SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 29 October 2025

Generated on 29 October 2025

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-64095	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to 10.1.1, the default HTML editor provider allows unauthenticated file uploads and images can overwrite existing files. An unauthenticated user can upload and replace existing files allowing defacing a website and combined with other issue, injection XSS payloads. This vulnerability is fixed in 10.1.1.	10.0	More Details
CVE-2025-57870	A SQL Injection vulnerability exists in Esri ArcGIS Server versions 11.3, 11.4 and 11.5 on Windows, Linux and Kubernetes. This vulnerability allows a remote, unauthenticated attacker to execute arbitrary SQL commands via a specific ArcGIS Feature Service operation. Successful exploitation can potentially result in unauthorized access, modification, or deletion of data from the underlying Enterprise Geodatabase.	10.0	More Details
CVE-2025-48106	Unrestricted Upload of File with Dangerous Type vulnerability in CMSSuperHeroes Clanora clanora allows Using Malicious Files.This issue affects Clanora: from n/a through < 1.3.1.	10.0	More Details
CVE-2025-49060	Unrestricted Upload of File with Dangerous Type vulnerability in CMSSuperHeroes Wastia wastia allows Upload a Web Shell to a Web Server.This issue affects Wastia: from n/a through < 1.1.3.	10.0	More Details
CVE-2025-61481	An issue in MikroTik RouterOS v.7.14.2 and SwitchOS v.2.18 allows a remote attacker to execute arbitrary code via the HTTP- only WebFig management component	10.0	More Details
CVE-2025-61934	A binding to an unrestricted IP address vulnerability was discovered in Productivity Suite software version v4.4.1.19. The vulnerability allows an unauthenticated remote attacker to interact with the ProductivityService PLC simulator and read, write, or delete arbitrary files and folders on the target machine	10.0	More Details
CVE-2025-60206	Improper Control of Generation of Code ('Code Injection') vulnerability in Bearsthemes Alone alone allows Code Injection.This issue affects Alone: from n/a through <= 7.8.3.	10.0	More Details
CVE-2025-59503	Server-side request forgery (ssrf) in Azure Compute Gallery allows an authorized attacker to elevate privileges over a network.	9.9	More Details
CVE-2025-58428	The TLS4B ATG system's SOAP-based interface is vulnerable due to its accessibility through the web services handler. This vulnerability enables remote attackers with valid credentials to execute system-level commands on the underlying Linux system. This could allow the attacker to achieve remote command execution, full shell access, and potential lateral movement within the network.	9.9	More Details
CVE-2025-47699	Exposure of Sensitive System Information to an Unauthorized Control Sphere (CWE-497) in the Gallagher Morpho integration could allow an authenticated operator with limited site permissions to make critical changes to local Morpho devices. This issue affects Command Centre Server: 9.30 prior to vEL9.30.2482 (MR2), 9.20 prior to vEL9.20.2819 (MR4), 9.10 prior to vEL9.10.3672 (MR7), 9.00 prior to vEL9.00.3831 (MR8), all versions of 8.90 and prior.	9.9	More Details
CVE-2025-58963	Unrestricted Upload of File with Dangerous Type vulnerability in 7oroof Medcity medcity allows Upload a Web Shell to a Web Server.This issue affects Medcity: from n/a through < 1.1.9.	9.8	More Details
CVE-2025-60803	Antabot White-Jotter up to commit 9bcadc was discovered to contain an unauthenticated remote code execution (RCE) vulnerability via the component /api/aaa;/../register.	9.8	More Details
	Inclusion of Functionality from Untrusted Control Sphere, Improper Control of Filename for Include/Require Statement		

