16 Gen 2 ThinkPads which could result in Secure Boot being disabled even when configured as “On” in the BIOS setup menu. This issue only affects systems where Secure Boot is set to User Mode.	6.5	More Details
CVE-2025-12641	The Awesome Support - WordPress HelpDesk & Support Plugin for WordPress is vulnerable to authorization bypass due to missing capability checks in all versions up to, and including, 6.3.6. This is due to the 'wpas_do_mr_activate_user' function not verifying that a user has permission to modify other users' roles, combined with a nonce reuse vulnerability where public registration nonces are valid for privileged actions because all actions share the same nonce namespace. This makes it possible for unauthenticated attackers to demote administrators to low-privilege roles via the 'wpas-do=mr_activate_user' action with a user-controlled 'user_id' parameter, granted they can access the publicly available registration/submit ticket page to extract a valid nonce.	6.5	More Details
CVE-2025-70299	A heap overflow in the avi_parse_input_file() function of GPAC v2.4.0 allows attackers to cause a Denial of Service (DoS) via a crafted AVI file.	6.5	More Details
CVE-2025-37184	A vulnerability exists in an Orchestrator service that could allow an unauthenticated remote attacker to bypass multi-factor authentication requirements. Successful exploitation could allow an attacker to create an admin user account without the necessary multi-factor authentication, thereby compromising the integrity of secured access to the system.	6.5	More Details
	The MailerLite - WooCommerce integration plugin for WordPress is vulnerable to unauthorized data modification and deletion in all versions up to, and including, 3.1.3. This is due to missing capability checks on the resetIntegration() function. This		

CVE-2026-1000	makes it possible for authenticated attackers, with Subscriber-level access and above, to reset the plugin's integration settings, delete all plugin options, and drop the plugin's database tables (woo_mailerlite_carts and woo_mailerlite_jobs), resulting in complete loss of plugin data including customer abandoned cart information and sync job history.	6.5	More Details
CVE-2025-15020	The Gotham Block Extra Light plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 1.5.0 via the 'ghostban' shortcode. This makes it possible for authenticated attackers, with contributor-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	6.5	More Details
CVE-2026-23769	lucy-xss-filter before commit e5826c0 allows an attacker to execute malicious JavaScript due to improper sanitization caused by misconfigured default superset rule files.	6.5	More Details
CVE-2026-21960	Vulnerability in the Oracle Applications DBA product of Oracle E-Business Suite (component: Java utils). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Applications DBA. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications DBA accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications DBA accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).	6.5	More Details
CVE-2025-67835	Paessler PRTG Network Monitor before 25.4.114 allows Denial-of-Service (DoS) by an authenticated attacker via the Notification Contacts functionality.	6.5	More Details
CVE-2026-0949	PEM versions prior to 9.8.1 are affected by a stored Cross-site Scripting (XSS) vulnerability that allows users with access to the Manage Charts menu to inject arbitrary JavaScript when creating a new chart, which is then executed by any user accessing the chart. By default only the superuser and users with pem_admin or pem_super_admin privileges are able to access the Manage Charts menu.	6.5	More Details
CVE-2026-21968	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.44, 8.4.0-8.4.7 and 9.0.0-9.5.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2026-21970	Vulnerability in the Oracle Life Sciences Central Designer product of Oracle Health Sciences Applications (component: Platform). The supported version that is affected is 7.0.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Life Sciences Central Designer. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Life Sciences Central Designer accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2025-67084	File upload vulnerability in InvoicePlane through 1.6.3 allows authenticated attackers to upload arbitrary PHP files into attachments, which can later be executed remotely, leading to Remote Code Execution (RCE).	6.5	More Details
	An SQL injection vulnerability in InvoicePlane through 1.6.3 has been identified in		

CVE-2025-67082	"maxQuantity" and "minQuantity" parameters when generating a report. An authenticated attacker can exploit this issue via error-based SQL injection, allowing for the extraction of arbitrary data from the database. The vulnerability arises from insufficient sanitizing of single quotes.	6.5	More Details
CVE-2026-0529	Improper Validation of Array Index (CWE-129) in Packetbeat's MongoDB protocol parser can allow an attacker to cause Overflow Buffers (CAPEC-100) through specially crafted network traffic. This requires an attacker to send a malformed payload to a monitored network interface where MongoDB protocol parsing is enabled.	6.5	More Details
CVE-2026-23878	HotCRP is conference review software. Starting in commit aa20ef288828b04550950cf67c831af8a525f508 and prior to commit ceacd5f1476458792c44c6a993670f02c984b4a0, authors with at least one submission on a HotCRP site could use the document API to download any documents (PDFs, attachments) associated with any submission. The problem was patched in commit ceacd5f1476458792c44c6a993670f02c984b4a0.	6.5	More Details
CVE-2026-0916	The Related Posts by Taxonomy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'related_posts_by_tax' shortcode in all versions up to, and including, 2.7.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13859	The AffiliateX – Amazon Affiliate Plugin plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_customization_settings AJAX action in versions 1.0.0 to 1.3.9.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to store arbitrary JavaScript that executes whenever an AffiliateX block renders on the site.	6.4	More Details
CVE-2026-0690	The FlatPM – Ad Manager, AdSense and Custom Code plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'rank_math_description' custom field in all versions up to, and including, 3.2.2 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-2026-0694	The SearchWiz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via post titles in search results in all versions up to, and including, 1.0.0. This is due to the plugin using `esc_attr()` instead of `esc_html()` when outputting post titles in search results. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in post titles that will execute whenever a user performs a search and views the search results page.	6.4	More Details
CVE-2025-12178	The SpiceForms Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'spiceforms' shortcode 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-2021-47834	Schlix CMS 2.2.6-6 contains a persistent cross-site scripting vulnerability that allows authenticated users to inject malicious scripts into category titles. Attackers can create a new contact category with a script payload that will execute when the page is viewed by other users.	6.4	More Details
	The Team Section Block plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's block in all versions up to, and including, 2.0.0 due to		

CVE-2026-0833	insufficient input sanitization and output escaping on user-supplied social network link URLs. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-0913	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 plugin's 'usp_access' shortcode in all versions up to, and including, 20260110 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-2025-8615	The CubeWP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's cubewp_shortcode_taxonomy shortcode in all versions up to, and including, 1.1.26 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-2025-36408	IBM ApplinX 11.1 is vulnerable to stored cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.4	More Details
CVE-2026-23733	LobeChat is an open source chat application platform. Prior to version 2.0.0-next.180, a stored Cross-Site Scripting (XSS) vulnerability in the Mermaid artifact renderer allows attackers to execute arbitrary JavaScript within the application context. This XSS can be escalated to Remote Code Execution (RCE) by leveraging the exposed `electronAPI` IPC bridge, allowing attackers to run arbitrary system commands on the victim's machine. Version 2.0.0-next.180 patches the issue.	6.4	More Details
CVE-2026-23525	1Panel is an open-source, web-based control panel for Linux server management. A stored Cross-Site Scripting (XSS) vulnerability exists in the 1Panel App Store when viewing application details. Malicious scripts can execute in the context of the user's browser, potentially compromising session data or sensitive system interfaces. All versions of 1Panel up to and including v1.10.33-lts and v2.0.16 are affected. An attacker could publish a malicious application that, when loaded by users (locally or remotely), can execute arbitrary scripts. This may result in theft of user cookies, unauthorized access to system functions, or other actions that compromise the confidentiality, integrity, and availability of the system. The vulnerability is caused by insufficient sanitization of content rendered by the MdEditor component with the `previewOnly` attribute enabled. Specifically, the App Store renders application README content without proper XSS protection, allowing script execution during content rendering; and similar issues exist in system upgrade-related components, which can be fixed by implementing proper XSS sanitization in the MdEditor component. These vulnerabilities can be mitigated by applying proper XSS protection and sanitization when rendering content in the MdEditor component. Safe versions with a patch incorporated are v1.10.34-lts and v2.0.17.	6.4	More Details
CVE-2026-0608	The Head Meta Data plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'head-meta-data' post meta field in all versions up to, and including, 20251118 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
	A weakness has been identified in EyouCMS up to 1.7.1/5.0. Impacted is the function check_userinfo of the file Diyajax.php of the component Member Avatar Handler.		

CVE-2026-1107	Executing a manipulation of the argument viewfile can lead to unrestricted upload. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-1066	A vulnerability was detected in kalcaddle kodbox up to 1.61.10. This issue affects some unknown processing of the file /?explorer/index/zip of the component Compression Handler. The manipulation results in command injection. The attack may be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-1061	A vulnerability was detected in xiweicheng TMS up to 2.28.0. Affected by this issue is the function Upload of the file src/main/java/com/lhjz/portal/controller/FileController.java. The manipulation of the argument filename results in unrestricted upload. The attack may be performed from remote. The exploit is now public and may be used.	6.3	More Details
CVE-2026-1062	A flaw has been found in xiweicheng TMS up to 2.28.0. This affects the function Summary of the file src/main/java/com/lhjz/portal/util/HtmlUtil.java. This manipulation of the argument url causes server-side request forgery. It is possible to initiate the attack remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-1193	A vulnerability was identified in MineAdmin 1.x/2.x. The impacted element is an unknown function of the file /system/cache/view of the component View Interface. The manipulation leads to improper authorization. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-1118	A vulnerability was detected in itsourcecode Society Management System 1.0. Impacted is an unknown function of the file /admin/add_activity.php. Performing a manipulation of the argument Title results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-1126	A security vulnerability has been detected in lwj flow up to a3d2fe8133db9d3b50fda4f66f68634640344641. This affects the function uploadFile of the file \flow-master\flow-front-rest\src\main\java\com\dragon\flow\web\resource\flow\FormResource.java of the component SVG File Handler. The manipulation of the argument File leads to unrestricted upload. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2025-36115	IBM Sterling Connect:Express Adapter for Sterling B2B Integrator 5.2.0.00 through 5.2.0.12 does not disallow the session id after use which could allow an authenticated user to impersonate another user on the system.	6.3	More Details
CVE-2025-36063	IBM Sterling Connect:Express Adapter for Sterling B2B Integrator 5.2.0 5.2.0.00 through 5.2.0.12 does not invalidate session after a logout which could allow an authenticated user to impersonate another user on the system.	6.3	More Details
CVE-2026-1218	A vulnerability was detected in Bjskzy Zhiyou ERP up to 11.0. Impacted is the function initRCForm of the file RichClientService.class of the component com.artery.richclient.RichClientService. Performing a manipulation results in xml external entity reference. The attack is possible to be carried out remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE-2026-1141	A vulnerability was identified in PHPGurukul News Portal 1.0. The affected element is an unknown function of the file /admin/add-subadmins.php of the component Add Sub-Admin Page. Such manipulation leads to improper authorization. The attack can be launched remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-1144	A vulnerability was detected in quickjs-ng quickjs up to 0.11.0. Affected is an unknown function of the file quickjs.c of the component Atomics Ops Handler. The manipulation results in use after free. The attack can be executed remotely. The exploit is now public and may be used. The patch is identified as ea3e9d77454e8fc9cb3ef3c504e9c16af5a80141. Applying a patch is advised to resolve this issue.	6.3	More Details
CVE-2026-1145	A flaw has been found in quickjs-ng quickjs up to 0.11.0. Affected by this vulnerability is the function js_typed_array_constructor_ta of the file quickjs.c. This manipulation causes heap-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been published and may be used. Patch name: 53aebe66170d545bb6265906fe4324e4477de8b4. It is suggested to install a patch to address this issue.	6.3	More Details
CVE-2026-1150	A security flaw has been discovered in Totolink LR350 9.3.5u.6369_B20220309. Impacted is the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. The manipulation of the argument command results in command injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-1149	A vulnerability was identified in Totolink LR350 9.3.5u.6369_B20220309. This issue affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. The manipulation of the argument ip leads to command injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-36065	IBM Sterling Connect:Express Adapter for Sterling B2B Integrator 5.2.0 5.2.0.00 through 5.2.0.12 does not invalidate session after a browser closure which could allow an authenticated user to impersonate another user on the system.	6.3	More Details
CVE-2021-47765	AbsoluteTelnet 11.24 contains a denial of service vulnerability that allows local attackers to crash the application by manipulating username and error report fields. Attackers can trigger the crash by inserting 1000 characters into the username or email address fields, causing the application to become unresponsive.	6.2	More Details
CVE-2025-68959	Permission verification bypass vulnerability in the media library module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.2	More Details
CVE-2025-68964	Data verification vulnerability in the HiView module. Impact: Successful exploitation of this vulnerability may affect availability.	6.2	More Details
CVE-2021-47759	MTPutty 1.0.1.21 contains a sensitive information disclosure vulnerability that allows local attackers to view SSH connection passwords through Windows PowerShell process listing. Attackers can run a PowerShell command to retrieve the full command line of MTPutty processes, exposing plaintext SSH credentials.	6.2	More Details
CVE-2021-47764	AbsoluteTelnet 11.24 contains a denial of service vulnerability that allows local attackers to crash the application by manipulating DialUp connection and license name fields. Attackers can generate a 1000-character payload and paste it into specific input fields to trigger application crashes and force unexpected termination.	6.2	More Details
CVE-2021-	RDP Manager 4.9.9.3 contains a denial of service vulnerability in connection input fields that allows local attackers to crash the application. Attackers can add	6.2	More

47771	oversized entries in Verbindungsname and Server fields to permanently freeze and crash the software, potentially requiring full reinstallation.		Details
CVE-2021-47799	Visual Tools DVR VX16 version 4.2.28 contains a local privilege escalation vulnerability in its Sudo configuration that allows attackers to gain root access. Attackers can exploit the unsafe Sudo settings by using mount commands to bind a shell, enabling unauthorized system-level privileges.	6.2	More Details
CVE-2021-47795	GeoVision GeoWebServer 5.3.3 contains multiple vulnerabilities including local file inclusion, cross-site scripting, and remote code execution through improper input sanitization. Attackers can exploit the WebStrings.srf endpoint by manipulating path traversal and injection parameters to access system files and execute malicious scripts.	6.2	More Details
CVE-2025-56451	Cross site scripting vulnerability in seeyon Zhiyuan A8+ Collaborative Management Software 7.0 via the topValue parameter to the seeyon/main.do endpoint.	6.1	More Details
CVE-2025-14375	The RSS Aggregator – RSS Import, News Feeds, Feed to Post, and Autoblogging plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘className’ parameter in all versions up to, and including, 5.0.10 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-0858	Versions of the package net.sourceforge.plantuml:plantuml before 1.2026.0 are vulnerable to Stored XSS due to insufficient sanitization of interactive attributes in GraphViz diagrams. As a result, a crafted PlantUML diagram can inject malicious JavaScript into generated SVG output, leading to arbitrary script execution in the context of applications that render the SVG.	6.1	More Details
CVE-2021-47836	Markdown Explorer 0.1.1 contains a cross-site scripting vulnerability that allows attackers to inject malicious code through file uploads and editor inputs. Attackers can upload markdown files with embedded JavaScript payloads to execute remote commands and potentially gain system access.	6.1	More Details
CVE-2021-47841	SnipCommand 0.1.0 contains a cross-site scripting vulnerability that allows attackers to inject malicious payloads into command snippets. Attackers can execute arbitrary code by embedding malicious JavaScript that triggers remote command execution through file or title inputs.	6.1	More Details
CVE-2026-23768	lucy-xss-filter before commit 7c1de6d allows an attacker to induce server-side HEAD requests to arbitrary URLs when the ObjectSecurityListener or EmbedSecurityListener option is enabled and embed or object tags are used with a src attribute missing a file extension.	6.1	More Details
CVE-2021-47844	Xmind 2020 contains a cross-site scripting vulnerability that allows attackers to inject malicious payloads into mind mapping files or custom headers. Attackers can craft malicious files with embedded JavaScript that execute system commands when opened, enabling remote code execution through mouse interactions or file opening.	6.1	More Details
CVE-2026-0594	The List Site Contributors plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'alpha' parameter in versions up to, and including, 1.1.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-	A reflected cross-site scripting (xss) vulnerability exists in the modifyHL7Route functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious	6.1	More

53854	URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.		Details
CVE-2025-66523	URL parameters are directly embedded into JavaScript code or HTML attributes without proper encoding or sanitization. This allows attackers to inject arbitrary scripts when an authenticated user visits a crafted link. This issue affects na1.foxitesign.foxit.com: before 2026-01-16.	6.1	More Details
CVE-2025-65368	SparkyFitness v0.15.8.2 is vulnerable to Cross Site Scripting (XSS) via user input and LLM output.	6.1	More Details
CVE-2025-54861	A reflected cross-site scripting (xss) vulnerability exists in the modifyCoercion functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-55071	A reflected cross-site scripting (xss) vulnerability exists in the modifyAnonymize functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-57786	A reflected cross-site scripting (xss) vulnerability exists in the notifynewstudy functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-57787	A reflected cross-site scripting (xss) vulnerability exists in the modifyRoute functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-57881	A reflected cross-site scripting (xss) vulnerability exists in the modifyEmail functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-58080	A reflected cross-site scripting (xss) vulnerability exists in the modifyHL7App functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-58087	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the status parameter.	6.1	More Details
CVE-2025-58088	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the archivedir parameter.	6.1	More Details
CVE-2025-58089	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the longtermdir parameter.	6.1	More Details
	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php		

CVE-2025-58090	functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the uploaddir parameter.	6.1	More Details
CVE-2025-58091	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the thumbnaildir parameter.	6.1	More Details
CVE-2025-58092	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the phpexe parameter.	6.1	More Details
CVE-2025-70891	A stored cross-site scripting (XSS) vulnerability exists in Phpgurukul Cyber Cafe Management System v1.0 within the user management module. The application does not properly sanitize or encode user-supplied input submitted via the uadd parameter in the add-users.php endpoint. An authenticated attacker can inject arbitrary JavaScript code that is persistently stored in the database. The malicious payload is triggered when a privileged user clicks the View button on the view-allusers.php page.	6.1	More Details
CVE-2025-67025	Cross Site Scripting vulnerability in Anycomment anycomment.io 0.4.4 allows a remote attacker to execute arbitrary code via the Anycomment comment section	6.1	More Details
CVE-2025-52987	A clickjacking vulnerability exists in the web portal of Juniper Networks Paragon Automation (Pathfinder, Planner, Insights) due to the application's failure to set appropriate X-Frame-Options and X-Content-Type HTTP headers. This vulnerability allows an attacker to trick users into interacting with the interface under the attacker's control. This issue affects all versions of Paragon Automation (Pathfinder, Planner, Insights) before 24.1.1.	6.1	More Details
CVE-2025-54852	A reflected cross-site scripting (xss) vulnerability exists in the modifyAeTitle functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-58093	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the phpdir parameter.	6.1	More Details
CVE-2025-58094	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the worklistsrc parameter.	6.1	More Details
CVE-2025-58095	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the imagedir parameter.	6.1	More Details

CVE-2025-36066	IBM Sterling Connect:Express Adapter for Sterling B2B Integrator 5.2.0 5.2.0.00 through 5.2.0.12 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.1	More Details
CVE-2025-67263	Abacre Retail Point of Sale 14.0.0.396 is affected by a stored cross-site scripting (XSS) vulnerability in the Clients module. The application fails to properly sanitize user-supplied input stored in the Name and Surname fields. An attacker can insert malicious HTML or script content into these fields, which, persisted in the database.	6.1	More Details
CVE-2026-21933	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17 and 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2026-21938	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.60, 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2026-21943	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: Scripting Admin). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Scripting, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Scripting accessible data as well as unauthorized read access to a subset of Oracle Scripting accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards		

CVE-2026-21946	(component: Web Runtime SEC). Supported versions that are affected are 9.2.0.0-9.2.26.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2021-47768	ImportExportTools NG 10.0.4 contains a persistent HTML injection vulnerability in the email export module that allows remote attackers to inject malicious HTML payloads. Attackers can send emails with crafted HTML in the subject that execute during HTML export, potentially compromising user data or session credentials.	6.1	More Details
CVE-2026-21951	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Integration Broker). Supported versions that are affected are 8.60, 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2025-68970	Permission verification bypass vulnerability in the media library module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.1	More Details
CVE-2026-21961	Vulnerability in the PeopleSoft Enterprise HCM Human Resources product of Oracle PeopleSoft (component: Company Dir / Org Chart Viewer, Employee Snapshot). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Human Resources. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM Human Resources, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Human Resources accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Human Resources accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2026-21966	Vulnerability in the Oracle Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). Supported versions that are affected are 5.6.19.23, 5.6.25.17, 5.6.26.10 and 5.6.27.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality OPERA 5 Property Services, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality OPERA 5 Property Services accessible data as well as unauthorized read access to a subset of Oracle Hospitality OPERA 5 Property Services accessible data. CVSS 3.1	6.1	More Details

	Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).		
CVE-2025-54853	A reflected cross-site scripting (xss) vulnerability exists in the modifyUser functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-70890	A stored cross-site scripting (XSS) vulnerability exists in Cyber Cafe Management System v1.0. An authenticated attacker can inject arbitrary JavaScript code into the username parameter via the add-users.php endpoint. The injected payload is stored and executed in the victim s browser when the affected page is accessed.	6.1	More Details
CVE-2025-46270	A reflected cross-site scripting (xss) vulnerability exists in the fetchPriorStudies functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-54157	A reflected cross-site scripting (xss) vulnerability exists in the encapsulatedDoc functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-36556	A reflected cross-site scripting (xss) vulnerability exists in the ldapUser functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-44000	A reflected cross-site scripting (xss) vulnerability exists in the sendOruReport functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-65396	A vulnerability in the boot process of Blurams Flare Camera version 24.1114.151.929 and earlier allows a physically proximate attacker to hijack the boot mechanism and gain a bootloader shell via the UART interface. This is achieved by inducing a read error from the SPI flash memory during the boot, by shorting a data pin of the IC to ground. An attacker can then dump the entire firmware, leading to the disclosure of sensitive information including cryptographic keys and user configurations.	6.1	More Details
CVE-2025-67833	Paessler PRTG Network Monitor before 25.4.114 allows XSS by an unauthenticated attacker via the tag parameter.	6.1	More Details
CVE-2025-53516	A reflected cross-site scripting (xss) vulnerability exists in the downloadZip functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious url can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2026-22694	AliasVault is a privacy-first password manager with built-in email aliasing. AliasVault Android versions 0.24.0 through 0.25.2 contained an issue in how passkey requests from Android apps were validated. Under certain local conditions, a malicious app could attempt to obtain a passkey response for a site it was not authorized to access. The issue involved incomplete validation of calling app identity, origin, and RP ID in the Android credential provider. This issue was fixed in AliasVault Android 0.25.3.	6.1	More Details
CVE-2025-	A reflected cross-site scripting (xss) vulnerability exists in the modifyTranscript functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious	6.1	More

53707	URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.		Details
CVE-2025-54495	A reflected cross-site scripting (xss) vulnerability exists in the emailfailedjob functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious url can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-63644	A stored cross-site scripting (XSS) vulnerability exists in pH7Software pH7-Social-Dating-CMS 17.9.1 in the user profile Description field.	6.1	More Details
CVE-2025-54817	A reflected cross-site scripting (xss) vulnerability exists in the autoPurge functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious url can lead to arbitrary javascript code execution. An attacker can provide a URL to a malicious website to trigger this vulnerability.	6.1	More Details
CVE-2025-54814	A reflected cross-site scripting (xss) vulnerability exists in the modifyAutopurgeFilter functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-54778	A reflected cross-site scripting (xss) vulnerability exists in the existingUser functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2026-1011	A stored cross-site scripting (XSS) vulnerability exists in the Altium Support Center AddComment endpoint due to missing server-side input sanitization. Although the client interface applies HTML escaping, the backend accepts and stores arbitrary HTML and JavaScript supplied via modified POST requests. The injected content is rendered verbatim when support cases are viewed by other users, including support staff with elevated privileges, allowing execution of arbitrary JavaScript in the victim’s browser context.	6.1	More Details
CVE-2026-21985	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2026-21963	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2025-12002	The Feeds for YouTube Pro plugin for WordPress is vulnerable to arbitrary file read in all versions up to, and including, 2.6.0 via the 'sby_check_wp_submit' AJAX action. This is due to insufficient sanitization of user-supplied data and the use of that data in a file operation. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information,	5.9	More Details

	granted the 'Save Featured Images' setting is enabled and 'Disable WP Posts' is disabled. Note: This vulnerability only affects the Pro version of Feeds for YouTube.		
CVE-2026-22819	Outray openSource ngrok alternative. Prior to 0.1.5, this vulnerability allows a user i.e a free plan user to get more than the desired subdomains due to lack of db transaction lock mechanisms in main/apps/web/src/routes/api/$orgSlug/subdomains/index.ts. This vulnerability is fixed in 0.1.5.	5.9	More Details
CVE-2026-22851	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, a race condition between the RDPGFX dynamic virtual channel thread and the SDL render thread leads to a heap use-after-free. Specifically, an escaped pointer to sdl->primary (SDL_Surface) is accessed after it has been freed during RDPGFX ResetGraphics handling. This vulnerability is fixed in 3.20.1.	5.9	More Details
CVE-2025-1719	IBM Concert 1.0.0 through 2.1.0 could allow a remote attacker to obtain sensitive information from allocated memory due to improper clearing of heap memory.	5.9	More Details
CVE-2026-0990	A flaw was found in libxml2, an XML parsing library. This uncontrolled recursion vulnerability occurs in the xmlCatalogXMLResolveURI function when an XML catalog contains a delegate URI entry that references itself. A remote attacker could exploit this configuration-dependent issue by providing a specially crafted XML catalog, leading to infinite recursion and call stack exhaustion. This ultimately results in a segmentation fault, causing a Denial of Service (DoS) by crashing affected applications.	5.9	More Details
CVE-2026-21907	A Use of a Broken or Risky Cryptographic Algorithm vulnerability in the TLS/SSL server of Juniper Networks Junos Space allows the use of static key ciphers (ssl-static-key-ciphers), reducing the confidentiality of on-path traffic communicated across the connection. These ciphers also do not support Perfect Forward Secrecy (PFS), affecting the long-term confidentiality of encrypted communications.This issue affects all versions of Junos Space before 24.1R5.	5.9	More Details
CVE-2025-1722	IBM Concert 1.0.0 through 2.1.0 could allow a remote attacker to obtain sensitive information from allocated memory due to improper clearing of heap memory.	5.9	More Details
CVE-2026-22045	Traefik is an HTTP reverse proxy and load balancer. Prior to 2.11.35 and 3.6.7, there is a potential vulnerability in Traefik ACME TLS certificates' automatic generation: the ACME TLS-ALPN fast path can allow unauthenticated clients to tie up go routines and file descriptors indefinitely when the ACME TLS challenge is enabled. A malicious client can open many connections, send a minimal ClientHello with acme-tls/1, then stop responding, leading to denial of service of the entry point. The vulnerability is fixed in 2.11.35 and 3.6.7.	5.9	More Details
CVE-2026-21935	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Driver). The supported version that is affected is 11. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Solaris accessible data as well as unauthorized access to critical data or complete access to all Oracle Solaris accessible data. CVSS 3.1 Base Score 5.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N).	5.8	More Details
CVE-	A flaw was identified in Keycloak’s OpenID Connect Dynamic Client Registration feature when clients authenticate using private_key_jwt. The issue allows a client to specify an arbitrary jwks_uri, which Keycloak then retrieves without validating the		

2026-1180	destination. This enables attackers to coerce the Keycloak server into making HTTP requests to internal or restricted network resources. As a result, attackers can probe internal services and cloud metadata endpoints, creating an information disclosure and reconnaissance risk.	5.8	More Details
CVE-2025-12718	The Quick Contact Form plugin for WordPress is vulnerable to Open Mail Relay in all versions up to, and including, 8.2.6. This is due to the 'qcf_validate_form' AJAX endpoint allowing a user controlled parameter to set the 'from' email address. This makes it possible for unauthenticated attackers to send emails to arbitrary recipients utilizing the server. The information is limited to the contact form submission details.	5.8	More Details
CVE-2026-21927	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Driver). The supported version that is affected is 11. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Solaris accessible data as well as unauthorized access to critical data or complete access to all Oracle Solaris accessible data. CVSS 3.1 Base Score 5.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N).	5.8	More Details
CVE-2026-23845	Mailpit is an email testing tool and API for developers. Versions prior to 1.28.3 are vulnerable to Server-Side Request Forgery (SSRF) via HTML Check CSS Download. The HTML Check feature (`/api/v1/message/{ID}/html-check`) is designed to analyze HTML emails for compatibility. During this process, the `inlineRemoteCSS()` function automatically downloads CSS files from external `<link rel="stylesheet" href="...">` tags to inline them for testing. Version 1.28.3 fixes the issue.	5.8	More Details
CVE-2025-60011	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause an availability impact for downstream devices. When an affected device receives a specific optional, transitive BGP attribute over an existing BGP session, it will be erroneously modified before propagation to peers. When the attribute is detected as malformed by the peers, these peers will most likely terminate the BGP sessions with the affected devices and thereby cause an availability impact due to the resulting routing churn. This issue affects: Junos OS: * all versions before 22.4R3-S8, * 23.2 versions before 23.2R2-S5 * 23.4 versions before 23.4R2-S6, * 24.2 versions before 24.2R2-S2, * 24.4 versions before 24.4R2; Junos OS Evolved: * all versions before 22.4R3-S8-EVO, * 23.2 versions before 23.2R2-S5-EVO, * 23.4 versions before 23.4R2-S6-EVO, * 24.2 versions before 24.2R2-S2-EVO, * 24.4 versions before 24.4R2-EVO.	5.8	More Details
CVE-2025-68967	Vulnerability of improper permission control in the print module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.7	More Details
CVE-2025-68963	Man-in-the-middle attack vulnerability in the Clone module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.7	More Details
CVE-2026-1203	A weakness has been identified in CRMEB up to 5.6.3. The impacted element is the function remoteRegister of the file crmeb/app/services/user/LoginServices.php of the component JSON Token Handler. Executing a manipulation of the argument uid can lead to improper authentication. The attack may be performed from remote. The attack requires a high level of complexity. The exploitability is regarded as 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	5.6	More Details

	way.		
CVE-2025-14369	dr_flac, an audio decoder within the dr_libs toolset, contains an integer overflow vulnerability flaw due to trusting the totalPCMFrameCount field from FLAC metadata before calculating buffer size, allowing an attacker with a specially crafted file to perform DoS against programs using the tool.	5.5	More Details
CVE-2025-41768	On an instance of TwinCAT 3 HMI Server running on a device an authenticated administrator can inject arbitrary content into the custom CSS field which is persisted on the device and later returned via the login page and error page.	5.5	More Details
CVE-2025-70310	A heap overflow in the vorbis_to_intern() function of GPAC v2.4.0 allows attackers to cause a Denial of Service (DoS) via a crafted .ogg file.	5.5	More Details
CVE-2026-23874	ImageMagick is free and open-source software used for editing and manipulating digital images. Versions prior to 7.1.2-13 have a stack overflow via infinite recursion in MSL (Magick Scripting Language) `<write>` command when writing to MSL format. Version 7.1.2-13 fixes the issue.	5.5	More Details
CVE-2026-22640	An access control vulnerability was discovered in Grafana OSS where an Organization administrator could permanently delete the Server administrator account. This vulnerability exists in the DELETE /api/org/users/ endpoint. The vulnerability can be exploited when: 1. An Organization administrator exists 2. The Server administrator is either: - Not part of any organization, or - Part of the same organization as the Organization administrator Impact: - Organization administrators can permanently delete Server administrator accounts - If the only Server administrator is deleted, the Grafana instance becomes unmanageable - No super-user permissions remain in the system - Affects all users, organizations, and teams managed in the instance The vulnerability is particularly serious as it can lead to a complete loss of administrative control over the Grafana instance.	5.5	More Details
CVE-2025-70305	A stack overflow in the dmx_saf function of GPAC v2.4.0 allows attackers to cause a Denial of Service (DoS) via a crafted .saf file.	5.5	More Details
CVE-2025-70309	A stack overflow in the pcmreframe_flush_packet function of GPAC v2.4.0 allows attackers to cause a Denial of Service (DoS) via a crafted WAV file.	5.5	More Details
CVE-2025-69581	An issue was discovered in Chamillo LMS 1.11.2. The Social Network /personal_data endpoint exposes full sensitive user information even after logout because proper cache-control is missing. Using the browser back button restores all personal data, allowing unauthorized users on the same device to view confidential information. This leads to profiling, impersonation, targeted attacks, and significant privacy risks.	5.5	More Details
CVE-2025-43508	A logging issue was addressed with improved data redaction. This issue is fixed in macOS Tahoe 26.1. An app may be able to access sensitive user data.	5.5	More Details
CVE-2026-21912	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the method to collect FPC Ethernet firmware statistics of Juniper Networks Junos OS on MX10k Series allows a local, low-privileged attacker executing the 'show system firmware' CLI command to cause an LC480 or LC2101 line card to reset. On MX10k Series systems with LC480 or LC2101 line cards, repeated execution of the 'show system firmware' CLI command can cause the line card to crash and restart. Additionally, some time after the line card crashes, chassisd may also crash and restart, generating a core dump.This issue affects Junos OS on MX10k Series: * all versions before 21.2R3-S10, * from 21.4 before 21.4R3-S9, * from 22.2 before 22.2R3-S7, * from 22.4 before 22.4R3-S6, * from 23.2 before 23.2R2-S2, * from 23.4 before	5.5	More Details

	23.4R2-S3, * from 24.2 before 24.2R2.		
CVE-2026-0961	BLF file parser crash in Wireshark 4.6.0 to 4.6.2 and 4.4.0 to 4.4.12 allows denial of service	5.5	More Details
CVE-2025-37185	Vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attacks against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface and thereby make unauthorized arbitrary configuration changes to the host.	5.5	More Details
CVE-2025-60007	A NULL Pointer Dereference vulnerability in the chassis daemon (chassisd) of Juniper Networks Junos OS on MX, SRX and EX Series allows a local attacker with low privileges to cause a Denial-of-Service (DoS). When a user executes the 'show chassis' command with specifically crafted options, chassisd will crash and restart. Due to this all components but the Routing Engine (RE) in the chassis are reinitialized, which leads to a complete service outage, which the system automatically recovers from. This issue affects: Junos OS on MX, SRX and EX Series: * all versions before 22.4R3-S8, * 23.2 versions before 23.2R2-S5, * 23.4 versions before 23.4R2-S6, * 24.2 versions before 24.2R2-S2, * 24.4 versions before 24.4R2.	5.5	More Details
CVE-2025-70302	A heap overflow in the ghi_dmx_declare_opid_bin() function of GPAC v2.4.0 allows attackers to cause a Denial of Service (DoS) via a crafted input.	5.5	More Details
CVE-2025-70303	A heap overflow in the uncv_parse_config() function of GPAC v2.4.0 allows attackers to cause a Denial of Service (DoS) via a crafted MP4 file.	5.5	More Details
CVE-2025-13154	An improper link following vulnerability was reported in the SmartPerformanceAddin for Lenovo Vantage that could allow an authenticated local user to perform an arbitrary file deletion with elevated privileges.	5.5	More Details
CVE-2025-36058	IBM Business Automation Workflow containers 25.0.0 through 25.0.0 Interim Fix 002, 24.0.1 through 24.0.1 Interim Fix 005, and 24.0.0 through 24.0.0 Interim Fix 006. IBM Cloud Pak for Business Automation and IBM Business Automation Workflow containers may disclose sensitve configuration information in a config map.	5.5	More Details
CVE-2025-59961	An Incorrect Permission Assignment for Critical Resource vulnerability in the Juniper DHCP daemon (jdhcpd) of Juniper Networks Junos OS and Junos OS Evolved allows a local, low-privileged user to write to the Unix socket used to manage the jdhcpd process, resulting in complete control over the resource. This vulnerability allows any low-privileged user logged into the system to connect to the Unix socket and issue commands to manage the DHCP service, in essence, taking administrative control of the local DHCP server or DHCP relay. This issue affects: Junos OS: * all versions before 21.2R3-S10, * all versions of 22.2, * from 21.4 before 21.4R3-S12, * from 22.4 before 22.4R3-S8, * from 23.2 before 23.2R2-S5, * from 23.4 before 23.4R2-S6, * from 24.2 before 24.2R2-S2, * from 24.4 before 24.4R2, * from 25.2 before 25.2R1-S1, 25.2R2; Junos OS Evolved: * all versions before 22.4R3-S8-EVO, * from 23.2 before 23.2R2-S5-EVO, * from 23.4 before 23.4R2-S6-EVO, * from 24.2 before 24.2R2-S2-EVO, * from 24.4 before 24.4R2-EVO, * from 25.2 before 25.2R1-S1-EVO, 25.2R2-EVO.	5.5	More Details
CVE-	An Untrusted Pointer Dereference vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a local, authenticated attacker with low privileges to cause a Denial-of-Service (DoS). When the command 'show route < (receive-protocol | advertising-protocol) bgp > detail' is executed, and at least one of the routes in the intended output has specific attributes, this will		

2025-59959	cause an rpd crash and restart. 'show route ... extensive' is not affected. This issue affects: Junos OS: * all versions before 22.4R3-S8, * 23.2 versions before 23.2R2-S5, * 23.4 versions before 23.4R2-S5, * 24.2 versions before 24.2R2-S2, * 24.4 versions before 24.4R2; Junos OS Evolved: * all versions before 22.4R3-S8-EVO, * 23.2 versions before 23.2R2-S5-EVO, * 23.4 versions before 23.4R2-S6-EVO, * 24.2 versions before 24.2R2-S2-EVO, * 24.4 versions before 24.4R2-EVO.	5.5	More Details
CVE-2026-21924	Vulnerability in the Oracle Utilities Application Framework product of Oracle Utilities Applications (component: General). Supported versions that are affected are 4.4.0.3.0, 4.5.0.0.0, 4.5.0.1.1, 4.5.0.1.3, 4.5.0.2.0, 25.4 and 25.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Utilities Application Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Utilities Application Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Utilities Application Framework accessible data as well as unauthorized read access to a subset of Oracle Utilities Application Framework accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2026-0901	Inappropriate implementation in Blink in Google Chrome on Android prior to 144.0.7559.59 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: High)	5.4	More Details
CVE-2026-0904	Incorrect security UI in Digital Credentials in Google Chrome prior to 144.0.7559.59 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Medium)	5.4	More Details
CVE-2026-21971	Vulnerability in the PeopleSoft Enterprise SCM Purchasing product of Oracle PeopleSoft (component: Purchasing). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM Purchasing. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise SCM Purchasing accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise SCM Purchasing accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2026-0903	Inappropriate implementation in Downloads in Google Chrome on Windows prior to 144.0.7559.59 allowed a remote attacker to bypass dangerous file type protections via a malicious file. (Chromium security severity: Medium)	5.4	More Details
CVE-2026-0548	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to unauthorized attachment deletion due to a missing capability check on the `delete_existing_user_photo` function in all versions up to, and including, 3.9.4. This makes it possible for authenticated attackers, with subscriber level access and above, to delete arbitrary attachments on the site.	5.4	More Details
CVE-2025-15466	The Image Photo Gallery Final Tiles Grid plugin for WordPress is vulnerable to unauthorized access and modification of data due to missing capability checks on multiple AJAX actions in all versions up to, and including, 3.6.9. This makes it possible for authenticated attackers, with Contributor-level access and above, to view, create, modify, clone, delete, and reassign ownership of galleries created by other users, including administrators.	5.4	More Details
CVE-2026-23643	CakePHP is a rapid development framework for PHP. The PaginatorHelper::limitControl() method has a cross-site-scripting vulnerability via query string parameter manipulation. This issue has been fixed in 5.2.12 and 5.3.1.	5.4	More Details

CVE-2026-1106	A security flaw has been discovered in Chamilo LMS up to 2.0.0 Beta 1. This issue affects the function deleteLegal of the file src/CoreBundle/Controller/SocialController.php of the component Legal Consent Handler. Performing a manipulation of the argument userId results in improper authorization. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2025-14854	The WP-CRM System plugin for WordPress is vulnerable to unauthorized access due to missing capability checks on the wpcrm_get_email_recipients and wpcrm_system_ajax_task_change_status AJAX functions in all versions up to, and including, 3.4.5. This makes it possible for authenticated attackers, with subscriber level access and above, to enumerate CRM contact email addresses (PII disclosure) and modify CRM task statuses.	5.4	More Details
CVE-2025-36396	IBM Application Gateway 23.10 through 25.09 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details
CVE-2026-21934	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Push Notifications). Supported versions that are affected are 8.60, 8.61 and 8.62. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2025-15043	The The Events Calendar plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the 'start_migration', 'cancel_migration', and 'revert_migration' functions in all versions up to, and including, 6.15.13. This makes it possible for authenticated attackers, with subscriber level access and above, to start, cancel, or revert the Custom Tables V1 database migration, including dropping the custom database tables entirely via the revert action.	5.4	More Details
CVE-2026-21931	Vulnerability in the Oracle APEX Sample Applications product of Oracle APEX (component: Brookstrut Sample App). Supported versions that are affected are 23.2.0, 23.2.1, 24.1.0, 24.2.0 and 24.2.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle APEX Sample Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle APEX Sample Applications, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle APEX Sample Applications accessible data as well as unauthorized read access to a subset of Oracle APEX Sample Applications accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2025-36397	IBM Application Gateway 23.10 through 25.09 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site.	5.4	More Details
CVE-2025-36409	IBM ApplinX 11.1 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details

CVE-2025-36113	IBM Sterling Connect:Express Adapter for Sterling B2B Integrator 5.2.0 5.2.0.00 through 5.2.0.12 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details
CVE-2026-1112	A vulnerability was found in Sanluan PublicCMS up to 5.202506.d. Affected is the function delete of the file publiccms-trade/src/main/java/com/publiccms/controller/web/trade/TradeAddressController.java of the component Trade Address Deletion Endpoint. Performing a manipulation of the argument ids results in improper authorization. The attack may be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2021-47783	Phpwcms 1.9.30 contains a file upload vulnerability that allows authenticated attackers to upload malicious SVG files with embedded JavaScript. Attackers can upload crafted SVG payloads through the multiple file upload feature to potentially execute cross-site scripting attacks on the platform.	5.4	More Details
CVE-2026-23497	Frappe Learning Management System (LMS) is a learning system that helps users structure their content. In 2.44.0 and earlier, there is a stored XSS vulnerability where a specially crafted image filename could execute malicious JavaScript when rendered on course or jobs pages.	5.4	More Details
CVE-2026-23496	Pimcore Web2Print Tools Bundle adds tools for web-to-print use cases to Pimcore. Prior to 5.2.2 and 6.1.1, the application fails to enforce proper server-side authorization checks on the API endpoint responsible for managing "Favourite Output Channel Configurations." Testing revealed that an authenticated backend user without explicitely lacking permissions for this feature was still able to successfully invoke the endpoint and modify or retrieve these configurations. This vulnerability is fixed in 5.2.2 and 6.1.1.	5.4	More Details
CVE-2025-65349	A Stored Cross-Site Scripting (XSS) vulnerability in Web management interface in Each Italy Wireless Mini Router WIRELESS-N 300M v28K.MiniRouter.20190211 allows attackers to execute arbitrary scripts via a crafted payload due to unsanitized repeater AP SSID value when is displayed in any page at /index.htm.	5.4	More Details
CVE-2025-67834	Paessler PRTG Network Monitor before 25.4.114 allows XSS by an unauthenticated attacker via the filter parameter.	5.4	More Details
CVE-2025-14448	The WP-Members Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Multiple Checkbox and Multiple Select user profile fields in all versions up to, and including, 3.5.4.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2025-14173	The Perfit WooCommerce plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.0.1. This is due to missing authorization checks on the `logout` function called via the `actions` function hooked to `admin_init`. This makes it possible for unauthenticated attackers to delete arbitrary plugin settings via the `action` parameter.	5.3	More Details
CVE-2025-15475	The PayHere Payment Gateway Plugin for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to an improper validation logic in the check_payhere_response function in all versions up to, and including, 2.3.9. This makes it possible for unauthenticated attackers to change the status of pending WooCommerce orders to paid/completed/on hold.	5.3	More Details

CVE-2025-15512	The Aplazo Payment Gateway plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the check_success_response() function in all versions up to, and including, 1.4.2. This makes it possible for unauthenticated attackers to set any WooCommerce order to `pending payment` status.	5.3	More Details
CVE-2025-15513	The Float Payment Gateway plugin for WordPress is vulnerable to unauthorized modification of data due to improper error handling in the verifyFloatResponse() function in all versions up to, and including, 1.1.9. This makes it possible for unauthenticated attackers to mark any WooCommerce order as failed.	5.3	More Details
CVE-2025-15537	A security vulnerability has been detected in Mapnik up to 4.2.0. This issue affects the function mapnik::dbf_file::string_value of the file plugins/input/shape/dbfile.cpp. Such manipulation leads to heap-based buffer overflow. The attack must be carried out locally. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-21928	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2026-21929	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 9.0.0-9.5.0. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.3	More Details
CVE-2026-23829	Mailpit is an email testing tool and API for developers. Prior to version 1.28.3, Mailpit's SMTP server is vulnerable to Header Injection due to an insufficient Regular Expression used to validate `RCPT TO` and `MAIL FROM` addresses. An attacker can inject arbitrary SMTP headers (or corrupt existing ones) by including carriage return characters (`\r`) in the email address. This header injection occurs because the regex intended to filter control characters fails to exclude `\r` and `\n` when used inside a character class. Version 1.28.3 fixes this issue.	5.3	More Details
CVE-2025-15539	A vulnerability was determined in Open5GS up to 2.7.6. Impacted is the function sgwc_s11_handle_downlink_data_notification_ack of the file src/sgwc/s11-handler.c of the component sgwc. This manipulation causes denial of service. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. Patch name: b4707272c1caf6a7d4dca905694ea55557a0545f. To fix this issue, it is recommended to deploy a patch. The issue report is flagged as already-fixed.	5.3	More Details
CVE-2025-15538	A security vulnerability has been detected in Open Asset Import Library Assimp up to 6.0.2. Affected by this vulnerability is the function Assimp::LWOImporter::FindUVChannels of the file /src/assimp/code/AssetLib/LWO/LWOMaterial.cpp. Such manipulation leads to use after free. The attack needs to be performed locally. The exploit has been disclosed publicly and may be used. This and similar defects are tracked and handled via issue #6128.	5.3	More Details
CVE-2025-24089	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 18.3 and iPadOS 18.3. An app may be able to enumerate a user's installed apps.	5.3	More Details

CVE-2025-15534	A vulnerability was identified in raysan5 raylib up to 909f040. Affected by this issue is the function LoadFontData of the file src/rtext.c. The manipulation leads to integer overflow. The attack can only be performed from a local environment. The exploit is publicly available and might be used. The identifier of the patch is 5a3391fdce046bc5473e52afbd835dd2dc127146. It is suggested to install a patch to address this issue.	5.3	More Details
CVE-2025-15536	A weakness has been identified in BYVoid OpenCC up to 1.1.9. This vulnerability affects the function opencc::MaxMatchSegmentation of the file src/MaxMatchSegmentation.cpp. This manipulation causes heap-based buffer overflow. The attack is restricted to local execution. The exploit has been made available to the public and could be used for attacks. Patch name: 345c9a50ab07018f1b4439776bad78a0d40778ec. To fix this issue, it is recommended to deploy a patch.	5.3	More Details
CVE-2026-1170	A vulnerability was detected in birkir prime up to 0.4.0.beta.0. This issue affects some unknown processing of the file /graphql of the component GraphQL API. Performing a manipulation results in information disclosure. The attack may be initiated remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-1110	A flaw has been found in cijliu librtsp up to 2ec1a81ad65280568a0c7c16420d7c10fde13b04. This affects the function rtsp_parse_method. This manipulation causes buffer overflow. It is possible to launch the attack on the local host. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-15533	A vulnerability was determined in raysan5 raylib up to 909f040. Affected by this vulnerability is the function GenImageFontAtlas of the file src/rtext.c. Executing a manipulation can lead to heap-based buffer overflow. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized. This patch is called 5a3391fdce046bc5473e52afbd835dd2dc127146. Applying a patch is advised to resolve this issue.	5.3	More Details
CVE-2026-1109	A vulnerability was detected in cijliu librtsp up to 2ec1a81ad65280568a0c7c16420d7c10fde13b04. The impacted element is the function rtsp_parse_request. The manipulation results in buffer overflow. Attacking locally is a requirement. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-1108	A security vulnerability has been detected in cijliu librtsp up to 2ec1a81ad65280568a0c7c16420d7c10fde13b04. The affected element is the function rtsp_rely_dumps. The manipulation leads to buffer overflow. An attack has to be approached locally. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2021-47820	Ubee EVW327 contains a cross-site request forgery vulnerability that allows attackers to enable remote access without user interaction. Attackers can craft a malicious webpage that automatically submits a form to change router remote access settings to port 8080 without the user's consent.	5.3	More Details
	Umbraco CMS v8.14.1 contains a server-side request forgery vulnerability that		

CVE-2021-47776	allows attackers to manipulate baseUrl parameters in multiple dashboard and help controller endpoints. Attackers can craft malicious requests to the GetContextHelpForPage, GetRemoteDashboardContent, and GetRemoteDashboardCss endpoints to trigger unauthorized server-side requests to external hosts.	5.3	More Details
CVE-2026-22911	Firmware update files may expose password hashes for system accounts, which could allow a remote attacker to recover credentials and gain unauthorized access to the device.	5.3	More Details
CVE-2025-15532	A security flaw has been discovered in Open5GS up to 2.7.5. This issue affects some unknown processing of the component Timer Handler. The manipulation results in resource consumption. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. The patch is identified as c7c131f8d2cb1195ada5e0e691b6868ebcd8a845. It is best practice to apply a patch to resolve this issue.	5.3	More Details
CVE-2025-15531	A vulnerability was identified in Open5GS up to 2.7.5. This vulnerability affects the function sgwc_bearer_add of the file src/sgwc/context.c. The manipulation leads to reachable assertion. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The issue report is flagged as already-fixed.	5.3	More Details
CVE-2026-0717	The LottieFiles – Lottie block for Gutenberg plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.0.0 via the `/wp-json/lottiefiles/v1/settings/` REST API endpoint. This makes it possible for unauthenticated attackers to retrieve the site owner's LottieFiles.com account credentials including their API access token and email address when the 'Share LottieFiles account with other WordPress users' option is enabled.	5.3	More Details
CVE-2026-1172	A vulnerability has been found in birkir prime up to 0.4.0.beta.0. The affected element is an unknown function of the file /graphql of the component GraphQL Directive Handler. The manipulation leads to denial of service. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-1171	A flaw has been found in birkir prime up to 0.4.0.beta.0. Impacted is an unknown function of the file /graphql of the component GraphQL Field Handler. Executing a manipulation can lead to denial of service. The attack may be launched remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2025-14464	The PDF Resume Parser plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0. This is due to the plugin registering an AJAX action handler that is accessible to unauthenticated users and exposes SMTP configuration data including credentials. This makes it possible for unauthenticated attackers to extract sensitive SMTP credentials (username and password) from the WordPress configuration, which could be leveraged to compromise email accounts and potentially gain unauthorized access to other systems using the same credentials.	5.3	More Details
CVE-2021-47800	b2evolution 7.2.2 contains a cross-site request forgery vulnerability that allows attackers to modify admin account details without authentication. Attackers can craft a malicious HTML form to submit unauthorized changes to user profiles by tricking victims into loading a specially crafted webpage.	5.3	More Details
CVE-2026-0959	IEEE 802.11 protocol dissector crash in Wireshark 4.6.0 to 4.6.2 and 4.4.0 to 4.4.12 allows denial of service	5.3	More Details

CVE-2026-0962	SOME/IP-SD protocol dissector crash in Wireshark 4.6.0 to 4.6.2 and 4.4.0 to 4.4.12 allows denial of service	5.3	More Details
CVE-2026-23511	ZITADEL is an open source identity management platform. Prior to 4.9.1 and 3.4.6, a user enumeration vulnerability has been discovered in Zitadel's login interfaces. An unauthenticated attacker can exploit this flaw to confirm the existence of valid user accounts by iterating through usernames and userIDs. This vulnerability is fixed in 4.9.1 and 3.4.6.	5.3	More Details
CVE-2025-36419	IBM ApplinX 11.1 could disclose sensitive information about server architecture that could aid in further attacks against the system.	5.3	More Details
CVE-2025-14880	The Netcash WooCommerce Payment Gateway plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the handle_return_url function in all versions up to, and including, 4.1.3. This makes it possible for unauthenticated attackers to mark any WooCommerce order as processing/completed.	5.3	More Details
CVE-2026-1020	Police Statistics Database System developed by Gotac has a Absolute Path Traversal vulnerability, allowing unauthenticated remote attackers to enumerate the system file directory.	5.3	More Details
CVE-2025-14348	The weMail - Email Marketing, Lead Generation, Optin Forms, Email Newsletters, A/B Testing, and Automation plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.0.7. This is due to the plugin's REST API trusting the `x-wemail-user` HTTP header to identify users without verifying the request originates from an authenticated WordPress session. This makes it possible for unauthenticated attackers who know or can guess an admin email (easily enumerable via `/wp-json/wp/v2/users`) to impersonate that user and access the CSV subscriber endpoints, potentially exfiltrating subscriber PII (emails, names, phone numbers) from imported CSV files.	5.3	More Details
CVE-2025-14351	The Custom Fonts – Host Your Fonts Locally plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'BCF_Google_Fonts_Compatibility' class constructor function in all versions up to, and including, 2.1.16. This makes it possible for unauthenticated attackers to delete font directory and rewrite theme.json file.	5.3	More Details
CVE-2025-14978	The PeachPay — Payments & Express Checkout for WooCommerce (supports Stripe, PayPal, Square, Authorize.net) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability checks on the ConvesioPay webhook REST endpoint in all versions up to, and including, 1.119.8. This makes it possible for unauthenticated attackers to modify the status of arbitrary WooCommerce orders.	5.3	More Details
CVE-2026-1194	A security flaw has been discovered in MineAdmin 1.x/2.x. This affects an unknown function of the component Swagger. The manipulation results in information disclosure. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-14078	The PAYGENT for WooCommerce plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 2.4.6. This is due to missing authorization checks on the paygent_check_webhook function combined with the paygent_permission_callback function unconditionally returning true on line 199. This makes it possible for unauthenticated attackers to manipulate payment callbacks and modify order statuses by sending forged payment notifications via the `/wp-json/paygent/v1/check/` endpoint.	5.3	More Details

CVE-2025-15526	The Fancy Product Designer plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 6.4.8. This is due to improper error handling in the PDF upload functionality that exposes server filesystem paths and stack traces in error messages. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2026-23886	Swift W3C TraceContext is a Swift implementation of the W3C Trace Context standard, and Swift OTel is an OpenTelemetry Protocol (OTLP) backend for Swift Log, Swift Metrics, and Swift Distributed Tracing. Prior to Swift W3C TraceContext version 1.0.0-beta.5 and Swift OTel version 1.0.4, a denial-of-service vulnerability due to improper input validation allows a remote attacker to crash the service via a malformed HTTP header. This allows crashing the process with data coming from the network when used with, for example, an HTTP server. Most common way of using Swift W3C Trace Context is through Swift OTel. Version 1.0.0-beta.5 of Swift W3C TraceContext and version 1.0.4 of Swift OTel contain a patch for this issue. As a workaround, disable either Swift OTel or the code that extracts the trace information from an incoming header (such as a `TracingMiddleware`).	5.3	More Details
CVE-2026-0939	The Rede Itaú for WooCommerce plugin for WordPress is vulnerable to order status manipulation due to insufficient verification of data authenticity in all versions up to, and including, 5.1.2. This is due to the plugin failing to verify the authenticity of payment callbacks. This makes it possible for unauthenticated attackers to manipulate WooCommerce order statuses, either marking unpaid orders as paid, or failed.	5.3	More Details
CVE-2026-23849	File Browser provides a file managing interface within a specified directory and can be used to upload, delete, preview, rename, and edit files. Prior to version 2.55.0, the JSONAuth. Auth function contains a logic flaw that allows unauthenticated attackers to enumerate valid usernames by measuring the response time of the /api/login endpoint. The vulnerability exists due to a "short-circuit" evaluation in the authentication logic. When a username is not found in the database, the function returns immediately. However, if the username does exist, the code proceeds to verify the password using bcrypt (users.CheckPwd), which is a computationally expensive operation designed to be slow. This difference in execution path creates a measurable timing discrepancy. Version 2.55.0 contains a patch for the issue.	5.3	More Details
CVE-2026-0942	The Rede Itaú for WooCommerce — Payment PIX, Credit Card and Debit plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the clearOrderLogs() function in all versions up to, and including, 5.1.2. This makes it possible for unauthenticated attackers to delete the Rede Order Logs metadata from all WooCommerce orders.	5.3	More Details
CVE-2026-1175	A vulnerability was identified in birkir prime up to 0.4.0.beta.0. This impacts an unknown function of the file /graphql of the component GraphQL Directive Handler. Such manipulation leads to information exposure through error message. The attack may be performed from remote. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2025-14757	The Cost Calculator Builder plugin for WordPress is vulnerable to Unauthenticated Payment Status Bypass in all versions up to, and including, 3.6.9 only when used in combination with Cost Calculator Builder PRO. This is due to the complete_payment AJAX action being registered via wp_ajax_nopriv, making it accessible to unauthenticated users, and the complete() function only verifying a nonce without checking user capabilities or order ownership. Since nonces are exposed to all visitors via window.ccb_nonces in the page source, any unauthenticated attacker can mark any order's payment status as "completed" without actual payment.	5.3	More Details

CVE-2026-1174	A vulnerability was determined in birkir prime up to 0.4.0.beta.0. This affects an unknown function of the file /graphql of the component GraphQL Alias Handler. This manipulation causes resource consumption. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-1173	A vulnerability was found in birkir prime up to 0.4.0.beta.0. The impacted element is an unknown function of the file /graphql of the component GraphQL Array Based Query Batch Handler. The manipulation results in denial of service. The attack can be executed remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-1004	The Essential Addons for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to and including 6.5.5 via the 'eael_product_quickview_popup' function. This makes it possible for unauthenticated attackers to retrieve WooCommerce product information for products with draft, pending, or private status, which should normally be restricted.	5.3	More Details
CVE-2025-15530	A vulnerability was determined in Open5GS up to 2.7.6. This affects the function sgwc_s11_handle_create_indirect_data_forwarding_tunnel_request of the file /src/sgwc/s11-handler.c. Executing a manipulation can lead to reachable assertion. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The issue report is flagged as already-fixed.	5.3	More Details
CVE-2025-14798	The LearnPress – WordPress LMS Plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 4.3.2.4 via the get_item_permissions_check function. This makes it possible for unauthenticated attackers to extract sensitive data including user first names and last names. Other information such as social profile links and enrollment are also included.	5.3	More Details
CVE-2026-21972	Vulnerability in the Oracle Configurator product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Configurator accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2025-15529	A vulnerability was found in Open5GS up to 2.7.6. Affected by this issue is the function sgwc_s5c_handle_create_session_response of the file src/sgwc/s5c-handler.c. Performing a manipulation results in denial of service. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The patch is named b19cf6a2dbf5d30811be4488bf059c865bd7d1d2. To fix this issue, it is recommended to deploy a patch.	5.3	More Details
CVE-2026-22644	Certain requests pass the authentication token in the URL as string query parameter, making it vulnerable to theft through server logs, proxy logs and Referer headers, which could allow an attacker to hijack the user's session and gain unauthorized access.	5.3	More Details
CVE-2021-47754	Arunna 1.0.0 contains a cross-site request forgery vulnerability that allows attackers to manipulate user profile settings without authentication. Attackers can craft a malicious form to change user details, including passwords, email, and administrative privileges by tricking authenticated users into submitting the form.	5.3	More Details
	The WP Hotel Booking plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.2.7. This is due to the plugin		

CVE-2025-14075	exposing the 'hotel_booking_fetch_customer_info' AJAX action to unauthenticated users without proper capability checks, relying only on a nonce for protection. This makes it possible for unauthenticated attackers to retrieve sensitive customer information including full names, addresses, phone numbers, and email addresses by providing a valid email address and a publicly accessible nonce.	5.3	More Details
CVE-2026-22645	The application discloses all used components, versions and license information to unauthenticated actors, giving attackers the opportunity to target known security vulnerabilities of used components.	5.3	More Details
CVE-2025-14463	The Payment Button for PayPal plugin for WordPress is vulnerable to unauthorized order creation in all versions up to, and including, 1.2.3.41. This is due to the plugin exposing a public AJAX endpoint (`wppaypalcheckout_ajax_process_order`) that processes checkout results without any authentication or server-side verification of the PayPal transaction. This makes it possible for unauthenticated attackers to create arbitrary orders on the site with any chosen transaction ID, payment status, product name, amount, or customer information via direct POST requests to the AJAX endpoint, granted they can bypass basic parameter validation. If email sending is enabled, the plugin will also trigger purchase receipt emails to any email address supplied in the request, leading to order database corruption and unauthorized outgoing emails without any real PayPal transaction taking place.	5.3	More Details
CVE-2025-15528	A vulnerability has been found in Open5GS up to 2.7.6. Affected by this vulnerability is an unknown functionality of the component GTPv2 Bearer Response Handler. Such manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 98f76e98df35cd6a35e868aa62715db7f8141ac1. A patch should be applied to remediate this issue.	5.3	More Details
CVE-2026-0820	The RepairBuddy – Repair Shop CRM & Booking Plugin for WordPress plugin for WordPress is vulnerable to Insecure Direct Object Reference due to missing capability checks on the wc_upload_and_save_signature_handler function in all versions up to, and including, 4.1116. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary signatures to any order in the system, potentially modifying order metadata and triggering unauthorized status changes.	5.3	More Details
CVE-2025-12825	The User Registration Using Contact Form 7 plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'get_cf7_form_data' function in all versions up to, and including, 2.5. This makes it possible for unauthenticated attackers to retrieve form settings which includes Facebook app secrets.	5.3	More Details
CVE-2025-14029	The Community Events plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ajax_admin_event_approval() function in all versions up to, and including, 1.5.6. This makes it possible for unauthenticated attackers to approve arbitrary events via the 'eventlist' parameter.	5.3	More Details
CVE-2026-21974	Vulnerability in the Oracle Life Sciences Central Designer product of Oracle Health Sciences Applications (component: Platform). The supported version that is affected is 7.0.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Life Sciences Central Designer. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Life Sciences Central Designer accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
	The CubeWP – All-in-One Dynamic Content Framework plugin for WordPress is		

CVE-2025-12129	vulnerable to Information Exposure in all versions up to, and including, 1.1.27 via the /cubewp-posts/v1/query-new and /cubewp-posts/v1/query REST API endpoints 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.	5.3	More Details
CVE-2025-66169	Cypher Injection vulnerability in Apache Camel camel-neo4j component. This issue affects Apache Camel: from 4.10.0 before 4.10.8, from 4.14.0 before 4.14.3, from 4.15.0 before 4.17.0 Users are recommended to upgrade to version 4.10.8 for 4.10.x LTS and 4.14.3 for 4.14.x LTS and 4.17.0.	5.3	More Details
CVE-2025-12895	The Kalium 3 | Creative WordPress & WooCommerce Theme theme for WordPress is vulnerable to unauthorized email sending due to a missing capability check on the kalium_vc_contact_form_request() function in all versions up to, and including, 3.29. This makes it possible for unauthenticated attackers to use the theme an an open mail relay and send email to arbitrary email addresses on the server's behalf.	5.3	More Details
CVE-2025-67083	Directory traversal vulnerability in InvoicePlane through 1.6.3 allows unauthenticated attackers to read files from the server. The ability to read files and the file type depends on the web server and its configuration.	5.3	More Details
CVE-2026-0808	The Spin Wheel plugin for WordPress is vulnerable to client-side prize manipulation in all versions up to, and including, 2.1.0. This is due to the plugin trusting client-supplied prize selection data without server-side validation or randomization. This makes it possible for unauthenticated attackers to manipulate which prize they win by modifying the 'prize_index' parameter sent to the server, allowing them to always select the most valuable prizes.	5.3	More Details
CVE-2025-56226	Libsndfile <=1.2.2 contains a memory leak vulnerability in the mpeg_l3_encoder_init() function within the mpeg_l3_encode.c file.	5.3	More Details
CVE-2025-68966	Permission control vulnerability in the Notepad module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.1	More Details
CVE-2025-68961	Multi-thread race condition vulnerability in the camera framework module. Impact: Successful exploitation of this vulnerability may affect availability.	5.1	More Details
CVE-2026-21223	Microsoft Edge Elevation Service exposes a privileged COM interface that inadequately validates the privileges of the calling process. A standard (non-administrator) local user can invoke the IElevatorEdge interface method LaunchUpdateCmdElevatedAndWait, causing the service to execute privileged update commands as LocalSystem. This allows a non-administrator to enable or disable Windows Virtualization-Based Security (VBS) by modifying protected system registry keys under HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard. Disabling VBS weakens critical platform protections such as Credential Guard, Hypervisor-protected Code Integrity (HVCI), and the Secure Kernel, resulting in a security feature bypass.	5.1	More Details
CVE-2025-68962	Multi-thread race condition vulnerability in the camera framework module. Impact: Successful exploitation of this vulnerability may affect availability.	5.1	More Details
CVE-2025-14793	The DK PDF – WordPress PDF Generator plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.3.0 via the 'addContentToMpdf' function. This makes it possible for authenticated attackers, author level 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	5.0	More Details

	services.		
CVE-2026-1195	A weakness has been identified in MineAdmin 1.x/2.x. This impacts the function refresh of the file /system/refresh of the component JWT Token Handler. This manipulation causes insufficient verification of data authenticity. It is possible to initiate the attack remotely. The attack is considered to have high complexity. The exploitability is said to be difficult. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.0	More Details
CVE-2026-21942	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystems). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H).	5.0	More Details
CVE-2026-22641	This vulnerability in Grafana's datasource proxy API allows authorization checks to be bypassed by adding an extra slash character in the URL path. Users with minimal permissions could gain unauthorized read access to GET endpoints in Alertmanager and Prometheus datasources. The issue primarily affects datasources that implement route-specific permissions, including Alertmanager and certain Prometheus-based datasources.	5.0	More Details
CVE-2025-67081	An SQL injection vulnerability in Itflow through 25.06 has been identified in the "role_id" parameter when editing a profile. An attacker with admin account can exploit this issue via blind SQL injection, allowing for the extraction of arbitrary data from the database. The vulnerability arises from insufficient sanitizing on integer parameter.	4.9	More Details
CVE-2025-13925	IBM Aspera Console 3.4.7 stores potentially sensitive information in log files that could be read by a local privileged user.	4.9	More Details
CVE-2025-12984	The Advanced Ads – Ad Manager & AdSense plugin for WordPress is vulnerable to SQL Injection via the 'order' parameter in all versions up to, and including, 2.0.15 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-2026-21959	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Workflow Loader). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Workflow accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.9	More Details
CVE-2026-21964	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.0-8.0.44, 8.4.0-8.4.7 and 9.0.0-9.5.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE-2026-21936	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.44, 8.4.0-8.4.7 and 9.0.0-9.5.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-1223	PrismX MX100 AP controller developed by BROWAN COMMUNICATIONS has an Insufficiently Protected Credentials vulnerability, allowing privileged remote attackers to allowing authenticated remote attackers to obtain SMTP plaintext passwords through the web frontend.	4.9	More Details
CVE-2026-0678	The Flat Shipping Rate by City for WooCommerce plugin for WordPress is vulnerable to time-based SQL Injection via the 'cities' parameter in all versions up to, and including, 1.0.3 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 Shop Manager-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-2026-21941	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.44, 8.4.0-8.4.7 and 9.0.0-9.5.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-21937	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.0-8.0.44, 8.4.0-8.4.7 and 9.0.0-9.5.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-21952	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 9.0.0-9.5.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2026-21948	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.44, 8.4.0-8.4.7 and 9.0.0-9.5.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability is		

CVE-2026-20076	due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid administrative credentials.	4.8	More Details
CVE-2026-20075	A vulnerability in the web-based management interface of Cisco Evolved Programmable Network Manager (EPNM) and Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against users of the interface of an affected system. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious code into specific data fields in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, an attacker must have valid administrative credentials.	4.8	More Details
CVE-2025-51602	mmstu.c in VideoLAN VLC media player before 3.0.22 allows an out-of-bounds read and denial of service via a crafted 0x01 response from an MMS server.	4.8	More Details
CVE-2026-21925	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: RMI). Supported versions that are affected are Oracle Java SE: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17 and 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	4.8	More Details
CVE-2026-20047	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid administrative credentials.	4.8	More Details
CVE-2026-1152	A security vulnerability has been detected in technical-laohu mpay up to 1.2.4. The impacted element is an unknown function of the component QR Code Image Handler. Such manipulation of the argument codeimg leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	4.7	More Details
CVE-	Permission control vulnerability in the Notepad module. Impact: Successful		More

2025-68965	exploitation of this vulnerability may affect service confidentiality.	4.7	Details
CVE-2026-0960	HTTP3 protocol dissector infinite loop in Wireshark 4.6.0 to 4.6.2 allows denial of service	4.7	More Details
CVE-2026-1111	A vulnerability has been found in Sanluan PublicCMS up to 5.202506.d. This impacts the function Save of the file com/publiccms/controller/admin/sys/TaskTemplateAdminController.java of the component Task Template Management Handler. Such manipulation of the argument path leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-1064	A vulnerability was found in bastillion-io Bastillion up to 4.0.1. This issue affects some unknown processing of the file src/main/java/io/bastillion/manage/control/SystemKtrl.java of the component System Management Module. Performing a manipulation results in command injection. The attack can be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-1063	A vulnerability has been found in bastillion-io Bastillion up to 4.0.1. This vulnerability affects unknown code of the file src/main/java/io/bastillion/manage/control/AuthKeysKtrl.java of the component Public Key Management System. Such manipulation leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-36059	IBM Business Automation Workflow containers 25.0.0 through 25.0.0 Interim Fix 002, 24.0.1 through 24.0.1 Interim Fix 005, and 24.0.0 through 24.0.0 Interim Fix 006. IBM Cloud Pak for Business Automation could allow a local user with access to the container to execute OS system calls.	4.7	More Details
CVE-2025-13454	A potential vulnerability was reported in ThinkPlus configuration software that could allow a local authenticated user to gain access to sensitive device information.	4.7	More Details
CVE-2025-67399	An issue in AIRTH SMART HOME AQI MONITOR Bootloader v.1.005 allows a physically proximate attacker to obtain sensitive information via the UART port of the BK7231N controller (Wi-Fi and BLE module) on the device is open to access	4.6	More Details
CVE-2026-21981	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.14 and 7.2.4. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.6 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:L).	4.6	More Details
CVE-	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.29 and 21.3-21.20. Easily exploitable vulnerability allows high privileged attacker having Authenticated User privilege with		

2026-21975	network access via Oracle Net to compromise Java VM. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java VM. CVSS 3.1 Base Score 4.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H).	4.5	More Details
CVE-2025-14379	The Testimonials Creator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in version 1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-14632	The Filr – Secure document library plugin for WordPress is vulnerable to Stored Cross-Site Scripting via unrestricted file upload in all versions up to, and including, 1.2.11 due to insufficient file type restrictions in the FILR_Uploader class. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload malicious HTML files containing JavaScript that will execute whenever a user accesses the uploaded file, granted they have permission to create or edit posts with the 'filr' post type.	4.4	More Details
CVE-2025-13627	The Makesweat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'makesweat_clubid' setting in all versions up to, and including, 0.1 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.	4.4	More Details
CVE-2025-15021	The Gotham Block Extra Light plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings 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 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-2026-1045	The Viet contact plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-14725	The Internal Link Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings 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 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-2026-0680	The Real Post Slider Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin settings in all versions up to, and including, 2.4 due to insufficient input sanitization and output escaping. 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. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details

CVE-2025-15486	The Kunze Law plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin's shortcode in all versions up to, and including, 2.1 due to the plugin fetching HTML content from a remote server and injecting it into pages without any sanitization or 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. Additional presence of a path traversal vulnerability in the shortcode name allows writing malicious HTML files to arbitrary writable locations on the server.	4.4	More Details
CVE-2026-1042	The WP Hello Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'digit_one' and 'digit_two' parameters in all versions up to, and including, 1.02 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.	4.4	More Details
CVE-2026-0739	The WMF Mobile Redirector plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin settings in all versions up to, and including, 1.2 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.	4.4	More Details
CVE-2026-0741	The Electric Studio Download Counter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin settings in all versions up to, and including, 2.4 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.	4.4	More Details
CVE-2026-0812	The LinkedIn SC plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'linkedin_sc_date_format', 'linkedin_sc_api_key', and 'linkedin_sc_secret_key' parameters in all versions up to, and including, 1.1.9 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 the injected page.	4.4	More Details
CVE-2026-0813	The Short Link plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'short_link_post_title' and 'short_link_page_title' 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 the injected page.	4.4	More Details
CVE-2026-0725	The Integrate Dynamics 365 CRM plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.1.1 due to insufficient input sanitization and output escaping on user supplied attributes. 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.	4.4	More Details
CVE-2026-0691	The CM E-Mail Blacklist – Simple email filtering for safer registration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'black_email' parameter in all versions up to, and including, 1.6.2. This is 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-2026-0734	The WP Allowed Hosts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'allowed-hosts' parameter in all versions up to, and including, 1.0.8 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-2026-22646	Certain error messages returned by the application expose internal system details that should not be visible to end users, providing attackers with valuable reconnaissance information (like file paths, database errors, or software versions) that can be used to map the application's internal structure and discover other, more critical vulnerabilities.	4.3	More Details
CVE-2026-0635	The Responsive Accordion Slider plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'resp_accordion_silder_save_images' function in all versions up to, and including, 1.2.2. This makes it possible for authenticated attackers, with Contributor-level access and above, to modify any slider's image metadata including titles, descriptions, alt text, and links.	4.3	More Details
CVE-2026-1003	The GetGenie plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.3.0. This is due to the plugin not properly verifying that a user is authorized to delete a specific post. This makes it possible for authenticated attackers, with Author-level access and above, to delete any post on the WordPress site, including posts authored by other users.	4.3	More Details
CVE-2026-23721	OpenProject is an open-source, web-based project management software. When using groups in OpenProject to manage users, the group members should only be visible to users that have the View Members permission in any project that the group is also a member of. Prior to versions 17.0.1 and 16.6.5, due to a failed permission check, if a user had the View Members permission in any project, they could enumerate all Groups and view which other users are part of the group. The issue has been fixed in OpenProject 17.0.1 and 16.6.5. No known workarounds are available.	4.3	More Details
CVE-2026-23494	Pimcore is an Open Source Data & Experience Management Platform. Prior to 12.3.1 and 11.5.14, the application fails to enforce proper server-side authorization checks on the API endpoint responsible for reading or listing static routes. In Pimcore, static routes are custom URL patterns defined via the backend interface or the var/config/staticroutes.php file, including details like regex-based patterns, controllers, variables, and priorities. These routes are registered automatically through the PimcoreStaticRoutesBundle and integrated into the MVC routing system. Testing revealed that an authenticated backend user lacking explicit permissions was able to invoke the endpoint (e.g., GET /api/static-routes) and retrieve sensitive route configurations. This vulnerability is fixed in 12.3.1 and 11.5.14.	4.3	More Details
CVE-2026-22639	Grafana is an open-source platform for monitoring and observability. The Grafana Alerting DingDing integration was not properly protected and could be exposed to users with Viewer permission. Fixed in versions 10.4.19+security-01, 11.2.10+security-01, 11.3.7+security-01, 11.4.5+security-01, 11.5.5+security-01, 11.6.2+security-01 and 12.0.1+security-01	4.3	More Details
CVE-2025-14853	The LEAV Last Email Address Validator plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions <= 1.7.1. This is due to missing or incorrect nonce validation on the display_settings_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-2026-0554	The NotificationX plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'regenerate' and 'reset' REST API endpoints in all versions up to, and including, 3.1.11. This makes it possible for authenticated attackers, with Contributor-level access and above, to reset analytics for any NotificationX campaign, regardless of ownership.	4.3	More Details
CVE-2025-15527	The WP Recipe Maker plugin for WordPress is vulnerable to Information Exposure in versions up to, and including, 10.2.2 via the api_get_post_summary function due to insufficient restrictions on which posts can be retrieved. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from posts they may not be able to edit or read otherwise. This also affects password protected, private, or draft posts that they should not have access to.	4.3	More Details
CVE-2025-14482	The Crush.pics Image Optimizer - Image Compression and Optimization plugin for WordPress is vulnerable to unauthorized modification of data due to missing capability checks on multiple functions in all versions up to, and including, 1.8.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify plugin settings including disabling auto-compression and changing image quality settings.	4.3	More Details
CVE-2025-15370	The Shield: Blocks Bots, Protects Users, and Prevents Security Breaches plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 21.0.9 via the MfaGoogleAuthToggle class due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to disable Google Authenticator for any user.	4.3	More Details
CVE-2025-14982	The Booking Calendar plugin for WordPress is vulnerable to Missing Authorization leading to Sensitive Information Exposure in all versions up to, and including, 10.14.11. This makes it possible for authenticated attackers, with Subscriber-level access and above, to view all booking records in the database, including personally identifiable information (PII) such as names, email addresses, phone numbers, physical addresses, payment status, booking costs, and booking hashes belonging to other users.	4.3	More Details
CVE-2025-14384	The All in One SEO – Powerful SEO Plugin to Boost SEO Rankings & Increase Traffic plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the `/aioseo/v1/ai/credits` REST route in all versions up to, and including, 4.9.2. This makes it possible for authenticated attackers, with Contributor-level access and above, to disclose the global AI access token.	4.3	More Details
CVE-2025-15377	The Sosh Share Buttons plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.0. This is due to missing nonce validation on the 'admin_page_content' function. This makes it possible for unauthenticated attackers to update the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-23495	Pimcore's Admin Classic Bundle provides a Backend UI for Pimcore. Prior to 2.2.3 and 1.7.16, the API endpoint for listing Predefined Properties in the Pimcore platform lacks adequate server-side authorization checks. Predefined Properties are configurable metadata definitions (e.g., name, key, type, default value) used across documents, assets, and objects to standardize custom attributes and improve editorial workflows, as documented in Pimcore's official properties guide. Testing confirmed that an authenticated backend user without explicit permissions for property management could successfully call the endpoint and retrieve the complete list of these configurations. The vulnerability is fixed in 2.2.3 and 1.7.16.	4.3	More Details
CVE-	The Newsletter – Send awesome emails from WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 9.1.0.		

2026-1051	This is due to missing or incorrect nonce validation on the hook_newsletter_action() function. This makes it possible for unauthenticated attackers to unsubscribe newsletter subscribers via a forged request granted they can trick a logged-in user into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-23724	WeGIA is a web manager for charitable institutions. Prior to 3.6.2, a Stored Cross-Site Scripting (XSS) vulnerability was identified in the html/atendido/cadastro_ocorrencia.php endpoint of the WeGIA application. The application does not sanitize user-controlled data before rendering it inside the “Atendido” selection dropdown. This vulnerability is fixed in 3.6.2.	4.3	More Details
CVE-2026-1169	A security vulnerability has been detected in birkir prime up to 0.4.0.beta.0. This vulnerability affects unknown code. Such manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-23731	WeGIA is a web manager for charitable institutions. Prior to 3.6.2, The web application is vulnerable to clickjacking attacks. The WeGIA application does not send any defensive HTTP headers related to framing protection. In particular, X-Frame-Options is missing andContent-Security-Policy with frame-ancestors directive is not configured. Because of this, an attacker can load any WeGIA page inside a malicious HTML document, overlay deceptive elements, hide real buttons, or force accidental interaction with sensitive workflows. This vulnerability is fixed in 3.6.2.	4.3	More Details
CVE-2026-22912	Improper validation of a login parameter may allow attackers to redirect users to malicious websites after authentication. This can lead to various risk including stealing credentials from unsuspecting users.	4.3	More Details
CVE-2025-14846	The SocialChamp with WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.3. This is due to missing nonce validation on the wpsc_settings_tab_menu 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-2026-22916	An attacker with low privileges may be able to trigger critical system functions such as reboot or factory reset without proper restrictions, potentially leading to service disruption or loss of configuration.	4.3	More Details
CVE-2026-1134	A vulnerability was identified in itsourcecode Society Management System 1.0. This affects an unknown function of the file /admin/expenses.php. The manipulation of the argument detail leads to cross site scripting. The attack may be initiated remotely. The exploit is publicly available and might be used.	4.3	More Details
CVE-2026-22918	An attacker may exploit missing protection against clickjacking by tricking users into performing unintended actions through maliciously crafted web pages, leading to the extraction of sensitive data.	4.3	More Details
CVE-2026-22914	An attacker with limited permissions may still be able to write files to specific locations on the device, potentially leading to system manipulation.	4.3	More Details
CVE-2026-1135	A security flaw has been discovered in itsourcecode Society Management System 1.0. This impacts an unknown function of the file /admin/activity.php. The manipulation of the argument Title results in cross site scripting. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	4.3	More Details
	The Phrase TMS Integration for WordPress plugin for WordPress is vulnerable to		

CVE-2025-12168	unauthorized modification of data due to a missing capability check on the 'wp_ajax_delete_log' AJAX endpoint in all versions up to, and including, 4.7.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete log files.	4.3	More Details
CVE-2026-1142	A security flaw has been discovered in PHPGurukul News Portal 1.0. The impacted element is an unknown function. Performing a manipulation results in cross-site request forgery. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	4.3	More Details
CVE-2026-22917	Improper input handling in a system endpoint may allow attackers to overload resources, causing a denial of service.	4.3	More Details
CVE-2025-14389	The WPBlogSyn plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0. This is due to missing or incorrect nonce validation. This makes it possible for unauthenticated attackers to update the plugin's remote sync 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-2026-1148	A vulnerability was determined in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0. This vulnerability affects unknown code. Executing a manipulation can lead to cross-site request forgery. It is possible to launch the attack remotely.	4.3	More Details
CVE-2026-1153	A vulnerability was detected in technical-laohu mpay up to 1.2.4. This affects an unknown function. Performing a manipulation results in cross-site request forgery. Remote exploitation of the attack is possible. The exploit is now public and may be used.	4.3	More Details
CVE-2026-1154	A flaw has been found in SourceCodester E-Learning System 1.0. This impacts an unknown function of the file /admin/modules/lesson/index.php of the component Lesson Module Handler. Executing a manipulation of the argument Title/Description can lead to basic cross site scripting. The attack can be executed remotely. The exploit has been published and may be used.	4.3	More Details
CVE-2025-15376	The Stopwords for comments 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 'set_stopwords_for_comments' and 'delete_stopwords_for_comments' functions. This makes it possible for unauthenticated attackers to add or delete stopwords 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-2026-22913	Improper handling of a URL parameter may allow attackers to execute code in a user's browser after login. This can lead to the extraction of sensitive data.	4.3	More Details
CVE-2026-22915	An attacker with low privileges may be able to read files from specific directories on the device, potentially exposing sensitive information.	4.3	More Details
CVE-2026-21979	Vulnerability in the Oracle Planning and Budgeting Cloud Service product of Oracle Hyperion (component: EPM Agent). The supported version that is affected is 25.04.07. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Planning and Budgeting Cloud Service executes to compromise Oracle Planning and Budgeting Cloud Service. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Planning and Budgeting Cloud Service accessible data. Note:	4.2	More Details

	Update EPM Agent. Please refer to <a href="https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/diepm/epm_agent_downloading_agent_110x80569d70.html">Downloading the EPM Agent for more information. CVSS 3.1 Base Score 4.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:N/A:N).		
CVE-2026-22642	An open redirect vulnerability has been identified in Grafana OSS organization switching functionality. Prerequisites for exploitation: - Multiple organizations must exist in the Grafana instance - Victim must be on a different organization than the one specified in the URL	4.2	More Details
CVE-2026-21922	Vulnerability in the Oracle Planning and Budgeting Cloud Service product of Oracle Hyperion (component: EPM Agent). The supported version that is affected is 25.04.07. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Planning and Budgeting Cloud Service executes to compromise Oracle Planning and Budgeting Cloud Service. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Planning and Budgeting Cloud Service accessible data. Note: Update EPM Agent. Please refer to <a href="https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/diepm/epm_agent_downloading_agent_110x80569d70.html">Downloading the EPM Agent for more information. CVSS 3.1 Base Score 4.2 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N).	4.2	More Details
CVE-2025-43904	In SchedMD Slurm before 24.11.5, 24.05.8, and 23.11.11, the accounting system can allow a Coordinator to promote a user to Administrator.	4.2	More Details
CVE-2026-23766	Istio through 1.28.2 allows iptables rule injection for changing firewall behavior via the traffic.sidecar.istio.io/excludeInterfaces annotation. NOTE: the reporter's position is "this doesn't represent a security vulnerability (pod creators can already exclude sidecar injection entirely)."	4.1	More Details
CVE-2026-22919	An attacker with administrative access may inject malicious content into the login page, potentially enabling cross-site scripting (XSS) attacks, leading to the extraction of sensitive data.	3.8	More Details
CVE-2026-23522	LobeChat is an open source chat application platform. Prior to version 2.0.0-next.193, `knowledgeBase.removeFilesFromKnowledgeBase` tRPC ep allows authenticated users to delete files from any knowledge base without verifying ownership. `userId` filter in the database query is commented out, so it's enabling attackers to delete other users' KB files if they know the knowledge base ID and file ID. While the vulnerability is confirmed, practical exploitation requires knowing target's KB ID and target's file ID. These IDs are random and not easily enumerable. However, IDs may leak through shared links, logs, referrer headers and so on. Missing authorization check is a critical security flaw regardless. Users should upgrade to version 2.0.0-next.193 to receive a patch.	3.7	More Details
CVE-2026-22820	Outray openSource ngrok alternative. Prior to 0.1.5, a TOCTOU race condition vulnerability allows a user to exceed the set number of active tunnels in their subscription plan. This vulnerability is fixed in 0.1.5.	3.7	More Details
CVE-2025-14457	The Drag and Drop Multiple File Upload for Contact Form 7 plugin for WordPress is vulnerable to unauthorized modification of data due to a missing ownership check in the dnd_codedropz_upload_delete() function in all versions up to, and including, 1.3.9.2. This makes it possible for unauthenticated attackers to delete arbitrary uploaded files when the "Send attachments as links" setting is enabled.	3.7	More Details
	A flaw was identified in the RelaxNG parser of libxml2 related to how external		

CVE-2026-0989	schema inclusions are handled. The parser does not enforce a limit on inclusion depth when resolving nested <include> directives. Specially crafted or overly complex schemas can cause excessive recursion during parsing. This may lead to stack exhaustion and application crashes, creating a denial-of-service risk.	3.7	More Details
CVE-2026-22920	The device's passwords have not been adequately salted, making them vulnerable to password extraction attacks.	3.7	More Details
CVE-2026-22036	Undici is an HTTP/1.1 client for Node.js. Prior to 7.18.0 and 6.23.0, the number of links in the decompression chain is unbounded and the default maxHeaderSize allows a malicious server to insert thousands compression steps leading to high CPU usage and excessive memory allocation. This vulnerability is fixed in 7.18.0 and 6.23.0.	3.7	More Details
CVE-2026-0976	A flaw was found in Keycloak. This improper input validation vulnerability occurs because Keycloak accepts RFC-compliant matrix parameters in URL path segments, while common reverse proxy configurations may ignore or mishandle them. A remote attacker can craft requests to mask path segments, potentially bypassing proxy-level path filtering. This could expose administrative or sensitive endpoints that operators believe are not externally reachable.	3.7	More Details
CVE-2026-1048	A weakness has been identified in LigeroSmart up to 6.1.26. Impacted is an unknown function of the file /otrs/index.pl?Action=AgentTicketZoom. This manipulation of the argument TicketID causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	3.5	More Details
CVE-2026-1049	A security vulnerability has been detected in LigeroSmart up to 6.1.26. The affected element is an unknown function of the file /otrs/index.pl. Such manipulation of the argument TicketID leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.5	More Details
CVE-2025-36411	IBM ApplinX 11.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	3.5	More Details
CVE-2026-1147	A vulnerability was found in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0. This affects an unknown part of the file /php/api_patient_schedule.php. Performing a manipulation of the argument Reason results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	3.5	More Details
CVE-2026-1146	A vulnerability has been found in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0. Affected by this issue is some unknown functionality of the file /php/api_register_patient.php. Such manipulation of the argument firstName/lastName leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2026-1136	A weakness has been identified in lcg0124 BootDo up to e93dd428ef6f5c881aa74d49a2099ab0cf1e0fcb. Affected is the function Save of the file /blog/bContent/save of the component ContentController. This manipulation of the argument content/author/title causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided.	3.5	More Details

CVE-2026-1161	A vulnerability was detected in pbrong hrms 1.0.1. The affected element is the function UpdateRecruitmentById of the file /handler/recruitment.go. The manipulation results in cross site scripting. The attack may be launched remotely. The exploit is now public and may be used.	3.5	More Details
CVE-2025-55249	HCL AION is affected by a Missing Security Response Headers vulnerability. The absence of standard security headers may weaken the application’s overall security posture and increase its susceptibility to common web-based attacks.	3.5	More Details
CVE-2024-44210	This issue was addressed with improved permissions checking. This issue is fixed in macOS Sequoia 15.1. An app may be able to access user-sensitive data.	3.3	More Details
CVE-2025-24090	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 18.3 and iPadOS 18.3. An app may be able to enumerate a user's installed apps.	3.3	More Details
CVE-2025-15535	A security flaw has been discovered in nicbarker clay up to 0.14. This affects the function Clay__MeasureTextCached in the library clay.h. The manipulation results in null pointer dereference. The attack is only possible with local access. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2025-31186	A permissions issue was addressed with additional restrictions. This issue is fixed in Xcode 16.3. An app may be able to bypass Privacy preferences.	3.3	More Details
CVE-2025-14058	A potential missing authentication vulnerability was reported in some Lenovo Tablets that could allow an unauthorized user with physical access to modify Control Center settings if the device is locked when the "Allow Control Center access when locked" option is disabled.	3.2	More Details
CVE-2025-36410	IBM ApplinX 11.1 could allow an authenticated user to perform unauthorized administrative actions on the server due to server-side enforcement of client-side security.	3.1	More Details
CVE-2026-1197	A vulnerability was detected in MineAdmin 1.x/2.x. Affected by this vulnerability is an unknown functionality of the file /system/downloadById. Performing a manipulation of the argument ID results in information disclosure. The attack can be initiated remotely. The attack's complexity is rated as high. The exploitation appears to be 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.	3.1	More Details
CVE-2025-14822	Mattermost versions 10.11.x <= 10.11.8 fail to validate input size before processing hashtags which allows an authenticated attacker to exhaust CPU resources via a single HTTP request containing a post with thousands space-separated tokens	3.1	More Details
CVE-2025-55251	HCL AION is affected by an Unrestricted File Upload vulnerability. This can allow malicious file uploads, potentially resulting in unauthorized code execution or system compromise.	3.1	More Details
CVE-2026-21947	Vulnerability in Oracle Java SE (component: JavaFX). Supported versions that are affected are Oracle Java SE: 8u471-b50. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for	3.1	More Details

	security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).		
CVE-2025-55252	HCL AION version 2 is affected by a Weak Password Policy vulnerability. This can allow the use of easily guessable passwords, potentially resulting in unauthorized access	3.1	More Details
CVE-2026-1196	A security vulnerability has been detected in MineAdmin 1.x/2.x. Affected is an unknown function of the file /system/getFileInfoById. Such manipulation of the argument ID leads to information disclosure. It is possible to launch the attack remotely. The attack requires a high level of complexity. The exploitability is told to be 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.	3.1	More Details
CVE-2026-21977	Vulnerability in the Oracle Zero Data Loss Recovery Appliance Software product of Oracle Zero Data Loss Recovery Appliance (component: Security). Supported versions that are affected are 23.1.0-23.1.202509. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Oracle Zero Data Loss Recovery Appliance Software. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Zero Data Loss Recovery Appliance Software accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	3.1	More Details
CVE-2026-0992	A flaw was found in the libxml2 library. This uncontrolled resource consumption vulnerability occurs when processing XML catalogs that contain repeated <nextCatalog> elements pointing to the same downstream catalog. A remote attacker can exploit this by supplying crafted catalogs, causing the parser to redundantly traverse catalog chains. This leads to excessive CPU consumption and degrades application availability, resulting in a denial-of-service condition.	2.9	More Details
CVE-2025-52659	HCL AION version 2 is affected by a Cacheable HTTP Response vulnerability. This may lead to unintended storage of sensitive or dynamic content, potentially resulting in unauthorized access or information disclosure.	2.8	More Details
CVE-2026-21965	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Pluggable Auth). Supported versions that are affected are 9.0.0-9.5.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.7	More Details
CVE-2025-52660	HCL AION is affected by an Unrestricted File Upload vulnerability. This can allow malicious file uploads, potentially resulting in unauthorized code execution or system compromise.	2.7	More Details
CVE-2025-61873	Best Practical Request Tracker (RT) before 4.4.9, 5.0.9, and 6.0.2 allows CSV Injection via ticket values when TSV export is used.	2.6	More Details
CVE-2024-54556	This issue was addressed through improved state management. This issue is fixed in iOS 18.1 and iPadOS 18.1. A user may be able to view restricted content from the lock screen.	2.4	More Details
CVE-	A weakness has been identified in technical-laohu mpay up to 1.2.4. The affected element is an unknown function of the component User Center. This manipulation of		

2026-1151	the argument Nickname causes cross site scripting. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.	2.4	More Details
CVE-2025-52661	HCL AION version 2 is affected by a JWT Token Expiry Too Long vulnerability. This may increase the risk of token misuse, potentially resulting in unauthorized access if the token is compromised.	2.4	More Details
CVE-2026-21930	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Filesystems). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 2.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2.3	More Details
CVE-2026-0682	The Church Admin plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.0.28 due to insufficient validation of user-supplied URLs in the 'audio_url' parameter. This makes it possible for authenticated attackers, with Administrator-level access, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	2.2	More Details
CVE-2025-55250	HCL AION version 2 is affected by a Technical Error Disclosure vulnerability. This can expose sensitive technical details, potentially resulting in information disclosure or aiding further attacks.	1.8	More Details
CVE-2026-23634	Pepr is a type safe K8s middleware. Prior to 1.0.5 , Pepr defaults to a cluster-admin RBAC configuration and does not explicitly force or enforce least-privilege guidance for module authors. The default behavior exists to make the “getting started” experience smooth: new users can experiment with Pepr and create resources dynamically without needing to pre-configure RBAC. This vulnerability is fixed in 1.0.5.	0.0	More Details
CVE-2026-22803	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. From 2.49.0 to 2.49.4, the experimental form remote function uses a binary data format containing a representation of submitted form data. A specially-crafted payload can cause the server to allocate a large amount of memory, causing DoS via memory exhaustion. This vulnerability is fixed in 2.49.5.	N/A	More Details
CVE-2025-12533	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-15265	An SSR XSS exists in async hydration when attacker-controlled keys are passed to hydratable. The key is embedded inside a <script> block without HTML-safe escaping, allowing </script> to terminate the script and inject arbitrary JavaScript. This enables remote script execution in users' browsers, with potential for session theft and account compromise. This issue affects Svelte: from 5.46.0 before 5.46.3.	N/A	More Details
CVE-2026-0227	A vulnerability in Palo Alto Networks PAN-OS software enables an unauthenticated attacker to cause a denial of service (DoS) to the firewall. Repeated attempts to trigger this issue results in the firewall entering into maintenance mode.	N/A	More Details
CVE-	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. Prior to 2.49.5, SvelteKit is vulnerable to a server side request forgery (SSRF) and denial of service (DoS) under certain conditions. From 2.44.0 through 2.49.4, the vulnerability results in a DoS when your app has at least one		

2025-67647	prerendered route (export const prerender = true). From 2.19.0 through 2.49.4, the vulnerability results in a DoS when your app has at least one prerendered route and you are using adapter-node without a configured ORIGIN environment variable, and you are not using a reverse proxy that implements Host header validation. This vulnerability is fixed in 2.49.5.	N/A	More Details
CVE-2025-14883	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2025-68016. Reason: This candidate is a reservation duplicate of CVE-2025-68016. Notes: All CVE users should reference CVE-2025-68016 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-21663	HackerOne community member Patrick Lang (7yr) has reported a reflected XSS vulnerability in the banner-acl.php script of Revive Adserver. An attacker can craft a specific URL that includes an HTML payload in a parameter. If a logged in administrator visits the URL, the HTML is sent to the browser and malicious scripts would be executed.	N/A	More Details
CVE-2026-23519	RustCrypto CMOV provides conditional move CPU intrinsics which are guaranteed on major platforms to execute in constant-time and not be rewritten as branches by the compiler. Prior to 0.4.4, the thumbv6m-none-eabi (Cortex M0, M0+ and M1) compiler emits non-constant time assembly when using cmovnz (portable version). This vulnerability is fixed in 0.4.4.	N/A	More Details
CVE-2026-21664	HackerOne community member Huynh Pham Thanh Luc (nigh7c0r3) has reported a reflected XSS vulnerability in the afr.php delivery script of Revive Adserver. An attacker can craft a specific URL that includes an HTML payload in a parameter. If a logged in administrator visits the URL, the HTML is sent to the browser and malicious scripts would be executed.	N/A	More Details
CVE-2025-13845	CWE-416: Use After Free vulnerability that could cause remote code execution when the end user imports the malicious project file (SSD file) into Rapsody.	N/A	More Details
CVE-2026-21642	HackerOne community member Patrick Lang (7yr) has reported a reflected XSS vulnerability in the `banner-acl.php` and `channel-acl.php` scripts of Revive Adserver. An attacker can craft a specific URL that includes an HTML payload in a parameter. If a logged in administrator visits the URL, the HTML is sent to the browser and malicious scripts would be executed.	N/A	More Details
CVE-2025-59465	A malformed `HTTP/2 HEADERS` frame with oversized, invalid `HPACK` data can cause Node.js to crash by triggering an unhandled `TLSSocket` error `ECONNRESET`. Instead of safely closing the connection, the process crashes, enabling a remote denial of service. This primarily affects applications that do not attach explicit error handlers to secure sockets, for example: ``` server.on('secureConnection', socket => { socket.on('error', err => { console.log(err) }) }) ```	N/A	More Details
CVE-2026-23622	Easy!Appointments is a self hosted appointment scheduler. In 1.5.2 and earlier, application/core/EA_Security.php::csrf_verify() only enforces CSRF for POST requests and returns early for non-POST methods. Several application endpoints perform state-changing operations while accepting parameters from GET (or $_REQUEST), so an attacker can perform CSRF by forcing a victim's browser to issue a crafted GET request. Impact: creation of admin accounts, modification of admin email/password, and full admin account takeover.	N/A	More Details
CVE-	Typesetter CMS versions up to and including 5.1 contain a reflected cross-site scripting (XSS) vulnerability in the administrative interface within the Tools Status functionality. The path parameter is reflected into the HTML response without proper		More

2025-71165	output encoding in include/admin/Tools/Status.php. An authenticated attacker can supply crafted input containing HTML or JavaScript, resulting in arbitrary script execution in the context of an authenticated user's browser session.	N/A	Details
CVE-2026-22787	html2pdf.js converts any webpage or element into a printable PDF entirely client-side. Prior to 0.14.0, html2pdf.js contains a cross-site scripting (XSS) vulnerability when given a text source rather than an element. This text is not sufficiently sanitized before being attached to the DOM, allowing malicious scripts to be run on the client browser and risking the confidentiality, integrity, and availability of the page's data. This vulnerability has been fixed in html2pdf.js@0.14.0.	N/A	More Details
CVE-2025-15366	The imaplib module, when passed a user-controlled command, can have additional commands injected using newlines. Mitigation rejects commands containing control characters.	N/A	More Details
CVE-2025-14556	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Drupal Flag allows Cross-Site Scripting (XSS).This issue affects Flag: from 7.X-3.0 through 7.X-3.9.	N/A	More Details
CVE-2026-22863	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Before 2.6.0, node:crypto doesn't finalize cipher. The vulnerability allows an attacker to have infinite encryptions. This can lead to naive attempts at brute forcing, as well as more refined attacks with the goal to learn the server secrets. This vulnerability is fixed in 2.6.0.	N/A	More Details
CVE-2026-1012	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-14557	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Drupal Facebook Pixel facebook_pixel allows Stored XSS.This issue affects Facebook Pixel: from 7.X-1.0 through 7.X-1.1.	N/A	More Details
CVE-2025-71164	Typesetter CMS versions up to and including 5.1 contain a reflected cross-site scripting (XSS) vulnerability in the Editing component. The images parameter (submitted as images[] in a POST request) is reflected into an HTML href attribute without proper context-aware output encoding in include/tool/Editing.php. An authenticated attacker with editing privileges can supply a JavaScript pseudo-protocol (e.g., javascript:) to trigger arbitrary JavaScript execution in the context of the victim's browser session.	N/A	More Details
CVE-2025-71166	Typesetter CMS versions up to and including 5.1 contain a reflected cross-site scripting (XSS) vulnerability in the administrative interface within the Tools Status move message handling. The path parameter is reflected into the HTML output without proper output encoding in include/admin/Tools/Status.php. An authenticated attacker can supply crafted input containing HTML or JavaScript, resulting in arbitrary script execution in the context of an authenticated user's browser session.	N/A	More Details
CVE-2026-23746	Entrust Instant Financial Issuance (IFI) On Premise software (formerly referred to as CardWizard) versions 5.x, prior to 6.10.5, and prior to 6.11.1 contain an insecure .NET Remoting exposure in the SmartCardController service (DCG.SmartCardControllerService.exe). The service registers a TCP remoting channel with unsafe formatter/settings that permit untrusted remoting object invocation. A remote, unauthenticated attacker who can reach the remoting port can invoke exposed remoting objects to read arbitrary files from the server and coerce outbound authentication, and may achieve arbitrary file write and remote code execution via known .NET Remoting exploitation techniques. This can lead to disclosure of sensitive installation and service-account data and compromise of the affected host.	N/A	More Details

CVE-2023-7334	Changjetong T+ versions up to and including 16.x contain a .NET deserialization vulnerability in an AjaxPro endpoint that can lead to remote code execution. A remote attacker can send a crafted request to /tplus/ajaxpro/Ufida.T.CodeBehind._PriorityLevel,App_Code.ashx?method=GetStoreWarehouseByStore with a malicious JSON body that leverages deserialization of attacker-controlled .NET types to invoke arbitrary methods such as System.Diagnostics.Process.Start. This can result in execution of arbitrary commands in the context of the T+ application service account. Exploitation evidence was observed by the Shadowserver Foundation on 2023-08-19 (UTC).	N/A	More Details
CVE-2011-10041	Uploadify WordPress plugin versions up to and including 1.0 contain an arbitrary file upload vulnerability in process_upload.php due to missing file type validation. An unauthenticated remote attacker can upload arbitrary files to the affected WordPress site, which may allow remote code execution by uploading executable content to a web-accessible location.	N/A	More Details
CVE-2025-15282	User-controlled data URLs parsed by urllib.request.DataHandler allow injecting headers through newlines in the data URL mediatype.	N/A	More Details
CVE-2025-11468	When folding a long comment in an email header containing exclusively unfoldable characters, the parenthesis would not be preserved. This could be used for injecting headers into email messages where addresses are user-controlled and not sanitized.	N/A	More Details
CVE-2026-1002	The Vert.x Web static handler component cache can be manipulated to deny the access to static files served by the handler using specifically crafted request URI. The issue comes from an improper implementation of the C. rule of section 5.2.4 of RFC3986 and is fixed in Vert.x Core component (used by Vert.x Web): https://github.com/eclipse-vertx/vert.x/pull/5895 Steps to reproduce Given a file served by the static handler, craft an URI that introduces a string like bar%2F..%2F after the last / char to deny the access to the URI with an HTTP 404 response. For example https://example.com/foo/index.html can be denied with https://example.com/foo/bar%2F..%2Findex.html Mitgation Disabling Static Handler cache fixes the issue. StaticHandler staticHandler = StaticHandler.create().setCachingEnabled(false);	N/A	More Details
CVE-2026-0601	A reflected cross-site scripting vulnerability exists in Nexus Repository 3 that allows unauthenticated attackers to execute arbitrary JavaScript in a victim's browser through a specially crafted request requiring user interaction.	N/A	More Details
CVE-2025-58741	Insufficiently Protected Credentials vulnerability in the Credential Field of Milner ImageDirector Capture allows retrieval of credential material and enables database access.This issue affects ImageDirector Capture: from 7.0.9 through 7.6.3.25808.	N/A	More Details
CVE-2025-13844	CWE-415: Double Free vulnerability exists that could cause heap memory corruption when the end user imports a malicious project file (SSD file) shared by the attacker into Rapsody.	N/A	More Details
CVE-2026-23581	Rejected reason: Not used	N/A	More Details
CVE-2026-23582	Rejected reason: Not used	N/A	More Details
CVE-	A flaw in Node.js's Permissions model allows attackers to bypass `--allow-fs-read` and `--allow-fs-write` restrictions using crafted relative symlink paths. By chaining directories and symlinks, a script granted access only to the current directory can		More

2025-55130	escape the allowed path and read sensitive files. This breaks the expected isolation guarantees and enables arbitrary file read/write, leading to potential system compromise. This vulnerability affects users of the permission model on Node.js v20, v22, v24, and v25.	N/A	Details
CVE-2025-66803	Race condition in the turbo-frame element handler in Hotwired Turbo before 8.0.x causes logout operations to fail when delayed frame responses reapply session cookies after logout. This can be exploited by remote attackers via selective network delays (e.g. delaying requests based on sequence or timing) or by physically proximate attackers when the race condition occurs naturally on shared computers.	N/A	More Details
CVE-2026-23576	Rejected reason: Not used	N/A	More Details
CVE-2025-58743	Use of a Broken or Risky Cryptographic Algorithm (DES) vulnerability in the Password class in C2SConnections.dll in Milner ImageDirector Capture on Windows allows Encryption Brute Forcing to obtain database credentials.This issue affects ImageDirector Capture: from 7.0.9.0 before 7.6.3.25808.	N/A	More Details
CVE-2026-1245	A code injection vulnerability in the binary-parser library prior to version 2.3.0 allows arbitrary JavaScript code execution when untrusted values are used in parser field names or encoding parameters. The library directly interpolates these values into dynamically generated code without sanitization, enabling attackers to execute arbitrary code in the context of the Node.js process.	N/A	More Details
CVE-2026-0622	Open 5GS WebUI uses a hard-coded JWT signing key (change-me) whenever the environment variable JWT_SECRET_KEY is unset	N/A	More Details
CVE-2025-66692	A buffer over-read in the PublicKey::verify() method of Binance - Trust Wallet Core before commit 5668c67 allows attackers to cause a Denial of Service (DoS) via a crafted input.	N/A	More Details
CVE-2025-58744	Use of Default Credentials, Hard-coded Credentials vulnerability in C2SGlobalSettings.dll in Milner ImageDirector Capture on Windows allows decryption of document archive files using credentials decrypted with hard-coded application encryption key. This issue affects ImageDirector Capture: from 7.0.9.0 before 7.6.3.25808.	N/A	More Details
CVE-2026-23575	Rejected reason: Not used	N/A	More Details
CVE-2025-55131	A flaw in Node.js's buffer allocation logic can expose uninitialized memory when allocations are interrupted, when using the `vm` module with the timeout option. Under specific timing conditions, buffers allocated with `Buffer.alloc` and other `TypedArray` instances like `Uint8Array` may contain leftover data from previous operations, allowing in-process secrets like tokens or passwords to leak or causing data corruption. While exploitation typically requires precise timing or in-process code execution, it can become remotely exploitable when untrusted input influences workload and timeouts, leading to potential confidentiality and integrity impact.	N/A	More Details
CVE-2025-67261	Abacre Retail Point of Sale 14.0.0.396 is vulnerable to content-based blind SQL injection. The vulnerability exists in the Search function of the Orders page.	N/A	More Details
CVE-2026-0672	When using http.cookies.Morsel, user-controlled cookie values and parameters can allow injecting HTTP headers into messages. Patch rejects all control characters within cookie names, values, and parameters.	N/A	More Details

CVE-2025-63648	A NULL pointer dereference in the dacp_reply_playqueueedit_move function (src/httpd_dacp.c) of owntone-server commit b7e385f allows attackers to cause a Denial of Service (DoS) via sending a crafted DACP request to the server.	N/A	More Details
CVE-2025-55132	A flaw in Node.js's permission model allows a file's access and modification timestamps to be changed via `futimes()` even when the process has only read permissions. Unlike `utimes()`, `futimes()` does not apply the expected write-permission checks, which means file metadata can be modified in read-only directories. This behavior could be used to alter timestamps in ways that obscure activity, reducing the reliability of logs. This vulnerability affects users of the permission model on Node.js v20, v22, v24, and v25.	N/A	More Details
CVE-2025-57155	NULL pointer dereference in the daap_reply_groups function in src/httpd_daap.c in owntone-server through commit 5e6f19a (newer commit after version 28.2) allows remote attackers to cause a Denial of Service.	N/A	More Details
CVE-2026-0865	User-controlled header names and values containing newlines can allow injecting HTTP headers.	N/A	More Details
CVE-2025-57156	NULL pointer dereference in the dacp_reply_playqueueedit_clear function in src/httpd_dacp.c in owntone-server through commit 6d604a1 (newer commit after version 28.12) allows remote attackers to cause a Denial of Service (crash).	N/A	More Details
CVE-2025-63647	A NULL pointer dereference in the parse_meta function (src/httpd_daap.c) of owntone-server commit 334beb allows attackers to cause a Denial of Service (DoS) via sending a crafted DAAP request to the server.	N/A	More Details
CVE-2025-59466	We have identified a bug in Node.js error handling where "Maximum call stack size exceeded" errors become uncatchable when `async_hooks.createHook()` is enabled. Instead of reaching `process.on('uncaughtException')`, the process terminates, making the crash unrecoverable. Applications that rely on `AsyncLocalStorage` (v22, v20) or `async_hooks.createHook()` (v24, v22, v20) become vulnerable to denial-of-service crashes triggered by deep recursion under specific conditions.	N/A	More Details
CVE-2025-66902	An input validation issue in in Pithikos websocket-server v.0.6.4 allows a remote attacker to obtain sensitive information or cause unexpected server behavior via the websocket_server/websocket_server.py, WebSocketServer._message_received components.	N/A	More Details
CVE-2026-21636	A flaw in Node.js's permission model allows Unix Domain Socket (UDS) connections to bypass network restrictions when `--permission` is enabled. Even without `--allow-net`, attacker-controlled inputs (such as URLs or socketPath options) can connect to arbitrary local sockets via net, tls, or undici/fetch. This breaks the intended security boundary of the permission model and enables access to privileged local services, potentially leading to privilege escalation, data exposure, or local code execution. * The issue affects users of the Node.js permission model on version v25. In the moment of this vulnerability, network permissions (`--allow-net`) are still in the experimental phase.	N/A	More Details
CVE-2025-9014	A Null Pointer Dereference vulnerability exists in the referer header check of the web portal of TP-Link TL-WR841N v14, caused by improper input validation. A remote, unauthenticated attacker can exploit this flaw and cause Denial of Service on the web portal service.This issue affects TL-WR841N v14: before 250908.	N/A	More Details
CVE-2026-23580	Rejected reason: Not used	N/A	More Details

CVE-2026-21641	HackerOne community member Jad Ghamloush (0xjad) has reported an authorization bypass vulnerability in the `tracker-delete.php` script of Revive Adserver. Users with permissions to delete trackers are mistakenly allowed to delete trackers owned by other accounts.	N/A	More Details
CVE-2026-21640	HackerOne community member Faraz Ahmed (PakCyberbot) has reported a format string injection in the Revive Adserver settings. When specific character combinations are used in a setting, the admin user console could be disabled due to a fatal PHP error.	N/A	More Details
CVE-2025-59464	A memory leak in Node.js's OpenSSL integration occurs when converting `X.509` certificate fields to UTF-8 without freeing the allocated buffer. When applications call `socket.getPeerCertificate(true)`, each certificate field leaks memory, allowing remote clients to trigger steady memory growth through repeated TLS connections. Over time this can lead to resource exhaustion and denial of service.	N/A	More Details
CVE-2025-56353	In tinyMQTT commit 6226ade15bd4f97be2d196352e64dd10937c1962 (2024-02-18), a memory leak occurs due to the broker's failure to validate or reject malformed UTF-8 strings in topic filters. An attacker can exploit this by sending repeated subscription requests with arbitrarily large or invalid filter payloads. Each request causes memory to be allocated for the malformed topic filter, but the broker does not free the associated memory, leading to unbounded heap growth and potential denial of service under sustained attack.	N/A	More Details
CVE-2025-64087	A Server-Side Template Injection (SSTI) vulnerability in the FreeMarker component of opensagres XDocReport v1.0.0 to v2.1.0 allows attackers to execute arbitrary code via injecting crafted template expressions.	N/A	More Details
CVE-2025-65482	An XML External Entity (XXE) vulnerability in opensagres XDocReport v0.9.2 to v2.0.3 allows attackers to execute arbitrary code via uploading a crafted .docx file.	N/A	More Details
CVE-2025-67078	Cross site scripting (XSS) vulnerability in Omnispace Agora Project before 25.10 allowing attackers to execute arbitrary code via the notify parameter of the file controller used to display errors.	N/A	More Details
CVE-2025-67824	The WorklogPRO - Jira Timesheets plugin in the Jira Data Center before 4.24.1-jira9, 4.24.1-jira10, and 4.24.1-jira11 allows attackers to inject arbitrary HTML or JavaScript via XSS. This is exploited via a crafted payload placed in the name of a filter. This code is executed in the browser when the user attempts to create a timesheet with the filter timesheet type on the custom timesheet dialog because the filter name is not properly sanitized during the action.	N/A	More Details
CVE-2026-0600	Server-Side Request Forgery (SSRF) vulnerability in Sonatype Nexus Repository 3 versions 3.0.0 and later allows authenticated administrators to configure proxy repositories with URLs that can access unintended network destinations, potentially including cloud metadata services and internal network resources. A workaround configuration is available starting in version 3.88.0, but the product remains vulnerable by default.	N/A	More Details
CVE-2025-55423	ipTIME routers A2003NS-MU 10.00.6 to 12.16.2 , N600 10.00.8 to 12.16.2, A604-V3 10.01.6 to 10.07.2, A6ns-M 10.01.6 to 14.19.4 , V508 10.02.2 to 10.06.4, N704QCA 10.02.4 to 12.16.2, A8ns-M 10.03.2 to 14.19.4, A304 10.05.4 to 10.07.4, A3004NS-M,A5004NS-M,A9004M 10.05.4 to 14.19.4, N702R 10.05.8 to 10.06.8, A604M 10.06.4 to 10.07.2, A804NS-MU 10.06.4 to 12.10.2, N804R 10.06.4 to 12.16.2, A7004M,A8004T 10.06.8 to 14.19.4, A604G-MU 10.07.4 to 12.16.2, A3008-MU 10.08.4 to 14.19.4, A2004MU and A2004NS-MU 10.08.6 to 12.17.0, A604-V5,A604R, N702E 10.09.2 to 12.16.2, N2V 10.09.2 to 12.16.8, N604E 10.09.2 to 14.19.4, N104E 10.09.4 to 12.15.2, A8004ITL 11.00.4 to 14.19.4, N102E 11.00.8 to 12.15.2, N1V	N/A	More Details

	11.01.2 to 12.07.6, N102i 11.01.2 to 12.15.2, T5004 11.96.4 to 14.19.4, N602E 11.96.6 to 12.16.8, AX8004BCM and A8004T-XR 11.97.2 to 14.19.4, A9004M-X2, T5008 11.98.2 to 14.19.4, N704E 11.98.4 to 12.16.2, A8004BCM 11.99.1 to 12.16.2, AX3004ITL 12.01.2 to 14.19.4 and A604G-skylife 12.02.4 to 12.12 were discovered to contain an OS command injection vulnerability via the function upnp_relay().		
CVE-2026-23579	Rejected reason: Not used	N/A	More Details
CVE-2026-23574	Rejected reason: Not used	N/A	More Details
CVE-2026-23578	Rejected reason: Not used	N/A	More Details
CVE-2026-23577	Rejected reason: Not used	N/A	More Details
CVE-2026-21637	A flaw in Node.js TLS error handling allows remote attackers to crash or exhaust resources of a TLS server when `pskCallback` or `ALPNCallback` are in use. Synchronous exceptions thrown during these callbacks bypass standard TLS error handling paths (tlsClientError and error), causing either immediate process termination or silent file descriptor leaks that eventually lead to denial of service. Because these callbacks process attacker-controlled input during the TLS handshake, a remote client can repeatedly trigger the issue. This vulnerability affects TLS servers using PSK or ALPN callbacks across Node.js versions where these callbacks throw without being safely wrapped.	N/A	More Details
CVE-2026-22779	BlackSheep is an asynchronous web framework to build event based web applications with Python. Prior to 2.4.6, the HTTP Client implementation in BlackSheep is vulnerable to CRLF injection. Missing headers validation makes it possible for an attacker to modify the HTTP requests (e.g. insert a new header) or even create a new HTTP request. Exploitation requires developers to pass unsanitized user input directly into headers.The server part is not affected because BlackSheep delegates to an underlying ASGI server handling of response headers. This vulnerability is fixed in 2.4.6.	N/A	More Details
CVE-2025-15367	The poplib module, when passed a user-controlled command, can have additional commands injected using newlines. Mitigation rejects commands containing control characters.	N/A	More Details
CVE-2025-58742	Insufficiently Protected Credentials, Improper Restriction of Communication Channel to Intended Endpoints vulnerability in the Connection Settings dialog in Milner ImageDirector Capture on Windows allows Adversary in the Middle (AiTM) by modifying the 'Server' field to redirect client authentication.This issue affects ImageDirector Capture: from 7.0.9 before 7.6.3.25808.	N/A	More Details
CVE-2025-58740	The use of a hard-coded encryption key in calls to the Password function in C2SGlobalSettings.dll in Milner ImageDirector Capture on Windows allows a local attacker to decrypt database credentials by reading the cryptographic key from the executable. This issue affects ImageDirector Capture: from 7.0.9 before 7.6.3.25808.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: drm/msm: adreno: fix deferencing ifpc_reglist when not declared On plaforms with an a7xx GPU not supporting IFPC, the ifpc_reglist if still deferenced in a7xx_patch_pwrup_reglist()		

CVE-2025-71103	which causes a kernel crash: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000008 ... pc : a6xx_hw_init+0x155c/0x1e4c [msm] lr : a6xx_hw_init+0x9a8/0x1e4c [msm] ... Call trace: a6xx_hw_init+0x155c/0x1e4c [msm] (P) msm_gpu_hw_init+0x58/0x88 [msm] adreno_load_gpu+0x94/0x1fc [msm] msm_open+0xe4/0xf4 [msm] drm_file_alloc+0x1a0/0x2e4 [drm] drm_client_init+0x7c/0x104 [drm] drm_fbdev_client_setup+0x94/0xcf0 [drm_client_lib] drm_client_setup+0xb4/0xd8 [drm_client_lib] msm_drm_kms_post_init+0x2c/0x3c [msm] msm_drm_init+0x1a4/0x228 [msm] msm_drm_bind+0x30/0x3c [msm] ... Check the validity of ifpc_reglist before deferencing the table to setup the register values. Patchwork: https://patchwork.freedesktop.org/patch/688944/	N/A	More Details
CVE-2026-22708	Cursor is a code editor built for programming with AI. Prior to 2.3, hen the Cursor Agent is running in Auto-Run Mode with Allowlist mode enabled, certain shell built-ins can still be executed without appearing in the allowlist and without requiring user approval. This allows an attacker via indirect or direct prompt injection to poison the shell environment by setting, modifying, or removing environment variables that influence trusted commands. This vulnerability is fixed in 2.3.	N/A	More Details
CVE-2026-23528	Dask distributed is a distributed task scheduler for Dask. Prior to 2026.1.0, when Jupyter Lab, jupyter-server-proxy, and Dask distributed are all run together, it is possible to craft a URL which will result in code being executed by Jupyter due to a cross-side-scripting (XSS) bug in the Dask dashboard. It is possible for attackers to craft a phishing URL that assumes Jupyter Lab and Dask may be running on localhost and using default ports. If a user clicks on the malicious link it will open an error page in the Dask Dashboard via the Jupyter Lab proxy which will cause code to be executed by the default Jupyter Python kernel. This vulnerability is fixed in 2026.1.0.	N/A	More Details
CVE-2026-21624	Lack of input filterung leads to a persistent XSS vulnerability in the user avatar text handling of the Easy Discuss component for Joomla.	N/A	More Details
CVE-2026-21625	User provided uploads to the Easy Discuss component for Joomla aren't properly validated. Uploads are purely checked by file extensions, no mime type checks are happening.	N/A	More Details
CVE-2025-29943	Write what were condition within AMD CPUs may allow an admin-privileged attacker to modify the configuration of the CPU pipeline potentially resulting in the corruption of the stack pointer inside an SEV-SNP guest.	N/A	More Details
CVE-2025-71123	In the Linux kernel, the following vulnerability has been resolved: ext4: fix string copying in parse_apply_sb_mount_options() strscpy_pad() can't be used to copy a non-NUL-term string into a NUL-term string of possibly bigger size. Commit 0efc5990bca5 ("string.h: Introduce memtostr() and memtostr_pad()") provides additional information in that regard. So if this happens, the following warning is observed: strnlen: detected buffer overflow: 65 byte read of buffer size 64 WARNING: CPU: 0 PID: 28655 at lib/string_helpers.c:1032 __fortify_report+0x96/0xc0 lib/string_helpers.c:1032 Modules linked in: CPU: 0 UID: 0 PID: 28655 Comm: syz-executor.3 Not tainted 6.12.54-syzkaller-00144-g5f0270f1ba00 #0 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 RIP: 0010:__fortify_report+0x96/0xc0 lib/string_helpers.c:1032 Call Trace: <TASK> __fortify_panic+0x1f/0x30 lib/string_helpers.c:1039 strnlen include/linux/fortify-string.h:235 [inline] sized_strscpy include/linux/fortify-string.h:309 [inline] parse_apply_sb_mount_options fs/ext4/super.c:2504 [inline] __ext4_fill_super fs/ext4/super.c:5261 [inline] ext4_fill_super+0x3c35/0xad00 fs/ext4/super.c:5706 get_tree_bdev_flags+0x387/0x620 fs/super.c:1636 vfs_get_tree+0x93/0x380 fs/super.c:1814 do_new_mount fs/namespace.c:3553 [inline] path_mount+0x6ae/0x1f70 fs/namespace.c:3880 do_mount fs/namespace.c:3893	N/A	More Details

	[inline] __do_sys_mount fs/namespace.c:4103 [inline] __se_sys_mount fs/namespace.c:4080 [inline] __x64_sys_mount+0x280/0x300 fs/namespace.c:4080 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0x64/0x140 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x76/0x7e Since userspace is expected to provide s_mount_opts field to be at most 63 characters long with the ending byte being NUL-term, use a 64-byte buffer which matches the size of s_mount_opts, so that strscpy_pad() does its job properly. Return with error if the user still managed to provide a non-NUL-term string here. Found by Linux Verification Center (linuxtesting.org) with Syzkaller.		
CVE-2025-71122	In the Linux kernel, the following vulnerability has been resolved: iommufd/selftest: Check for overflow in IOMMU_TEST_OP_ADD_RESERVED syzkaller found it could overflow math in the test infrastructure and cause a WARN_ON by corrupting the reserved interval tree. This only effects test kernels with CONFIG_IOMMUFD_TEST. Validate the user input length in the test ioctl.	N/A	More Details
CVE-2026-23644	esm.sh is a no-build content delivery network (CDN) for web development. Prior to Go pseeudoversion 0.0.0-20260116051925-c62ab83c589e, the software has a path traversal vulnerability due to an incomplete fix. `path.Clean` normalizes a path but does not prevent absolute paths in a malicious tar file. Commit https://github.com/esm-dev/esm.sh/commit/9d77b88c320733ff6689d938d85d246a3af9af16, corresponding to pseudoversion 0.0.0-20260116051925-c62ab83c589e, fixes this issue.	N/A	More Details
CVE-2026-22782	RustFS is a distributed object storage system built in Rust. From >= 1.0.0-alpha.1 to 1.0.0-alpha.79, invalid RPC signatures cause the server to log the shared HMAC secret (and expected signature), which exposes the secret to log readers and enables forged RPC calls. In crates/ecstore/src/rpc/http_auth.rs, the invalid signature branch logs sensitive data. This log line includes secret and expected_signature, both derived from the shared HMAC key. Any invalidly signed request triggers this path. The function is reachable from RPC and admin request handlers. This vulnerability is fixed in 1.0.0-alpha.80.	N/A	More Details
CVE-2025-71121	In the Linux kernel, the following vulnerability has been resolved: parisc: Do not reprogram affinitiy on ASP chip The ASP chip is a very old variant of the GSP chip and is used e.g. in HP 730 workstations. When trying to reprogram the affinity it will crash with a HPMC as the relevant registers don't seem to be at the usual location. Let's avoid the crash by checking the sversion. Also note, that reprogramming isn't necessary either, as the HP730 is a just a single-CPU machine.	N/A	More Details
CVE-2026-23534	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.21.0, a client-side heap buffer overflow occurs in the ClearCodec bands decode path when crafted band coordinates allow writes past the end of the destination surface buffer. A malicious server can trigger a client-side heap buffer overflow, causing a crash (DoS) and potential heap corruption with code-execution risk depending on allocator behavior and surrounding heap layout. Version 3.21.0 contains a patch for the issue.	N/A	More Details
CVE-2025-71120	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: svcauth_gss: avoid NULL deref on zero length gss_token in gss_read_proxy_verf A zero length gss_token results in pages == 0 and in_token->pages[0] is NULL. The code unconditionally evaluates page_address(in_token->pages[0]) for the initial memcpy, which can dereference NULL even when the copy length is 0. Guard the first memcpy so it only runs when length > 0.	N/A	More Details
CVE-2025-14338	Polkit authentication dis isabled by default and a race condition in the Polkit authorization check in versions before v0.69.0 can lead to the same issues as in CVE-2025-66005.	N/A	More Details

CVE-2026-0897	Allocation of Resources Without Limits or Throttling in the HDF5 weight loading component in Google Keras 3.0.0 through 3.13.0 on all platforms allows a remote attacker to cause a Denial of Service (DoS) through memory exhaustion and a crash of the Python interpreter via a crafted .keras archive containing a valid model.weights.h5 file whose dataset declares an extremely large shape.	N/A	More Details
CVE-2026-0629	Authentication bypass in the password recovery feature of the local web interface across multiple VIGI camera models allows an attacker on the LAN to reset the admin password without verification by manipulating client-side state. Attackers can gain full administrative access to the device, compromising configuration and network security.	N/A	More Details
CVE-2025-71119	In the Linux kernel, the following vulnerability has been resolved: powerpc/kexec: Enable SMT before waking offline CPUs If SMT is disabled or a partial SMT state is enabled, when a new kernel image is loaded for kexec, on reboot the following warning is observed: kexec: Waking offline cpu 228. WARNING: CPU: 0 PID: 9062 at arch/powerpc/kexec/core_64.c:223 kexec_prepare_cpus+0x1b0/0x1bc [snip] NIP kexec_prepare_cpus+0x1b0/0x1bc LR kexec_prepare_cpus+0x1a0/0x1bc Call Trace: kexec_prepare_cpus+0x1a0/0x1bc (unreliable) default_machine_kexec+0x160/0x19c machine_kexec+0x80/0x88 kernel_kexec+0xd0/0x118 __do_sys_reboot+0x210/0x2c4 system_call_exception+0x124/0x320 system_call_vectored_common+0x15c/0x2ec This occurs as add_cpu() fails due to cpu_bootable() returning false for CPUs that fail the cpu_smt_thread_allowed() check or non primary threads if SMT is disabled. Fix the issue by enabling SMT and resetting the number of SMT threads to the number of threads per core, before attempting to wake up all present CPUs.	N/A	More Details
CVE-2025-71118	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Avoid walking the Namespace if start_node is NULL Although commit 0c9992315e73 ("ACPICA: Avoid walking the ACPI Namespace if it is not there") fixed the situation when both start_node and acpi_gbl_root_node are NULL, the Linux kernel mainline now still crashed on Honor Magicbook 14 Pro [1]. That happens due to the access to the member of parent_node in acpi_ns_get_next_node(). The NULL pointer dereference will always happen, no matter whether or not the start_node is equal to ACPI_ROOT_OBJECT, so move the check of start_node being NULL out of the if block. Unfortunately, all the attempts to contact Honor have failed, they refused to provide any technical support for Linux. The bad DSDT table's dump could be found on GitHub [2]. DMI: HONOR FMB-P/FMB-P-PCB, BIOS 1.13 05/08/2025 [rjw: Subject adjustment, changelog edits]	N/A	More Details
CVE-2025-71117	In the Linux kernel, the following vulnerability has been resolved: block: Remove queue freezing from several sysfs store callbacks Freezing the request queue from inside sysfs store callbacks may cause a deadlock in combination with the dm-multipath driver and the queue_if_no_path option. Additionally, freezing the request queue slows down system boot on systems where sysfs attributes are set synchronously. Fix this by removing the blk_mq_freeze_queue() / blk_mq_unfreeze_queue() calls from the store callbacks that do not strictly need these callbacks. Add the __data_racy annotation to request_queue.rq_timeout to suppress KCSAN data race reports about the rq_timeout reads. This patch may cause a small delay in applying the new settings. For all the attributes affected by this patch, I/O will complete correctly whether the old or the new value of the attribute is used. This patch affects the following sysfs attributes: * io_poll_delay * io_timeout * nomerges * read_ahead_kb * rq_affinity Here is an example of a deadlock triggered by running test srp/002 if this patch is not applied: task:multipathd Call Trace: <TASK> __schedule+0x8c1/0x1bf0 schedule+0xdd/0x270 schedule_preempt_disabled+0x1c/0x30 __mutex_lock+0xb89/0x1650 mutex_lock_nested+0x1f/0x30 dm_table_set_restrictions+0x823/0xdf0 __bind+0x166/0x590 dm_swap_table+0x2a7/0x490 do_resume+0x1b1/0x610 dev_suspend+0x55/0x1a0	N/A	More Details

	ctl_ioctl+0x3a5/0x7e0 dm_ctl_ioctl+0x12/0x20 __x64_sys_ioctl+0x127/0x1a0 x64_sys_call+0xe2b/0x17d0 do_syscall_64+0x96/0x3a0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 </TASK> task:(udev-worker) Call Trace: <TASK> __schedule+0x8c1/0x1bf0 schedule+0xdd/0x270 blk_mq_freeze_queue_wait+0xf2/0x140 blk_mq_freeze_queue_nomemsave+0x23/0x30 queue_ra_store+0x14e/0x290 queue_attr_store+0x23e/0x2c0 sysfs_kf_write+0xde/0x140 kernfs_fop_write_iter+0x3b2/0x630 vfs_write+0x4fd/0x1390 ksys_write+0xfd/0x230 __x64_sys_write+0x76/0xc0 x64_sys_call+0x276/0x17d0 do_syscall_64+0x96/0x3a0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 </TASK>		
CVE-2026-21623	Lack of input filterung leads to a persistent XSS vulnerability in the forum post handling of the Easy Discuss component for Joomla.	N/A	More Details
CVE-2025-71124	In the Linux kernel, the following vulnerability has been resolved: drm/msm/a6xx: move preempt_prepare_postamble after error check Move the call to preempt_prepare_postamble() after verifying that preempt_postamble_ptr is valid. If preempt_postamble_ptr is NULL, dereferencing it in preempt_prepare_postamble() would lead to a crash. This change avoids calling the preparation function when the postamble allocation has failed, preventing potential NULL pointer dereference and ensuring proper error handling. Patchwork: https://patchwork.freedesktop.org/patch/687659/	N/A	More Details
CVE-2026-0823	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-71125	In the Linux kernel, the following vulnerability has been resolved: tracing: Do not register unsupported perf events Synthetic events currently do not have a function to register perf events. This leads to calling the tracepoint register functions with a NULL function pointer which triggers: ------------[cut here]------------ WARNING: kernel/tracepoint.c:175 at tracepoint_add_func+0x357/0x370, CPU#2: perf/2272 Modules linked in: kvm_intel kvm irqbypass CPU: 2 UID: 0 PID: 2272 Comm: perf Not tainted 6.18.0-ftest-11964-ge022764176fc-dirty #323 PREEMPTLAZY Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.17.0-debian-1.17.0-1 04/01/2014 RIP: 0010:tracepoint_add_func+0x357/0x370 Code: 28 9c e8 4c 0b f5 ff eb 0f 4c 89 f7 48 c7 c6 80 4d 28 9c e8 ab 89 f4 ff 31 c0 5b 41 5c 41 5d 41 5e 41 5f 5d c3 cc cc cc cc cc <0f> 0b 49 c7 c6 ea ff ff ff e9 ee fe ff ff 0f 0b e9 f9 fe ff ff 0f RSP: 0018:ffffabc0c44d3c40 EFLAGS: 00010246 RAX: 0000000000000001 RBX: ffff9380aa9e4060 RCX: 0000000000000000 RDX: 000000000000000a RSI: ffffffff9e1d4a98 RDI: ffff937fcf5fd6c8 RBP: 0000000000000001 R08: 0000000000000007 R09: ffff937fcf5fc780 R10: 0000000000000003 R11: ffffffff9c193910 R12: 000000000000000a R13: ffffffff9e1e5888 R14: 0000000000000000 R15: ffffabc0c44d3c78 FS: 00007f6202f5f340(0000) GS:ffff93819f00f000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000055d3162281a8 CR3: 0000000106a56003 CR4: 0000000000172ef0 Call Trace: <TASK> tracepoint_probe_register+0x5d/0x90 synth_event_reg+0x3c/0x60 perf_trace_event_init+0x204/0x340 perf_trace_init+0x85/0xd0 perf_tp_event_init+0x2e/0x50 perf_try_init_event+0x6f/0x230 ? perf_event_alloc+0x4bb/0xdc0 perf_event_alloc+0x65a/0xdc0 __se_sys_perf_event_open+0x290/0x9f0 do_syscall_64+0x93/0x7b0 ? entry_SYSCALL_64_after_hwframe+0x76/0x7e ? trace_hardirqs_off+0x53/0xc0 entry_SYSCALL_64_after_hwframe+0x76/0x7e Instead, have the code return -ENODEV, which doesn't warn and has perf error out with: # perf record -e synthetic:futex_wait Error: The sys_perf_event_open() syscall returned with 19 (No such device) for event (synthetic:futex_wait). "dmesg | grep -i perf" may provide additional information. Ideally perf should support synthetic	N/A	More Details

	events, but for now just fix the warning. The support can come later.		
CVE-2026-23532	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.21.0, a client-side heap buffer overflow occurs in the FreeRDP client's `gdi_SurfaceToSurface` path due to a mismatch between destination rectangle clamping and the actual copy size. A malicious server can trigger a client-side heap buffer overflow, causing a crash (DoS) and potential heap corruption with code-execution risk depending on allocator behavior and surrounding heap layout. Version 3.21.0 contains a patch for the issue.	N/A	More Details
CVE-2026-23531	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.21.0, in ClearCodec, when `glyphData` is present, `clear_decompress` calls `freerdp_image_copy_no_overlap` without validating the destination rectangle, allowing an out-of-bounds read/write via crafted RDPGFX surface updates. A malicious server can trigger a client-side heap buffer overflow, causing a crash (DoS) and potential heap corruption with code-execution risk depending on allocator behavior and surrounding heap layout. Version 3.21.0 contains a patch for the issue.	N/A	More Details
CVE-2026-23530	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.21.0,`freerdp_bitmap_decompress_planar` does not validate `nSrcWidth`/`nSrcHeight` against `planar->maxWidth`/`maxHeight` before RLE decode. A malicious server can trigger a client-side heap buffer overflow, causing a crash (DoS) and potential heap corruption with code-execution risk depending on allocator behavior and surrounding heap layout. Version 3.21.0 contains a patch for the issue.	N/A	More Details
CVE-2026-22876	Path Traversal vulnerability exists in multiple Network Cameras TRIFORA 3 series provided by TOA Corporation. If this vulnerability is exploited, arbitrary files on the affected product may be retrieved by a logged-in user with the low("monitoring user") or higher privilege.	N/A	More Details
CVE-2025-71133	In the Linux kernel, the following vulnerability has been resolved: RDMA/irdma: avoid invalid read in irdma_net_event irdma_net_event() should not dereference anything from "neigh" (alias "ptr") until it has checked that the event is NETEVENT_NEIGH_UPDATE. Other events come with different structures pointed to by "ptr" and they may be smaller than struct neighbour. Move the read of neigh->dev under the NETEVENT_NEIGH_UPDATE case. The bug is mostly harmless, but it triggers KASAN on debug kernels: BUG: KASAN: stack-out-of-bounds in irdma_net_event+0x32e/0x3b0 [irdma] Read of size 8 at addr ffffc900075e07f0 by task kworker/27:2/542554 CPU: 27 PID: 542554 Comm: kworker/27:2 Kdump: loaded Not tainted 5.14.0-630.el9.x86_64+debug #1 Hardware name: [...] Workqueue: events rt6_probe_deferred Call Trace: <IRQ> dump_stack_lvl+0x60/0xb0 print_address_description.constprop.0+0x2c/0x3f0 print_report+0xb4/0x270 kasan_report+0x92/0xc0 irdma_net_event+0x32e/0x3b0 [irdma] notifier_call_chain+0x9e/0x180 atomic_notifier_call_chain+0x5c/0x110 rt6_do_redirect+0xb91/0x1080 tcp_v6_err+0xe9b/0x13e0 icmpv6_notify+0x2b2/0x630 ndisc_redirect_rcv+0x328/0x530 icmpv6_rcv+0xc16/0x1360 ip6_protocol_deliver_rcu+0xb84/0x12e0 ip6_input_finish+0x117/0x240 ip6_input+0xc4/0x370 ipv6_rcv+0x420/0x7d0 __netif_receive_skb_one_core+0x118/0x1b0 process_backlog+0xd1/0x5d0 __napi_poll.constprop.0+0xa3/0x440 net_rx_action+0x78a/0xba0 handle_softirqs+0x2d4/0x9c0 do_softirq+0xad/0xe0 </IRQ>	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: smc91x: fix broken irq-context in PREEMPT_RT When smc91x.c is built with PREEMPT_RT, the following splat occurs in FVP_RevC: [13.055000] smc91x LNRO0003:00 eth0: link up, 10Mbps, half-duplex, lpa 0x0000 [13.062137] BUG: workqueue leaked atomic, lock or RCU: kworker/2:1[106] [13.062137] preempt=0x00000000 lock=0->0 RCU=0->1 workfn=mld_ifc_work [13.062266] C ** replaying previous printk message ** [		

CVE-2025-71132	13.062266] CPU: 2 UID: 0 PID: 106 Comm: kworker/2:1 Not tainted 6.18.0-dirty #179 PREEMPT_{RT,(full)} [13.062353] Hardware name: , BIOS [13.062382] Workqueue: mld mld_ifc_work [13.062469] Call trace: [13.062494] show_stack+0x24/0x40 (C) [13.062602] __dump_stack+0x28/0x48 [13.062710] dump_stack_lvl+0x7c/0xb0 [13.062818] dump_stack+0x18/0x34 [13.062926] process_scheduled_works+0x294/0x450 [13.063043] worker_thread+0x260/0x3d8 [13.063124] kthread+0x1c4/0x228 [13.063235] ret_from_fork+0x10/0x20 This happens because smc_special_trylock() disables IRQs even on PREEMPT_RT, but smc_special_unlock() does not restore IRQs on PREEMPT_RT. The reason is that smc_special_unlock() calls spin_unlock_irqrestore(), and rcu_read_unlock_bh() in __dev_queue_xmit() cannot invoke rcu_read_unlock() through __local_bh_enable_ip() when current->softirq_disable_cnt becomes zero. To address this issue, replace smc_special_trylock() with spin_trylock_irqsave().	N/A	More Details
CVE-2025-71131	In the Linux kernel, the following vulnerability has been resolved: crypto: seqiv - Do not use req->iv after crypto_aead_encrypt As soon as crypto_aead_encrypt is called, the underlying request may be freed by an asynchronous completion. Thus dereferencing req->iv after it returns is invalid. Instead of checking req->iv against info, create a new variable unaligned_info and use it for that purpose instead.	N/A	More Details
CVE-2025-71130	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gem: Zero-initialize the eb.vma array in i915_gem_do_execbuffer Initialize the eb.vma array with values of 0 when the eb structure is first set up. In particular, this sets the eb->vma[i].vma pointers to NULL, simplifying cleanup and getting rid of the bug described below. During the execution of eb_lookup_vmas(), the eb->vma array is successively filled up with struct eb_vma objects. This process includes calling eb_add_vma(), which might fail; however, even in the event of failure, eb->vma[i].vma is set for the currently processed buffer. If eb_add_vma() fails, eb_lookup_vmas() returns with an error, which prompts a call to eb_release_vmas() to clean up the mess. Since eb_lookup_vmas() might fail during processing any (possibly not first) buffer, eb_release_vmas() checks whether a buffer's vma is NULL to know at what point did the lookup function fail. In eb_lookup_vmas(), eb->vma[i].vma is set to NULL if either the helper function eb_lookup_vma() or eb_validate_vma() fails. eb->vma[i+1].vma is set to NULL in case i915_gem_object_userptr_submit_init() fails; the current one needs to be cleaned up by eb_release_vmas() at this point, so the next one is set. If eb_add_vma() fails, neither the current nor the next vma is set to NULL, which is a source of a NULL deref bug described in the issue linked in the Closes tag. When entering eb_lookup_vmas(), the vma pointers are set to the slab poison value, instead of NULL. This doesn't matter for the actual lookup, since it gets overwritten anyway, however the eb_release_vmas() function only recognizes NULL as the stopping value, hence the pointers are being set to NULL as they go in case of intermediate failure. This patch changes the approach to filling them all with NULL at the start instead, rather than handling that manually during failure. (cherry picked from commit 08889b706d4f0b8d2352b7ca29c2d8df4d0787cd)	N/A	More Details
CVE-2026-21618	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in hexpm hexpm/hexpm ('Elixir.HexpmWeb.SharedAuthorizationView' modules) allows Cross-Site Scripting (XSS). This vulnerability is associated with program files lib/hexpm_web/views/shared_authorization_view.ex and program routines 'Elixir.HexpmWeb.SharedAuthorizationView':render_grouped_scopes/3. This issue affects hexpm: from 617e44c71f1dd9043870205f371d375c5c4d886d before c692438684ead90c3bcbfb9ccf4e63c768c668a8, from pkg:github/hexpm/hexpm@617e44c71f1dd9043870205f371d375c5c4d886d before pkg:github/hexpm/hexpm@c692438684ead90c3bcbfb9ccf4e63c768c668a8; hex.pm: from 2025-10-01 before 2026-01-19.	N/A	More Details

CVE-2025-71129	In the Linux kernel, the following vulnerability has been resolved: LoongArch: BPF: Sign extend kfunc call arguments The kfunc calls are native calls so they should follow LoongArch calling conventions. Sign extend its arguments properly to avoid kernel panic. This is done by adding a new emit_abi_ext() helper. The emit_abi_ext() helper performs extension in place meaning a value already store in the target register (Note: this is different from the existing sign_extend() helper and thus we can't reuse it).	N/A	More Details
CVE-2025-71128	In the Linux kernel, the following vulnerability has been resolved: erspan: Initialize options_len before referencing options. The struct ip_tunnel_info has a flexible array member named options that is protected by a counted_by(options_len) attribute. The compiler will use this information to enforce runtime bounds checking deployed by FORTIFY_SOURCE string helpers. As laid out in the GCC documentation, the counter must be initialized before the first reference to the flexible array member. After scanning through the files that use struct ip_tunnel_info and also refer to options or options_len, it appears the normal case is to use the ip_tunnel_info_opts_set() helper. Said helper would initialize options_len properly before copying data into options, however in the GRE ERSPAN code a partial update is done, preventing the use of the helper function. Before this change the handling of ERSPAN traffic in GRE tunnels would cause a kernel panic when the kernel is compiled with GCC 15+ and having FORTIFY_SOURCE configured: memcpy: detected buffer overflow: 4 byte write of buffer size 0 Call Trace: <IRQ> __fortify_panic+0xd/0xf erspan_rcv.cold+0x68/0x83 ? ip_route_input_slow+0x816/0x9d0 gre_rcv+0x1b2/0x1c0 gre_rcv+0x8e/0x100 ? raw_v4_input+0x2a0/0x2b0 ip_protocol_deliver_rcu+0x1ea/0x210 ip_local_deliver_finish+0x86/0x110 ip_local_deliver+0x65/0x110 ? ip_rcv_finish_core+0xd6/0x360 ip_rcv+0x186/0x1a0 Reported-at: https://launchpad.net/bugs/2129580	N/A	More Details
CVE-2025-71127	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: Discard Beacon frames to non-broadcast address Beacon frames are required to be sent to the broadcast address, see IEEE Std 802.11-2020, 11.1.3.1 ("The Address 1 field of the Beacon .. frame shall be set to the broadcast address"). A unicast Beacon frame might be used as a targeted attack to get one of the associated STAs to do something (e.g., using CSA to move it to another channel). As such, it is better have strict filtering for this on the received side and discard all Beacon frames that are sent to an unexpected address. This is even more important for cases where beacon protection is used. The current implementation in mac80211 is correctly discarding unicast Beacon frames if the Protected Frame bit in the Frame Control field is set to 0. However, if that bit is set to 1, the logic used for checking for configured BIGTK(s) does not actually work. If the driver does not have logic for dropping unicast Beacon frames with Protected Frame bit 1, these frames would be accepted in mac80211 processing as valid Beacon frames even though they are not protected. This would allow beacon protection to be bypassed. While the logic for checking beacon protection could be extended to cover this corner case, a more generic check for discard all Beacon frames based on A1=unicast address covers this without needing additional changes. Address all these issues by dropping received Beacon frames if they are sent to a non-broadcast address.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: mptcp: avoid deadlock on fallback while reinjecting Jakub reported an MPTCP deadlock at fallback time: WARNING: possible recursive locking detected 6.18.0-rc7-virtme #1 Not tainted -- mptcp_connect/20858 is trying to acquire lock: ff1100001da18b60 (&msk->fallback_lock){+.-.}-{3:3}, at: __mptcp_try_fallback+0xd8/0x280 but task is already holding lock: ff1100001da18b60 (&msk->fallback_lock){+.-.}-{3:3}, at: __mptcp_retrans+0x352/0xaa0 other info that might help us debug this: Possible unsafe locking scenario: CPU0 ---- lock(&msk->fallback_lock); lock(&msk-		

CVE-2025-71126	>fallback_lock); *** DEADLOCK *** May be due to missing lock nesting notation 3 locks held by mptcp_connect/20858: #0: ff1100001da18290 (sk_lock-AF_INET) {+.+.}-{0:0}, at: mptcp_sendmsg+0x114/0x1bc0 #1: ff1100001db40fd0 (k-sk_lock-AF_INET#2){+.+.}-{0:0}, at: __mptcp_retrans+0x2cb/0xaa0 #2: ff1100001da18b60 (&msk->fallback_lock){+.-.}-{3:3}, at: __mptcp_retrans+0x352/0xaa0 stack backtrace: CPU: 0 UID: 0 PID: 20858 Comm: mptcp_connect Not tainted 6.18.0-rc7-virtme #1 PREEMPT(full) Hardware name: Bochs, BIOS Bochs 01/01/2011 Call Trace: <TASK> dump_stack_lvl+0x6f/0xa0 print_deadlock_bug.cold+0xc0/0xcd validate_chain+0x2ff/0x5f0 __lock_acquire+0x34c/0x740 lock_acquire.part.0+0xbc/0x260 _raw_spin_lock_bh+0x38/0x50 __mptcp_try_fallback+0xd8/0x280 mptcp_sendmsg_frag+0x16c2/0x3050 __mptcp_retrans+0x421/0xaa0 mptcp_release_cb+0x5aa/0xa70 release_sock+0xab/0x1d0 mptcp_sendmsg+0xd5b/0x1bc0 sock_write_iter+0x281/0x4d0 new_sync_write+0x3c5/0x6f0 vfs_write+0x65e/0xbb0 ksys_write+0x17e/0x200 do_syscall_64+0xbb/0xfd0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x7fa5627cbc5e Code: 4d 89 d8 e8 14 bd 00 00 4c 8b 5d f8 41 8b 93 08 03 00 00 59 5e 48 83 f8 fc 74 11 c9 c3 0f 1f 80 00 00 00 00 48 8b 45 10 0f 05 <c9> c3 83 e2 39 83 fa 08 75 e7 e8 13 ff ff ff 0f 1f 00 f3 0f 1e fa RSP: 002b:00007fff1fe14700 EFLAGS: 00000202 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 0000000000000005 RCX: 00007fa5627cbc5e RDX: 0000000000001f9c RSI: 00007fff1fe16984 RDI: 0000000000000005 RBP: 00007fff1fe14710 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000202 R12: 00007fff1fe16920 R13: 0000000000002000 R14: 0000000000001f9c R15: 0000000000001f9c The packet scheduler could attempt a reinjection after receiving an MP_FAIL and before the infinite map has been transmitted, causing a deadlock since MPTCP needs to do the reinjection atomically from WRT fallback. Address the issue explicitly avoiding the reinjection in the critical scenario. Note that this is the only fallback critical section that could potentially send packets and hit the double-lock.	N/A	More Details
CVE-2025-15104	Nu Html Checker (validator.nu) contains a restriction bypass that allows remote attackers to make the server perform arbitrary HTTP/HTTPS requests to internal resources, including localhost services. While the validator implements hostname-based protections to block direct access to localhost and 127.0.0.1, these controls can be bypassed using DNS rebinding techniques or domains that resolve to loopback addresses.This issue affects The Nu Html Checker (vnu): latest (commit 23f090a11bab8d0d4e698f1ffc197a4fe226a9cd).	N/A	More Details
CVE-2025-68492	Chainlit versions prior to 2.8.5 contain an authorization bypass through user-controlled key vulnerability. If this vulnerability is exploited, threads may be viewed or thread ownership may be obtained by an attacker who can log in to the product.	N/A	More Details
CVE-2025-71116	In the Linux kernel, the following vulnerability has been resolved: libceph: make decode_pool() more resilient against corrupted osdmaps If the osdmap is (maliciously) corrupted such that the encoded length of ceph_pg_pool envelope is less than what is expected for a particular encoding version, out-of-bounds reads may ensue because the only bounds check that is there is based on that length value. This patch adds explicit bounds checks for each field that is decoded or skipped.	N/A	More Details
CVE-2025-71115	In the Linux kernel, the following vulnerability has been resolved: um: init cpu_tasks[] earlier This is currently done in uml_finishsetup(), but e.g. with KCOV enabled we'll crash because some init code can call into e.g. memparse(), which has coverage annotations, and then the checks in check_kcov_mode() crash because current is NULL. Simply initialize the cpu_tasks[] array statically, which fixes the crash. For the later SMP work, it seems to have not really caused any problems yet, but initialize all of the entries anyway.	N/A	More Details

CVE-2025-71114	In the Linux kernel, the following vulnerability has been resolved: via_wdt: fix critical boot hang due to unnamed resource allocation The VIA watchdog driver uses allocate_resource() to reserve a MMIO region for the watchdog control register. However, the allocated resource was not given a name, which causes the kernel resource tree to contain an entry marked as "<BAD>" under /proc/iomem on x86 platforms. During boot, this unnamed resource can lead to a critical hang because subsequent resource lookups and conflict checks fail to handle the invalid entry properly.	N/A	More Details
CVE-2025-71106	In the Linux kernel, the following vulnerability has been resolved: fs: PM: Fix reverse check in filesystems_freeze_callback() The freeze_all_ptr check in filesystems_freeze_callback() introduced by commit a3f8f8662771 ("power: always freeze efivarfs") is reverse which quite confusingly causes all file systems to be frozen when filesystem_freeze_enabled is false. On my systems it causes the WARN_ON_ONCE() in __set_task_frozen() to trigger, most likely due to an attempt to freeze a file system that is not ready for that. Add a logical negation to the check in question to reverse it as appropriate.	N/A	More Details
CVE-2025-67859	A Improper Authentication vulnerability in TLP allows local users to arbitrarily control the power profile in use as well as the daemon’s log settings.This issue affects TLP: from 1.9 before 1.9.1.	N/A	More Details
CVE-2026-23735	GraphQL Modules is a toolset of libraries and guidelines dedicated to create reusable, maintainable, testable and extendable modules out of your GraphQL server. From 2.2.1 to before 2.4.1 and 3.1.1, when 2 or more parallel requests are made which trigger the same service, the context of the requests is mixed up in the service when the context is injected via @ExecutionContext(). ExecutionContext is often used to pass authentication tokens from incoming requests to services loading data from backend APIs. This vulnerability is fixed in 2.4.1 and 3.1.1.	N/A	More Details
CVE-2026-23730	WeGIA is a web manager for charitable institutions. Prior to 3.6.2, an Open Redirect vulnerability was identified in the /WeGIA/controle/control.php endpoint of the WeGIA application, specifically through the nextPage parameter when combined with metodo=listarTodos and nomeClasse=ProdutoControle. The application fails to validate or restrict the nextPage parameter, allowing attackers to redirect users to arbitrary external websites. This can be abused for phishing attacks, credential theft, malware distribution, and social engineering using the trusted WeGIA domain. This vulnerability is fixed in 3.6.2.	N/A	More Details
CVE-2026-23729	WeGIA is a web manager for charitable institutions. Prior to 3.6.2, an Open Redirect vulnerability was identified in the /WeGIA/controle/control.php endpoint of the WeGIA application, specifically through the nextPage parameter when combined with metodo=listarDescricao and nomeClasse=ProdutoControle. The application fails to validate or restrict the nextPage parameter, allowing attackers to redirect users to arbitrary external websites. This can be abused for phishing attacks, credential theft, malware distribution, and social engineering using the trusted WeGIA domain. This vulnerability is fixed in 3.6.2.	N/A	More Details
CVE-2026-23728	WeGIA is a web manager for charitable institutions. Prior to 3.6.2, an Open Redirect vulnerability was identified in the /WeGIA/controle/control.php endpoint of the WeGIA application, specifically through the nextPage parameter when combined with metodo=listarTodos and nomeClasse=DestinoControle. The application fails to validate or restrict the nextPage parameter, allowing attackers to redirect users to arbitrary external websites. This can be abused for phishing attacks, credential theft, malware distribution, and social engineering using the trusted WeGIA domain. This vulnerability is fixed in 3.6.2.	N/A	More Details
	WeGIA is a web manager for charitable institutions. Prior to 3.6.2, an Open Redirect		

CVE-2026-23727	vulnerability was identified in the /WeGIA/controle/control.php endpoint of the WeGIA application, specifically through the nextPage parameter when combined with metodo=listarTodos and nomeClasse=TipoSaidaControle. The application fails to validate or restrict the nextPage parameter, allowing attackers to redirect users to arbitrary external websites. This can be abused for phishing attacks, credential theft, malware distribution, and social engineering using the trusted WeGIA domain. This vulnerability is fixed in 3.6.2.	N/A	More Details
CVE-2026-23726	WeGIA is a web manager for charitable institutions. Prior to 3.6.2, An Open Redirect vulnerability was identified in the /WeGIA/controle/control.php endpoint of the WeGIA application, specifically through the nextPage parameter when combined with metodo=listarTodos and nomeClasse=TipoEntradaControle. The application fails to validate or restrict the nextPage parameter, allowing attackers to redirect users to arbitrary external websites. This can be abused for phishing attacks, credential theft, malware distribution, and social engineering using the trusted WeGIA domain. This vulnerability is fixed in 3.6.2.	N/A	More Details
CVE-2026-23725	WeGIA is a web manager for charitable institutions. Prior to 3.6.2, a Stored Cross-Site Scripting (XSS) vulnerability was identified in the html/pet/adotantes/cadastro_adotante.php and html/pet/adotantes/informacao_adotantes.php endpoint of the WeGIA application. The application does not sanitize user-controlled input before rendering it inside the Adopters Information table, allowing persistent JavaScript injection. Any user who visits the page will have the payload executed automatically. This vulnerability is fixed in 3.6.2.	N/A	More Details
CVE-2025-71105	In the Linux kernel, the following vulnerability has been resolved: f2fs: use global inline_xattr_slab instead of per-sb slab cache As Hong Yun reported in mailing list: loop7: detected capacity change from 0 to 131072 ------------[cut here]------------ kmem_cache of name 'f2fs_xattr_entry-7:7' already exists WARNING: CPU: 0 PID: 24426 at mm/slab_common.c:110 kmem_cache_sanity_check mm/slab_common.c:109 [inline] WARNING: CPU: 0 PID: 24426 at mm/slab_common.c:110 __kmem_cache_create_args+0xa6/0x320 mm/slab_common.c:307 CPU: 0 UID: 0 PID: 24426 Comm: syz.7.1370 Not tainted 6.17.0-rc4 #1 PREEMPT(full) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.13.0-1ubuntu1.1 04/01/2014 RIP: 0010:kmem_cache_sanity_check mm/slab_common.c:109 [inline] RIP: 0010:__kmem_cache_create_args+0xa6/0x320 mm/slab_common.c:307 Call Trace: __kmem_cache_create include/linux/slab.h:353 [inline] f2fs_kmem_cache_create fs/f2fs/f2fs.h:2943 [inline] f2fs_init_xattr_caches+0xa5/0xe0 fs/f2fs/xattr.c:843 f2fs_fill_super+0x1645/0x2620 fs/f2fs/super.c:4918 get_tree_bdev_flags+0x1fb/0x260 fs/super.c:1692 vfs_get_tree+0x43/0x140 fs/super.c:1815 do_new_mount+0x201/0x550 fs/namespace.c:3808 do_mount fs/namespace.c:4136 [inline] __do_sys_mount fs/namespace.c:4347 [inline] __se_sys_mount+0x298/0x2f0 fs/namespace.c:4324 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0x8e/0x3a0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x76/0x7e The bug can be reproduced w/ below scripts: - mount /dev/vdb /mnt1 - mount /dev/vdc /mnt2 - umount /mnt1 - mounnt /dev/vdb /mnt1 The reason is if we created two slab caches, named f2fs_xattr_entry-7:3 and f2fs_xattr_entry-7:7, and they have the same slab size. Actually, slab system will only create one slab cache core structure which has slab name of "f2fs_xattr_entry-7:3", and two slab caches share the same structure and cache address. So, if we destroy f2fs_xattr_entry-7:3 cache w/ cache address, it will decrease reference count of slab cache, rather than release slab cache entirely, since there is one more user has referenced the cache. Then, if we try to create slab cache w/ name "f2fs_xattr_entry-7:3" again, slab system will find that there is existed cache which has the same name and trigger the warning. Let's changes to use global inline_xattr_slab instead of per-sb slab cache for fixing.	N/A	More Details

CVE-2026-23645	SiYuan is self-hosted, open source personal knowledge management software. Prior to 3.5.4-dev2, a Stored Cross-Site Scripting (XSS) vulnerability exists in SiYuan Note. The application does not sanitize uploaded SVG files. If a user uploads and views a malicious SVG file (e.g., imported from an untrusted source), arbitrary JavaScript code is executed in the context of their authenticated session. This vulnerability is fixed in 3.5.4-dev2.	N/A	More Details
CVE-2025-71104	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: Fix VM hard lockup after prolonged inactivity with periodic HV timer When advancing the target expiration for the guest's APIC timer in periodic mode, set the expiration to "now" if the target expiration is in the past (similar to what is done in update_target_expiration()). Blindly adding the period to the previous target expiration can result in KVM generating a practically unbounded number of hrtimer IRQs due to programming an expired timer over and over. In extreme scenarios, e.g. if userspace pauses/suspends a VM for an extended duration, this can even cause hard lockups in the host. Currently, the bug only affects Intel CPUs when using the hypervisor timer (HV timer), a.k.a. the VMX preemption timer. Unlike the software timer, a.k.a. hrtimer, which KVM keeps running even on exits to userspace, the HV timer only runs while the guest is active. As a result, if the vCPU does not run for an extended duration, there will be a huge gap between the target expiration and the current time the vCPU resumes running. Because the target expiration is incremented by only one period on each timer expiration, this leads to a series of timer expirations occurring rapidly after the vCPU/VM resumes. More critically, when the vCPU first triggers a periodic HV timer expiration after resuming, advancing the expiration by only one period will result in a target expiration in the past. As a result, the delta may be calculated as a negative value. When the delta is converted into an absolute value (tscdeadline is an unsigned u64), the resulting value can overflow what the HV timer is capable of programming. I.e. the large value will exceed the VMX Preemption Timer's maximum bit width of cpu_preemption_timer_multi + 32, and thus cause KVM to switch from the HV timer to the software timer (hrtimers). After switching to the software timer, periodic timer expiration callbacks may be executed consecutively within a single clock interrupt handler, because hrtimers honors KVM's request for an expiration in the past and immediately re-invokes KVM's callback after reprogramming. And because the interrupt handler runs with IRQs disabled, restarting KVM's hrtimer over and over until the target expiration is advanced to "now" can result in a hard lockup. E.g. the following hard lockup was triggered in the host when running a Windows VM (only relevant because it used the APIC timer in periodic mode) after resuming the VM from a long suspend (in the host). NMI watchdog: Watchdog detected hard LOCKUP on cpu 45 ... RIP: 0010:advance_periodic_target_expiration+0x4d/0x80 [kvm] ... RSP: 0018:ff4f88f5d98d8ef0 EFLAGS: 00000046 RAX: fff0103f91be678e RBX: fff0103f91be678e RCX: 00843a7d9e127bcc RDX: 0000000000000002 RSI: 0052ca4003697505 RDI: ff440d5bfbdbd500 RBP: ff440d5956f99200 R08: ff2ff2a42deb6a84 R09: 000000000002a6c0 R10: 0122d794016332b3 R11: 0000000000000000 R12: ff440db1af39cfc0 R13: ff440db1af39cfc0 R14: ffffffffc0d4a560 R15: ff440db1af39d0f8 FS: 00007f04a6ffd700(0000) GS:ff440db1af380000(0000) knlGS:000000e38a3b8000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000d5651feff8 CR3: 000000684e038002 CR4: 0000000000773ee0 PKRU: 55555554 Call Trace: <IRQ> apic_timer_fn+0x31/0x50 [kvm] __hrtimer_run_queues+0x100/0x280 hrtimer_interrupt+0x100/0x210 ? ttwu_do_wakeup+0x19/0x160 smp_apic_timer_interrupt+0x6a/0x130 apic_timer_interrupt+0xf/0x20 </IRQ> Moreover, if the suspend duration of the virtual machine is not long enough to trigger a hard lockup in this scenario, since commit 98c25ead5eda ("KVM: VMX: Move preemption timer <=> hrtimer dance to common x86"), KVM will continue using the software timer until the guest reprograms the APIC timer in some way. Since the periodic timer does not require frequent APIC timer register programming, the guest may continue to use the software timer in ---truncated---	N/A	More Details

CVE-2012-10064	Omni Secure Files plugin versions prior to 0.1.14 contain an arbitrary file upload vulnerability in the bundled plupload example endpoint. The /wp-content/plugins/omni-secure-files/plupload/examples/upload.php handler allows unauthenticated uploads without enforcing safe file type restrictions, enabling an attacker to place attacker-controlled files under the plugin's uploads directory. This can lead to remote code execution if a server-executable file type is uploaded and subsequently accessed.	N/A	More Details
CVE-2025-13175	Y Soft SafeQ 6 renders the Workflow Connector password field in a way that allows an administrator with UI access to reveal the value using browser developer/inspection tools. The affected customers are only those with a password-protected scan workflow connector. This issue affects Y Soft SafeQ 6 in versions before MU106.	N/A	More Details
CVE-2025-14317	In Crazy Bubble Tea mobile application authenticated attacker can obtain personal information about other users by enumerating a `loyaltyGuestId` parameter. Server does not verify the permissions required to obtain the data. This issue was fixed in version 915 (Android) and 7.4.1 (iOS).	N/A	More Details
CVE-2025-71102	In the Linux kernel, the following vulnerability has been resolved: scs: fix a wrong parameter in __scs_magic __scs_magic() needs a 'void *' variable, but a 'struct task_struct *' is given. 'task_scs(tsk)' is the starting address of the task's shadow call stack, and '__scs_magic(task_scs(tsk))' is the end address of the task's shadow call stack. Here should be '__scs_magic(task_scs(tsk))'. The user-visible effect of this bug is that when CONFIG_DEBUG_STACK_USAGE is enabled, the shadow call stack usage checking function (scs_check_usage) would scan an incorrect memory range. This could lead 1. **Inaccurate stack usage reporting**: The function would calculate wrong usage statistics for the shadow call stack, potentially showing incorrect value in kmsg. 2. **Potential kernel crash**: If the value of __scs_magic(tsk)is greater than that of __scs_magic(task_scs(tsk)), the for loop may access unmapped memory, potentially causing a kernel panic. However, this scenario is unlikely because task_struct is allocated via the slab allocator (which typically returns lower addresses), while the shadow call stack returned by task_scs(tsk) is allocated via vmalloc(which typically returns higher addresses). However, since this is purely a debugging feature (CONFIG_DEBUG_STACK_USAGE), normal production systems should be not unaffected. The bug only impacts developers and testers who are actively debugging stack usage with this configuration enabled.	N/A	More Details
CVE-2019-25297	Poll, Survey & Quiz Maker Plugin by Opinion Stage Wordpress plugin versions prior to 19.6.25 contain a stored cross-site scripting (XSS) vulnerability via multiple parameters due to insufficient input validation and output escaping. An unauthenticated attacker can inject arbitrary script into content that executes when a victim views an affected page.	N/A	More Details
CVE-2025-71107	In the Linux kernel, the following vulnerability has been resolved: f2fs: ensure node page reads complete before f2fs_put_super() finishes Xfstests generic/335, generic/336 sometimes crash with the following message: F2FS-fs (dm-0): detect filesystem reference count leak during umount, type: 9, count: 1 ------------[cut here]------------ kernel BUG at fs/f2fs/super.c:1939! Oops: invalid opcode: 0000 [#1] SMP NOPTI CPU: 1 UID: 0 PID: 609351 Comm: umount Tainted: G W 6.17.0-rc5-xfstests-g9dd1835ecda5 #1 PREEMPT(none) Tainted: [W]=WARN Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 RIP: 0010:f2fs_put_super+0x3b3/0x3c0 Call Trace: <TASK> generic_shutdown_super+0x7e/0x190 kill_block_super+0x1a/0x40 kill_f2fs_super+0x9d/0x190 deactivate_locked_super+0x30/0xb0 cleanup_mnt+0xba/0x150 task_work_run+0x5c/0xa0 exit_to_user_mode_loop+0xb7/0xc0 do_syscall_64+0x1ae/0x1c0 entry_SYSCALL_64_after_hwframe+0x76/0x7e </TASK> ---[end trace	N/A	More Details

	0000000000000000]--- It appears that sometimes it is possible that f2fs_put_super() is called before all node page reads are completed. Adding a call to f2fs_wait_on_all_pages() for F2FS_RD_NODE fixes the problem.		
CVE-2025-71113	In the Linux kernel, the following vulnerability has been resolved: crypto: af_alg - zero initialize memory allocated via sock_kmalloc Several crypto user API contexts and requests allocated with sock_kmalloc() were left uninitialized, relying on callers to set fields explicitly. This resulted in the use of uninitialized data in certain error paths or when new fields are added in the future. The ACVP patches also contain two user-space interface files: algif_kpp.c and algif_akcipher.c. These too rely on proper initialization of their context structures. A particular issue has been observed with the newly added 'inflight' variable introduced in af_alg_ctx by commit: 67b164a871af ("crypto: af_alg - Disallow multiple in-flight AIO requests") Because the context is not memset to zero after allocation, the inflight variable has contained garbage values. As a result, af_alg_alloc_areq() has incorrectly returned -EBUSY randomly when the garbage value was interpreted as true: https://github.com/gregkh/linux/blame/master/crypto/af_alg.c#L1209 The check directly tests ctx->inflight without explicitly comparing against true/false. Since inflight is only ever set to true or false later, an uninitialized value has triggered -EBUSY failures. Zero-initializing memory allocated with sock_kmalloc() ensures inflight and other fields start in a known state, removing random issues caused by uninitialized data.	N/A	More Details
CVE-2026-23745	node-tar is a Tar for Node.js. The node-tar library (<= 7.5.2) fails to sanitize the linkpath of Link (hardlink) and SymbolicLink entries when preservePaths is false (the default secure behavior). This allows malicious archives to bypass the extraction root restriction, leading to Arbitrary File Overwrite via hardlinks and Symlink Poisoning via absolute symlink targets. This vulnerability is fixed in 7.5.3.	N/A	More Details
CVE-2025-66005	Lack of authorization of the InputManager D-Bus interface in InputPlumber versions before v0.63.0 can lead to local Denial-of-Service, information leak or even privilege escalation in the context of the currently active user session.	N/A	More Details
CVE-2025-71112	In the Linux kernel, the following vulnerability has been resolved: net: hns3: add VLAN id validation before using Currently, the VLAN id may be used without validation when receive a VLAN configuration mailbox from VF. The length of vlan_del_fail_bmap is BITS_TO_LONGS(VLAN_N_VID). It may cause out-of-bounds memory access once the VLAN id is bigger than or equal to VLAN_N_VID. Therefore, VLAN id needs to be checked to ensure it is within the range of VLAN_N_VID.	N/A	More Details
CVE-2025-71111	In the Linux kernel, the following vulnerability has been resolved: hwmon: (w83791d) Convert macros to functions to avoid TOCTOU The macro FAN_FROM_REG evaluates its arguments multiple times. When used in lockless contexts involving shared driver data, this leads to Time-of-Check to Time-of-Use (TOCTOU) race conditions, potentially causing divide-by-zero errors. Convert the macro to a static function. This guarantees that arguments are evaluated only once (pass-by-value), preventing the race conditions. Additionally, in store_fan_div, move the calculation of the minimum limit inside the update lock. This ensures that the read-modify-write sequence operates on consistent data. Adhere to the principle of minimal changes by only converting macros that evaluate arguments multiple times and are used in lockless contexts.	N/A	More Details
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: mm/slub: reset KASAN tag in defer_free() before accessing freed memory When CONFIG_SLUB_TINY is enabled, kfree_nolock() calls kasan_slab_free() before defer_free(). On ARM64 with MTE (Memory Tagging Extension), kasan_slab_free() poisons the memory and changes the tag from the original (e.g., 0xf3) to a poison tag (0xfe). When defer_free() then tries to write to the freed object to build the deferred free list via llist_add(), the pointer still has the old tag, causing a tag mismatch and triggering a	N/A	More Details

71110	KASAN use-after-free report: BUG: KASAN: slab-use-after-free in defer_free+0x3c/0xbc mm/slub.c:6537 Write at addr f3f000000854f020 by task kworker/u8:6/983 Pointer tag: [f3], memory tag: [fe] Fix this by calling kasan_reset_tag() before accessing the freed memory. This is safe because defer_free() is part of the allocator itself and is expected to manipulate freed memory for bookkeeping purposes.		
CVE-2025-71109	In the Linux kernel, the following vulnerability has been resolved: MIPS: ftrace: Fix memory corruption when kernel is located beyond 32 bits Since commit e424054000878 ("MIPS: Tracing: Reduce the overhead of dynamic Function Tracer"), the macro UASM_i_LA_mostly has been used, and this macro can generate more than 2 instructions. At the same time, the code in ftrace assumes that no more than 2 instructions can be generated, which is why it stores them in an int[2] array. However, as previously noted, the macro UASM_i_LA_mostly (and now UASM_i_LA) causes a buffer overflow when _mcount is beyond 32 bits. This leads to corruption of the variables located in the __read_mostly section. This corruption was observed because the variable __cpu_primary_thread_mask was corrupted, causing a hang very early during boot. This fix prevents the corruption by avoiding the generation of instructions if they could exceed 2 instructions in length. Fortunately, insn_la_mcount is only used if the instrumented code is located outside the kernel code section, so dynamic ftrace can still be used, albeit in a more limited scope. This is still preferable to corrupting memory and/or crashing the kernel.	N/A	More Details
CVE-2025-71108	In the Linux kernel, the following vulnerability has been resolved: usb: typec: ucsi: Handle incorrect num_connectors capability The UCSI spec states that the num_connectors field is 7 bits, and the 8th bit is reserved and should be set to zero. Some buggy FW has been known to set this bit, and it can lead to a system not booting. Flag that the FW is not behaving correctly, and auto-fix the value so that the system boots correctly. Found on Lenovo P1 G8 during Linux enablement program. The FW will be fixed, but seemed worth addressing in case it hit platforms that aren't officially Linux supported.	N/A	More Details
CVE-2026-0519	In Secure Access 12.70 and prior to 14.20, the logging subsystem may write an unredacted authentication token to logs under certain configurations. Any party with access to those logs could read the token and reuse it to access an integrated system.	N/A	More Details
CVE-2026-0518	CVE-2026-0518 is a cross-site scripting vulnerability in versions of Secure Access prior to 14.20. An attacker with administrative privileges can interfere with another administrator’s use of the console.	N/A	More Details
CVE-2026-0517	CVE-2026-0517 is a denial-of-service vulnerability in versions of Secure Access Server prior to 14.20. An attacker can send a specially crafted packet to a server and cause the server to crash	N/A	More Details
CVE-2026-22865	Gradle is a build automation tool, and its native-platform tool provides Java bindings for native APIs. When resolving dependencies in versions before 9.3.0, some exceptions were not treated as fatal errors and would not cause a repository to be disabled. If a build encountered one of these exceptions, Gradle would continue to the next repository in the list and potentially resolve dependencies from a different repository. An exception like NoHttpResponseException can indicate transient errors. If the errors persist after a maximum number of retries, Gradle would continue to the next repository. This behavior could allow an attacker to disrupt the service of a repository and leverage another repository to serve malicious artifacts. This attack requires the attacker to have control over a repository after the disrupted repository. Gradle has introduced a change in behavior in Gradle 9.3.0 to stop searching other repositories when encountering these errors.	N/A	More Details
	Gradle is a build automation tool, and its native-platform tool provides Java bindings		

CVE-2026-22816	for native APIs. When resolving dependencies in versions before 9.3.0, some exceptions were not treated as fatal errors and would not cause a repository to be disabled. If a build encountered one of these exceptions, Gradle would continue to the next repository in the list and potentially resolve dependencies from a different repository. If a Gradle build used an unresolvable host name, Gradle would continue to work as long as all dependencies could be resolved from another repository. An unresolvable host name could be caused by allowing a repository's domain name registration to lapse or typo-ing the real domain name. This behavior could allow an attacker to register a service under the host name used by the build and serve malicious artifacts. The attack requires the repository to be listed before others in the build configuration. Gradle has introduced a change in behavior in Gradle 9.3.0 to stop searching other repositories when encountering these errors.	N/A	More Details
CVE-2025-5489	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-5102	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-8506	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-8491	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-23533	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.21.0, a client-side heap buffer overflow occurs in the RDPGFX ClearCodec decode path when maliciously crafted residual data causes out-of-bounds writes during color output. A malicious server can trigger a client-side heap buffer overflow, causing a crash (DoS) and potential heap corruption with code-execution risk depending on allocator behavior and surrounding heap layout. Version 3.21.0 contains a patch for the issue.	N/A	More Details
CVE-2026-20894	Cross-site scripting vulnerability exists in multiple Network Cameras TRIFORA 3 series provided by TOA Corporation. If an attacking administrator configures the affected product with some malicious input, an arbitrary script may be executed on the web browser of a victim administrator who accesses the setting screen.	N/A	More Details
CVE-2026-21889	Weblate is a web based localization tool. Prior to 5.15.2, the screenshot images were served directly by the HTTP server without proper access control. This could allow an unauthenticated user to access screenshots after guessing their filename. This vulnerability is fixed in 5.15.2.	N/A	More Details
CVE-2025-40644	Reflected Cross-Site Scripting (XSS) vulnerability in Riftzilla's QRGen. This vulnerability allows an attavker to execute JavaScript code in the victim's browser by sending them a malicious URL using the 'id' parameter in '/article.php'. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user.	N/A	More Details
CVE-2025-11743	A denial-of-service security issue in the affected product. The security issue occurs when a malformed CIP forward open message is sent. This could result in a major nonrecoverable fault a restart is required to recover.	N/A	More Details
CVE-2026-1183	HTML injection vulnerability in multiple Botble products such as TransP, Athena, Martfury, and Homzen, consisting of an HTML injection due to a lack of proper validation of user input by sending a request to '/search' using the 'q' parameter.	N/A	More Details

CVE-2025-71144	In the Linux kernel, the following vulnerability has been resolved: mptcp: ensure context reset on disconnect() After the blamed commit below, if the MPC subflow is already in TCP_CLOSE status or has fallback to TCP at mptcp_disconnect() time, mptcp_do_fastclose() skips setting the `send_fastclose flag` and the later __mptcp_close_ssk() does not reset anymore the related subflow context. Any later connection will be created with both the `request_mptcp` flag and the msk-level fallback status off (it is unconditionally cleared at MPTCP disconnect time), leading to a warning in subflow_data_ready(): WARNING: CPU: 26 PID: 8996 at net/mptcp/subflow.c:1519 subflow_data_ready (net/mptcp/subflow.c:1519 (discriminator 13)) Modules linked in: CPU: 26 UID: 0 PID: 8996 Comm: syz.22.39 Not tainted 6.18.0-rc7-05427-g11fc074f6c36 #1 PREEMPT(voluntary) Hardware name: Bochs Bochs, BIOS Bochs 01/01/2011 RIP: 0010:subflow_data_ready (net/mptcp/subflow.c:1519 (discriminator 13)) Code: 90 0f 0b 90 90 e9 04 fe ff ff e8 b7 1e f5 fe 89 ee bf 07 00 00 00 e8 db 19 f5 fe 83 fd 07 0f 84 35 ff ff ff e8 9d 1e f5 fe 90 <0f> 0b 90 e9 27 ff ff ff e8 8f 1e f5 fe 4c 89 e7 48 89 de e8 14 09 RSP: 0018:ffffc9002646fb30 EFLAGS: 00010293 RAX: 0000000000000000 RBX: ffff88813b218000 RCX: ffffffff825c8435 RDX: ffff8881300b3580 RSI: ffffffff825c8443 RDI: 0000000000000005 RBP: 000000000000000b R08: ffffffff825c8435 R09: 000000000000000b R10: 0000000000000005 R11: 0000000000000007 R12: ffff888131ac0000 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 00007f88330af6c0(0000) GS:ffff888a93dd2000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f88330aefe8 CR3: 000000010ff59000 CR4: 0000000000350ef0 Call Trace: <TASK> tcp_data_ready (net/ipv4/tcp_input.c:5356) tcp_data_queue (net/ipv4/tcp_input.c:5445) tcp_rcv_state_process (net/ipv4/tcp_input.c:7165) tcp_v4_do_rcv (net/ipv4/tcp_ipv4.c:1955) __release_sock (include/net/sock.h:1158 (discriminator 6) net/core/sock.c:3180 (discriminator 6)) release_sock (net/core/sock.c:3737) mptcp_sendmsg (net/mptcp/protocol.c:1763 net/mptcp/protocol.c:1857) inet_sendmsg (net/ipv4/af_inet.c:853 (discriminator 7)) __sys_sendto (net/socket.c:727 (discriminator 15) net/socket.c:742 (discriminator 15) net/socket.c:2244 (discriminator 15)) __x64_sys_sendto (net/socket.c:2247) do_syscall_64 (arch/x86/entry/syscall_64.c:63 (discriminator 1) arch/x86/entry/syscall_64.c:94 (discriminator 1)) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) RIP: 0033:0x7f883326702d Address the issue setting an explicit `fastclosing` flag at fastclose time, and checking such flag after mptcp_do_fastclose().	N/A	More Details
CVE-2025-41081	Reflected Cross-Site Scripting (XSS) vulnerability in IsMyGym by Zuinq Studio. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by sending them a malicious URL with '/<PATH>.php/<XSS>'. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user.	N/A	More Details
CVE-2025-41025	Stored Cross-Site Scripting (XSS) in Poultry Farm Management System v1.0 due to the lack of proper validation of user input by sending a POST request. The relationship between parameters and assigned identifiers is as follows: 'category' y 'product' parameters in '/farm/sell_product.php'.	N/A	More Details
CVE-2025-41024	Stored Cross-Site Scripting (XSS) in Poultry Farm Management System v1.0 due to the lack of proper validation of user input by sending a POST request. The relationship between parameters and assigned identifiers is as follows: 'companyaddress', 'companyemail', 'companyname', 'country', 'mobilenumber' y 'regno' parameters in '/farm/farmprofile.php'.	N/A	More Details
CVE-2025-40679	HTML Injection vulnerability in Isshue by Bdtask, consisting os an HTML injection due to a lack os proper validation of user input by sending a POST request to '/category_product_search', affecting the 'product_name' parameter.	N/A	More Details

CVE-2025-71143	In the Linux kernel, the following vulnerability has been resolved: clk: samsung: exynos-clkout: Assign .num before accessing .hws Commit f316cdff8d67 ("clk: Annotate struct clk_hw_onecell_data with __counted_by") annotated the hws member of 'struct clk_hw_onecell_data' with __counted_by, which informs the bounds sanitizer (UBSAN_BOUNDS) about the number of elements in .hws[], so that it can warn when .hws[] is accessed out of bounds. As noted in that change, the __counted_by member must be initialized with the number of elements before the first array access happens, otherwise there will be a warning from each access prior to the initialization because the number of elements is zero. This occurs in exynos_clkout_probe() due to .num being assigned after .hws[] has been accessed: UBSAN: array-index-out-of-bounds in drivers/clk/samsung/clk-exynos-clkout.c:178:18 index 0 is out of range for type 'clk_hw *[*]' Move the .num initialization to before the first access of .hws[], clearing up the warning.	N/A	More Details
CVE-2026-23732	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.21.0, FastGlyph parsing trusts `cbData`/remaining length and never validates against the minimum size implied by `cx/cy`. A malicious server can trigger a client-side global buffer overflow, causing a crash (DoS). Version 3.21.0 contains a patch for the issue.	N/A	More Details
CVE-2025-41084	Stored Cross-Site Scripting (XSS) vulnerability in Sesame web application, due to the fact that uploaded SVG images are not properly sanitized. This allows attackers to embed malicious scripts in SVG files by sending a POST request using the 'logo' parameter in '/api/v3/companies/<ID>/logo', which are then stored on the server and executed in the context of any user who accesses the compromised resource.	N/A	More Details
CVE-2025-71142	In the Linux kernel, the following vulnerability has been resolved: cpuset: fix warning when disabling remote partition A warning was triggered as follows: WARNING: kernel/cgroup/cpuset.c:1651 at remote_partition_disable+0xf7/0x110 RIP: 0010:remote_partition_disable+0xf7/0x110 RSP: 0018:ffffc90001947d88 EFLAGS: 00000206 RAX: 0000000000007fff RBX: ffff888103b6e000 RCX: 0000000000006f40 RDX: 0000000000006f00 RSI: ffffc90001947da8 RDI: ffff888103b6e000 RBP: ffff888103b6e000 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000001 R11: ffff88810b2e2728 R12: ffffc90001947da8 R13: 0000000000000000 R14: ffffc90001947da8 R15: ffff8881081f1c00 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f55c8bbe0b2 CR3: 000000010b14c000 CR4: 00000000000006f0 Call Trace: <TASK> update_prstate+0x2d3/0x580 cpuset_partition_write+0x94/0xf0 kernfs_fop_write_iter+0x147/0x200 vfs_write+0x35d/0x500 ksys_write+0x66/0xe0 do_syscall_64+0x6b/0x390 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x7f55c8cd4887 Reproduction steps (on a 16-CPU machine): # cd /sys/fs/cgroup/ # mkdir A1 # echo +cpuset > A1/cgroup.subtree_control # echo "0-14" > A1/cpuset.cpus.exclusive # mkdir A1/A2 # echo "0-14" > A1/A2/cpuset.cpus.exclusive # echo "root" > A1/A2/cpuset.cpus.partition # echo 0 > /sys/devices/system/cpu/cpu15/online # echo member > A1/A2/cpuset.cpus.partition When CPU 15 is offlined, subpartitions_cpus gets cleared because no CPUs remain available for the top_cpuset, forcing partitions to share CPUs with the top_cpuset. In this scenario, disabling the remote partition triggers a warning stating that effective_xcpus is not a subset of subpartitions_cpus. Partitions should be invalidated in this case to inform users that the partition is now invalid(cpus are shared with top_cpuset). To fix this issue: 1. Only emit the warning only if subpartitions_cpus is not empty and the effective_xcpus is not a subset of subpartitions_cpus. 2. During the CPU hotplug process, invalidate partitions if subpartitions_cpus is empty.	N/A	More Details
CVE-	The extension extends TYPO3’ FileSpool component, which was vulnerable to Insecure Deserialization prior to TYPO3-CORE-SA-2026-004 https://typo3.org/security/advisory/typo3-core-sa-2026-004 . Since the related fix is		

2026-0895	overwritten by the extension, using the extension with a patched TYPO3 core version still allows for Insecure Deserialization, because the affected vulnerable code was extracted from TYPO3 core to the extension. More information about this vulnerability can be found in the related TYPO3 Core Security Advisory TYPO3-CORE-SA-2026-004 https://typo3.org/security/advisory/typo3-core-sa-2026-004 .	N/A	More Details
CVE-2025-71141	In the Linux kernel, the following vulnerability has been resolved: drm/tilcdc: Fix removal actions in case of failed probe The drm_kms_helper_poll_fini() and drm_atomic_helper_shutdown() helpers should only be called when the device has been successfully registered. Currently, these functions are called unconditionally in tilcdc_fini(), which causes warnings during probe deferral scenarios. [7.972317] WARNING: CPU: 0 PID: 23 at drivers/gpu/drm/drm_atomic_state_helper.c:175 drm_atomic_helper_crtc_duplicate_state+0x60/0x68 ... [8.005820] drm_atomic_helper_crtc_duplicate_state from drm_atomic_get_crtc_state+0x68/0x108 [8.005858] drm_atomic_get_crtc_state from drm_atomic_helper_disable_all+0x90/0x1c8 [8.005885] drm_atomic_helper_disable_all from drm_atomic_helper_shutdown+0x90/0x144 [8.005911] drm_atomic_helper_shutdown from tilcdc_fini+0x68/0xf8 [tilcdc] [8.005957] tilcdc_fini [tilcdc] from tilcdc_pdev_probe+0xb0/0x6d4 [tilcdc] Fix this by rewriting the failed probe cleanup path using the standard goto error handling pattern, which ensures that cleanup functions are only called on successfully initialized resources. Additionally, remove the now-unnecessary is_registered flag.	N/A	More Details
CVE-2025-71140	In the Linux kernel, the following vulnerability has been resolved: media: mediatek: vcodec: Use spinlock for context list protection lock Previously a mutex was added to protect the encoder and decoder context lists from unexpected changes originating from the SCP IP block, causing the context pointer to go invalid, resulting in a NULL pointer dereference in the IPI handler. Turns out on the MT8173, the VPU IPI handler is called from hard IRQ context. This causes a big warning from the scheduler. This was first reported downstream on the ChromeOS kernels, but is also reproducible on mainline using Fluster with the FFmpeg v4l2m2m decoders. Even though the actual capture format is not supported, the affected code paths are triggered. Since this lock just protects the context list and operations on it are very fast, it should be OK to switch to a spinlock.	N/A	More Details
CVE-2025-71139	In the Linux kernel, the following vulnerability has been resolved: kernel/kexec: fix IMA when allocation happens in CMA area *** Bug description *** When I tested kexec with the latest kernel, I ran into the following warning: [40.712410] ------------[cut here]------------ [40.712576] WARNING: CPU: 2 PID: 1562 at kernel/kexec_core.c:1001 kimage_map_segment+0x144/0x198 [...] [40.816047] Call trace: [40.818498] kimage_map_segment+0x144/0x198 (P) [40.823221] ima_kexec_post_load+0x58/0xc0 [40.827246] __do_sys_kexec_file_load+0x29c/0x368 [...] [40.855423] ---[end trace 0000000000000000]--- *** How to reproduce *** This bug is only triggered when the kexec target address is allocated in the CMA area. If no CMA area is reserved in the kernel, use the "cma=" option in the kernel command line to reserve one. *** Root cause *** The commit 07d24902977e ("kexec: enable CMA based contiguous allocation") allocates the kexec target address directly on the CMA area to avoid copying during the jump. In this case, there is no IND_SOURCE for the kexec segment. But the current implementation of kimage_map_segment() assumes that IND_SOURCE pages exist and map them into a contiguous virtual address by vmap(). *** Solution *** If IMA segment is allocated in the CMA area, use its page_address() directly.	N/A	More Details
CVE-2025-71138	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dpu: Add missing NULL pointer check for pingpong interface It is checked almost always in dpu_encoder_phys_wb_setup_ctl(), but in a single place the check is missing. Also use convenient locals instead of phys_enc->* where available. Patchwork:	N/A	More Details

	https://patchwork.freedesktop.org/patch/693860/		
CVE-2025-14027	Multiple denial-of-service vulnerabilities exist in the affected product. These issues can be triggered through various crafted inputs, including malformed Class 3 messages, memory leak conditions, and other resource exhaustion scenarios. Exploitation may cause the device to become unresponsive and, in some cases, result in a major nonrecoverable fault. Recovery may require a restart.	N/A	More Details
CVE-2025-14376	A security issue was discovered within the legacy ADI server component of Verve Asset Manager, caused by plaintext secrets stored in environment variables on the ADI server. This component has been retired and has been optional since the 1.36 release in 2024.	N/A	More Details
CVE-2025-14377	A security issue was discovered within the legacy Ansible playbook component of Verve Asset Manager, caused by plaintext secrets incorrectly stored when a playbook is running. This component has been retired and has been optional since the 1.36 release in 2024.	N/A	More Details
CVE-2025-15281	Calling wordexp with WRDE_REUSE in conjunction with WRDE_APPEND in the GNU C Library version 2.0 to version 2.42 may cause the interface to return uninitialized memory in the we_wordv member, which on subsequent calls to wordfree may abort the process.	N/A	More Details
CVE-2026-22211	TinyOS versions up to and including 2.1.2 contain a global buffer overflow vulnerability in the printfUART formatted output implementation used within the ZigBee / IEEE 802.15.4 networking stack. The implementation formats output into a fixed-size global buffer and concatenates strings for %s format specifiers using strcat() without verifying remaining buffer capacity. When printfUART is invoked with a caller-controlled string longer than the available space, the unbounded sprintf/strcat sequence writes past the end of debugbuf, resulting in global memory corruption. This can cause denial of service, unintended behavior, or information disclosure via corrupted adjacent global state or UART output.	N/A	More Details
CVE-2026-22240	The vulnerability exists in BLUVOYIX due to an improper password storage implementation and subsequent exposure via unauthenticated APIs. An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the vulnerable users API to retrieve the plaintext passwords of all user users. Successful exploitation of this vulnerability could allow the attacker to gain full access to customers' data and completely compromise the targeted platform by logging in using an exposed admin email address and password.	N/A	More Details
CVE-2026-22239	The vulnerability exists in BLUVOYIX due to design flaws in the email sending API. An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the vulnerable email sending API. Successful exploitation of this vulnerability could allow the attacker to send unsolicited emails to anyone on behalf of the company.	N/A	More Details
CVE-2026-22238	The vulnerability exists in BLUVOYIX due to improper authentication in the BLUVOYIX admin APIs. An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the vulnerable admin API to create a new user with admin privileges. Successful exploitation of this vulnerability could allow the attacker to gain full access to customers' data and completely compromise the targeted platform by logging in to the newly-created admin user.	N/A	More Details
CVE-2026-22237	The vulnerability exists in BLUVOYIX due to the exposure of sensitive internal API documentation. An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the APIs exposed by the documentation. Successful exploitation of this vulnerability could allow the attacker	N/A	More Details

	to cause damage to the targeted platform by abusing internal functionality.		
CVE-2026-22236	The vulnerability exists in BLUVOYIX due to improper authentication in the BLUVOYIX backend APIs. An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the vulnerable APIs. Successful exploitation of this vulnerability could allow the attacker to gain full access to customers' data and completely compromise the targeted platform.	N/A	More Details
CVE-2025-9466	A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. During execution of the Achilles EtherNet/IP and CIP grammar tests, the device reboots unexpectedly, causing the Link State Monitor to go down for several seconds.	N/A	More Details
CVE-2025-9465	A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. During execution of the Achilles Comprehensive grammar tests, the device reboots unexpectedly, causing the Link State Monitor to go down for several seconds.	N/A	More Details
CVE-2025-9464	A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. This vulnerability is triggered during fuzzing of multiple CIP classes, which causes the CIP port to become unresponsive.	N/A	More Details
CVE-2025-9283	A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. During execution of the Achilles EtherNet/IP Step Limits Storms tests, the device reboots unexpectedly, causing the Link State Monitor to go down for several seconds.	N/A	More Details
CVE-2025-9282	A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. During execution of the Achilles Comprehensive limited storm tests, the device reboots unexpectedly, causing the Link State Monitor to go down for several seconds.	N/A	More Details
CVE-2025-9281	A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. During execution of the Achilles Comprehensive step limit storm tests, the device reboots	N/A	More Details
CVE-2025-9280	A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. Fuzzing performed using Defensics causes the device to become unresponsive, requiring a reboot.	N/A	More Details
CVE-2025-9279	A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. During execution of the Achilles EtherNet/IP Step Limit Storm tests, the device reboots unexpectedly, causing the Link State Monitor to go down for several seconds.	N/A	More Details
CVE-2025-9278	A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. After running a Burp Suite active scan, the device loses ICMP connectivity, causing the web application to become inaccessible.	N/A	More Details
CVE-2026-23917	Rejected reason: Not used	N/A	More Details
CVE-2026-23916	Rejected reason: Not used	N/A	More Details
CVE-2026-23915	Rejected reason: Not used	N/A	More Details

CVE-2026-23944	Arcane is an interface for managing Docker containers, images, networks, and volumes. Prior to version 1.13.2, unauthenticated requests could be proxied to remote environment agents, allowing access to remote environment resources without authentication. The environment proxy middleware handled `/api/environments/{id}/...` requests for remote environments before authentication was enforced. When the environment ID was not local, the middleware proxied the request and attached the manager-held agent token, even if the caller was unauthenticated. This enabled unauthenticated access to remote environment operations (e.g., listing containers, streaming logs, or other agent endpoints). An unauthenticated attacker could access and manipulate remote environment resources via the proxy, potentially leading to data exposure, unauthorized changes, or service disruption. Version 1.13.2 patches the vulnerability.	N/A	More Details
CVE-2026-23877	Swing Music is a self-hosted music player for local audio files. Prior to version 2.1.4, Swing Music's `list_folders()` function in the `/folder/dir-browser` endpoint is vulnerable to directory traversal attacks. Any authenticated user (including non-admin) can browse arbitrary directories on the server filesystem. Version 2.1.4 fixes the issue.	N/A	More Details
CVE-2026-23875	CrawlChat is an open-source, AI-powered platform that transforms technical documentation into intelligent chatbots. Prior to version 0.0.8, a non-existing permission check for the CrawlChat's Discord bot allows non-manage guild users to put malicious content onto the collection knowledge base. Usually, admin / mods of a Discord guild use the `jigsaw` emoji to save a specific message (chain) onto the collection's knowledge base of CrawlChat. Unfortunately an permission check (for e.g. MANAGE_SERVER; MANAGE_MESSAGES etc.) was not done, allowing normal users of the guild to information to the knowledge base. With targeting specific parts that are commonly asked, users can manipulate the content given out by the bot (on all integrations), to e.g. redirect users to a malicious site, or send information to a malicious user. Version 0.0.8 patches the issue.	N/A	More Details
CVE-2026-23844	Whisper Money is a personal finance application. Versions prior to 0.1.5 have an insecure direct object reference vulnerability. A user can update/create account balances in other users' bank accounts. Version 0.1.5 fixes the issue.	N/A	More Details
CVE-2026-23852	SiYuan is a personal knowledge management system. Versions prior to 3.5.4 have a stored Cross-Site Scripting (XSS) vulnerability that allows an attacker to inject arbitrary HTML attributes into the `icon` attribute of a block via the `/api/attr/setBlockAttrs` API. The payload is later rendered in the dynamic icon feature in an unsanitized context, leading to stored XSS and, in the desktop environment, potential remote code execution (RCE). This issue bypasses the previous fix for issue `#15970` (XSS → RCE via dynamic icons). Version 3.5.4 contains an updated fix.	N/A	More Details
CVE-2026-23851	SiYuan is a personal knowledge management system. Versions prior to 3.5.4 contain a logic vulnerability in the /api/file/globalCopyFiles endpoint. The function allows authenticated users to copy files from any location on the server's filesystem into the application's workspace without proper path validation. The vulnerability exists in the api/file.go source code. The function globalCopyFiles accepts a list of source paths (srcs) from the JSON request body. While the code checks if the source file exists using filelock.IsExist(src), it fails to validate whether the source path resides within the authorized workspace directory. Version 3.5.4 patches the issue.	N/A	More Details
CVE-2026-23850	SiYuan is a personal knowledge management system. In versions prior to 3.5.4, the markdown feature allows unrestricted server side html-rendering which allows arbitrary file read (LFD). Version 3.5.4 fixes the issue.	N/A	More Details
	SiYuan is a personal knowledge management system. Versions prior to 3.5.4 are		

CVE-2026-23847	vulnerable to reflected cross-site scripting in /api/icon/getDynamicIcon due to unsanitized SVG input. The endpoint generates SVG images for text icons (type=8). The content query parameter is inserted directly into the SVG <text> tag without XML escaping. Since the response Content-Type is image/svg+xml, injecting unescaped tags allows breaking the XML structure and executing JavaScript. Version 3.5.4 patches the issue.]	N/A	More Details
CVE-2026-21696	Wings is the server control plane for Pterodactyl, a free, open-source game server management panel. Starting in version 1.7.0 and prior to version 1.12.0, Wings does not consider SQLite max parameter limit when processing activity log entries allowing for low privileged user to trigger a condition that floods the panel with activity records. After Wings sends activity logs to the panel it deletes the processed activity entries from the wings SQLite database. However, it does not consider the max parameter limit of SQLite, 32766 as of SQLite 3.32.0. If wings attempts to delete more than 32766 entries from the SQLite database in one query, it triggers an error (SQL logic error: too many SQL variables (1)) and does not remove any entries from the database. These entries are then indefinitely re-processed and resent to the panel each time the cron runs. By successfully exploiting this vulnerability, an attacker can trigger a situation where wings will keep uploading the same activity data to the panel repeatedly (growing each time to include new activity) until the panels' database server runs out of disk space. Version 1.12.0 fixes the issue.	N/A	More Details
CVE-2025-69199	Wings is the server control plane for Pterodactyl, a free, open-source game server management panel. Prior to version 1.12.0, websockets within wings lack proper rate limiting and throttling. As a result a malicious user can open a large number of connections and then request data through these sockets, causing an excessive volume of data over the network and overloading the host system memory and cpu. Additionally, there is not a limit applied to the total size of messages being sent or received, allowing a malicious user to open thousands of websocket connections and then send massive volumes of information over the socket, overloading the host network, and causing increased CPU and memory load within Wings. Version 1.12.0 patches the issue.	N/A	More Details
CVE-2026-20759	OS Command Injection vulnerability exists in multiple Network Cameras TRIFORA 3 series provided by TOA Corporation, which may allow a logged-in user with the low("monitoring user") or higher privilege to execute an arbitrary OS command.	N/A	More Details
CVE-2026-23838	Tandoor Recipes is a recipe manager than can be installed with the Nix package manager. Starting in version 23.05 and prior to version 26.05, when using the default configuration of Tandoor Recipes, specifically using SQLite and default `MEDIA_ROOT`, the full database file may be externally accessible, potentially on the Internet. The root cause is that the NixOS module configures the working directory of Tandoor Recipes, as well as the value of `MEDIA_ROOT`, to be `/var/lib/tandoor-recipes`. This causes Tandoor Recipes to create its `db.sqlite3` database file in the same directory as `MEDIA_ROOT` causing it to be accessible without authentication through HTTP like any other media file. This is the case when using `GUNICORN_MEDIA=1` or when using a web server like nginx to serve media files. NixOS 26.05 changes the default value of `MEDIA_ROOT` to a sub folder of the data directory. This only applies to configurations with `system.stateVersion` >= 26.05. For older configurations, one of the workarounds should be applied instead. NixOS 25.11 has received a backport of this patch, though it doesn't fix this vulnerability without user intervention. A recommended workaround is to move `MEDIA_ROOT` into a subdirectory. Non-recommended workarounds include switching to PostgreSQL or disallowing access to `db.sqlite3`.	N/A	More Details
	Pterodactyl is a free, open-source game server management panel. Pterodactyl implements rate limits that are applied to the total number of resources (e.g.		

CVE-2025-69198	databases, port allocations, or backups) that can exist for an individual server. These resource limits are applied on a per-server basis, and validated during the request cycle. However, in versions prior to 1.12.0, it is possible for a malicious user to send a massive volume of requests at the same time that would create more resources than the server is allotted. This is because the validation occurs early in the request cycle and does not lock the target resource while it is processing. As a result sending a large volume of requests at the same time would lead all of those requests to validate as not using any of the target resources, and then all creating the resources at the same time. As a result a server would be able to create more databases, allocations, or backups than configured. A malicious user is able to deny resources to other users on the system, and may be able to excessively consume the limited allocations for a node, or fill up backup space faster than is allowed by the system. Version 1.12.0 fixes the issue.	N/A	More Details
CVE-2026-23884	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.21.0, offscreen bitmap deletion leaves `gdi->drawing` pointing to freed memory, causing UAF when related update packets arrive. A malicious server can trigger a client-side use after free, causing a crash (DoS) and potential heap corruption with code-execution risk depending on allocator behavior and surrounding heap layout. Version 3.21.0 contains a patch for the issue.	N/A	More Details
CVE-2026-23883	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.21.0, `xf_Pointer_New` frees `cursorPixels` on failure, then `pointer_free` calls `xf_Pointer_Free` and frees it again, triggering ASan UAF. A malicious server can trigger a client-side use after free, causing a crash (DoS) and potential heap corruption with code-execution risk depending on allocator behavior and surrounding heap layout. Version 3.21.0 contains a patch for the issue.	N/A	More Details
CVE-2026-23833	ESPHome is a system to control microcontrollers remotely through Home Automation systems. In versions 2025.9.0 through 2025.12.6, an integer overflow in the API component's protobuf decoder allows denial-of-service attacks when API encryption is not used. The bounds check `ptr + field_length > end` in `components/api/proto.cpp` can overflow when a malicious client sends a large `field_length` value. This affects all ESPHome device platforms (ESP32, ESP8266, RP2040, LibreTiny). The overflow bypasses the out-of-bounds check, causing the device to read invalid memory and crash. When using the plaintext API protocol, this attack can be performed without authentication. When noise encryption is enabled, knowledge of the encryption key is required. Users should upgrade to ESPHome 2025.12.7 or later to receive a patch, enable API encryption with a unique key per device, and follow the Security Best Practices.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: mm/page_alloc: change all pageblocks migrate type on coalescing When a page is freed it coalesces with a buddy into a higher order page while possible. When the buddy page migrate type differs, it is expected to be updated to match the one of the page being freed. However, only the first pageblock of the buddy page is updated, while the rest of the pageblocks are left unchanged. That causes warnings in later expand() and other code paths (like below), since an inconsistency between migration type of the list containing the page and the page-owned pageblocks migration types is introduced. [308.986589] ------------[cut here]------------ [308.987227] page type is 0, passed migratetype is 1 (nr=256) [308.987275] WARNING: CPU: 1 PID: 5224 at mm/page_alloc.c:812 expand+0x23c/0x270 [308.987293] Modules linked in: algif_hash(E) af_alg(E) nft_fib_inet(E) nft_fib_ipv4(E) nft_fib_ipv6(E) nft_fib(E) nft_reject_inet(E) nf_reject_ipv4(E) nf_reject_ipv6(E) nft_reject(E) nft_ct(E) nft_chain_nat(E) nf_nat(E) nf_conntrack(E) nf_defrag_ipv6(E) nf_defrag_ipv4(E) nf_tables(E) s390_trng(E) vfio_ccw(E) mdev(E) vfio_iommu_type1(E) vfio(E) sch_fq_codel(E) drm(E) i2c_core(E) drm_panel_orientation_quirks(E) loop(E) nfnetlink(E) vsock_loopback(E) vmw_vsock_virtio_transport_common(E) vsock(E) ctcm(E) fsm(E) diag288_wdt(E) watchdog(E) zfcp(E) scsi_transport_fc(E)		

CVE-2025-71134	ghash_s390(E) prng(E) aes_s390(E) des_generic(E) des_s390(E) libdes(E) sha3_512_s390(E) sha3_256_s390(E) sha_common(E) paes_s390(E) crypto_engine(E) pkey_cca(E) pkey_ep11(E) zcrypt(E) rng_core(E) pkey_pckmo(E) pkey(E) autofs4(E) [308.987439] Unloaded tainted modules: hmac_s390(E):2 [308.987650] CPU: 1 UID: 0 PID: 5224 Comm: mempig_verify Kdump: loaded Tainted: G E 6.18.0-gcc-bpf-debug #431 PREEMPT [308.987657] Tainted: [E]=UNSIGNED_MODULE [308.987661] Hardware name: IBM 3906 M04 704 (z/VM 7.3.0) [308.987666] Krnl PSW : 0404f00180000000 00000349976fa600 (expand+0x240/0x270) [308.987676] R:0 T:1 IO:0 EX:0 Key:0 M:1 W:0 P:0 AS:3 CC:3 PM:0 RI:0 EA:3 [308.987682] Krnl GPRS: 0000034980000004 0000000000000005 0000000000000030 000003499a0e6d88 [308.987688] 0000000000000005 0000034980000005 000002be803ac000 0000023efe6c8300 [308.987692] 0000000000000008 0000034998d57290 000002be00000100 0000023e00000008 [308.987696] 0000000000000000 0000000000000000 00000349976fa5fc 000002c99b1eb6f0 [308.987708] Krnl Code: 00000349976fa5f0: c020008a02f2 larl %r2,000003499883abd4 00000349976fa5f6: c0e5ffe3f4b5 brasl %r14,0000034997378f60 #00000349976fa5fc: af000000 mc 0,0 >00000349976fa600: a7f4ff4c brc 15,00000349976fa498 00000349976fa604: b9040026 lgr %r2,%r6 00000349976fa608: c0300088317f larl %r3,0000034998800906 00000349976fa60e: c0e5fffdb6e1 brasl %r14,00000349976b13d0 00000349976fa614: af000000 mc 0,0 [308.987734] Call Trace: [308.987738] [<00000349976fa600>] expand+0x240/0x270 [308.987744] ([<00000349976fa5fc>] expand+0x23c/0x270) [308.987749] [<00000349976ff95e>] rmqueue_bulk+0x71e/0x940 [308.987754] [<00000349976ffd7e>] __rmqueue_pcplist+0x1fe/0x2a0 [308.987759] [<0000034997700966>] rmqueue.isra.0+0xb46/0xf40 [308.987763] [<0000034997703ec8>] get_page_from_freelist+0x198/0x8d0 [308.987768] [<0000034997706fa8>] __alloc_frozen_pages_noprof+0x198/0x400 [308.987774] [<00000349977536f8>] alloc_pages_mpol+0xb8/0x220 [308.987781] [<0000034997753bf6>] folio_alloc_mpol_noprof+0x26/0xc0 [308.987786] [<0000034997753e4c>] vma_alloc_folio_noprof+0x6c/0xa0 [308.987791] [<0000034997775b22>] vma_alloc_anon_folio_pmd+0x42/0x240 [308.987799] [<000003499777bfea>] __do_huge_pmd_anonymous_page+0x3a/0x210 [308.987804] [<00000349976cb0 ---truncated---	N/A	More Details
CVE-2026-22218	Chainlit versions prior to 2.9.4 contain an arbitrary file read vulnerability in the /project/element update flow. An authenticated client can send a custom Element with a user-controlled path value, causing the server to copy the referenced file into the attacker’s session. The resulting element identifier (chainlitKey) can then be used to retrieve the file contents via /project/file/<chainlitKey>, allowing disclosure of any file readable by the Chainlit service.	N/A	More Details
CVE-2026-23914	Rejected reason: Not used	N/A	More Details
CVE-2026-22219	Chainlit versions prior to 2.9.4 contain a server-side request forgery (SSRF) vulnerability in the /project/element update flow when configured with the SQLAlchemy data layer backend. An authenticated client can provide a user-controlled url value in an Element, which is fetched by the SQLAlchemy element creation logic using an outbound HTTP GET request. This allows an attacker to make arbitrary HTTP requests from the Chainlit server to internal network services or cloud metadata endpoints and store the retrieved responses via the configured storage provider.	N/A	More Details
CVE-2026-23913	Rejected reason: Not used	N/A	More Details

CVE-2026-23912	Rejected reason: Not used	N/A	More Details
CVE-2026-23911	Rejected reason: Not used	N/A	More Details
CVE-2026-23910	Rejected reason: Not used	N/A	More Details
CVE-2026-23909	Rejected reason: Not used	N/A	More Details
CVE-2025-71137	In the Linux kernel, the following vulnerability has been resolved: octeontx2-pf: fix "UBSAN: shift-out-of-bounds error" This patch ensures that the RX ring size (rx_pending) is not set below the permitted length. This avoids UBSAN shift-out-of-bounds errors when users passes small or zero ring sizes via ethtool -G.	N/A	More Details
CVE-2025-71136	In the Linux kernel, the following vulnerability has been resolved: media: adv7842: Avoid possible out-of-bounds array accesses in adv7842_cp_log_status() It's possible for cp_read() and hdmi_read() to return -EIO. Those values are further used as indexes for accessing arrays. Fix that by checking return values where it's needed. Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2026-23709	Rejected reason: Not used	N/A	More Details
CVE-2026-23710	Rejected reason: Not used	N/A	More Details
CVE-2026-23711	Rejected reason: Not used	N/A	More Details
CVE-2026-23712	Rejected reason: Not used	N/A	More Details
CVE-2026-23947	Orval generates type-safe JS clients (TypeScript) from any valid OpenAPI v3 or Swagger v2 specification. Versions 7.10.0 until 8.0.2 are vulnerable to arbitrary code execution in environments consuming generated clients. This issue is similar in nature to CVE-2026-22785, but affects a different code path in @orval/core that was not addressed by CVE-2026-22785's fix. The vulnerability allows untrusted OpenAPI specifications to inject arbitrary TypeScript/JavaScript code into generated clients via the x-enumDescriptions field, which is embedded without proper escaping in getEnumImplementation(). I have confirmed that the injection occurs during const enum generation and results in executable code within the generated schema files. Orval 8.0.2 contains a fix for the issue.	N/A	More Details
CVE-2026-23713	Rejected reason: Not used	N/A	More Details
CVE-2026-	Rejected reason: Not used	N/A	More Details

23714			
CVE-2025-71135	In the Linux kernel, the following vulnerability has been resolved: md/raid5: fix possible null-pointer dereferences in raid5_store_group_thread_cnt() The variable mddev->private is first assigned to conf and then checked: conf = mddev->private; if (!conf) ... If conf is NULL, then mddev->private is also NULL. In this case, null-pointer dereferences can occur when calling raid5_quiesce(): raid5_quiesce(mddev, true); raid5_quiesce(mddev, false); since mddev->private is assigned to conf again in raid5_quiesce(), and conf is dereferenced in several places, for example: conf->quiesce = 0; wake_up(&conf->wait_for_quiescent); To fix this issue, the function should unlock mddev and return before invoking raid5_quiesce() when conf is NULL, following the existing pattern in raid5_change_consistency_policy().	N/A	More Details
CVE-2026-0933	SummaryA command injection vulnerability (CWE-78) has been found to exist in the `wrangler pages deploy` command. The issue occurs because the `--commit-hash` parameter is passed directly to a shell command without proper validation or sanitization, allowing an attacker with control of `--commit-hash` to execute arbitrary commands on the system running Wrangler. Root causeThe commitHash variable, derived from user input via the --commit-hash CLI argument, is interpolated directly into a shell command using template literals (e.g., execSync(`git show -s --format=%B ${commitHash}`)). Shell metacharacters are interpreted by the shell, enabling command execution. ImpactThis vulnerability is generally hard to exploit, as it requires --commit-hash to be attacker controlled. The vulnerability primarily affects CI/CD environments where `wrangler pages deploy` is used in automated pipelines and the --commit-hash parameter is populated from external, potentially untrusted sources. An attacker could exploit this to: * Run any shell command. * Exfiltrate environment variables. * Compromise the CI runner to install backdoors or modify build artifacts. Credits Disclosed responsibly by kny4hacker. Mitigation * Wrangler v4 users are requested to upgrade to Wrangler v4.59.1 or higher. * Wrangler v3 users are requested to upgrade to Wrangler v3.114.17 or higher. * Users on Wrangler v2 (EOL) should upgrade to a supported major version.	N/A	More Details