CVE-2025-11023	in PHP Program ('PHP Remote File Inclusion') vulnerability in ArkSigner Software and Hardware Inc. AcBakImzala allows PHP Local File Inclusion.This issue affects AcBakImzala: before v5.1.4.	9.8	More Details
CVE-2025-11253	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Aksis Technology Inc. Netty ERP allows SQL Injection.This issue affects Netty ERP: before V.1.1000.	9.8	More Details
CVE-2025-43995	Dell Storage Center - Dell Storage Manager, version(s) 20.1.21, contain(s) an Improper Authentication vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Protection mechanism bypass. Authentication Bypass in DSM Data Collector. An unauthenticated remote attacker can access APIs exposed by ApiProxy.war in DataCollectorEar.ear by using a special SessionKey and UserId. These userid are special users created in compellentservicesapi for special purposes.	9.8	More Details
CVE-2025-60548	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formLanSetupRouterSettings.	9.8	More Details
CVE-2025-60553	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formSetWAN_Wizard52.	9.8	More Details
CVE-2025-60554	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formSetEnableWizard.	9.8	More Details
CVE-2025-62906	Missing Authorization vulnerability in epiphanyit321 Referral Link Tracker referral-link-tracker allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Referral Link Tracker: from n/a through <= 1.1.4.	9.8	More Details
CVE-2025-62025	Deserialization of Untrusted Data vulnerability in eyecix JobSearch wp-jobsearch.This issue affects JobSearch: from n/a through < 3.0.8.	9.8	More Details
CVE-2025-62908	Missing Authorization vulnerability in gerritvanaaken Podlove Web Player podlove-web-player allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Podlove Web Player: from n/a through <= 5.9.1.	9.8	More Details
CVE-2025-62944	Missing Authorization vulnerability in Mark O'Donnell MSTW CSV EXPORTER mstw-csv-exporter allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MSTW CSV EXPORTER: from n/a through <= 1.4.	9.8	More Details
CVE-2025-49901	Authentication Bypass Using an Alternate Path or Channel vulnerability in quantumcloud Simple Link Directory qc-simple-link-directory allows Authentication Abuse.This issue affects Simple Link Directory: from n/a through < 14.8.1.	9.8	More Details
CVE-2025-27224	TRUfusion Enterprise through 7.10.4.0 uses the /trufusionPortal/fileupload endpoint to upload files. However, the application doesn't properly sanitize the input to this endpoint, ultimately allowing path traversal sequences to be included. This can be used to write to any filename with any file type at any location on the local server, ultimately allowing execution of arbitrary code.	9.8	More Details
CVE-2025-62516	Landlord Onboarding & Rental Signup introduces the landlord onboarding workflow and rental signup system for VivaTurbo Rentals & Property Services. In 2.0.0 and earlier, a vulnerability was identified in the TurboTenant property listing activation workflow that could allow unauthorized access to certain Stripe payment session data. This could potentially expose sensitive business metadata, including landlord dashboard sync details and tenant information. The issue affects the API endpoints handling the property listing activation, subscription metadata, and payment link generation.	9.8	More Details
CVE-2025-36386	IBM Maximo Application Suite 9.0.0 through 9.0.15 and 9.1.0 through 9.1.4 could allow a remote attacker to bypass authentication mechanisms and gain unauthorized access to the application.	9.8	More Details
CVE-2025-56447	TM2 Monitoring v3.04 contains an authentication bypass and plaintext credential disclosure.	9.8	More Details
CVE-2025-6440	The WooCommerce Designer Pro plugin for WordPress, used by the Pricom - Printing Company & Design Services WordPress theme, is vulnerable to arbitrary file uploads due to missing file type validation in the 'wcdp_save_canvas_design_ajax' function in all versions up to, and including, 1.9.26. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2025-62023	Improper Control of Generation of Code ('Code Injection') vulnerability in Cristián Lávaque s2Member s2member.This issue affects s2Member: from n/a through <= 250905.	9.8	More Details
CVE-2025-60221	Deserialization of Untrusted Data vulnerability in captivateaudio Captivate Sync captivatesync-trade allows Object Injection.This issue affects Captivate Sync: from n/a through <= 3.0.3.	9.8	More Details
CVE-2025-60039	Deserialization of Untrusted Data vulnerability in rascals Noisa noisa allows Object Injection.This issue affects Noisa: from n/a through <= 2.6.0.	9.8	More Details
CVE-2025-60209	Deserialization of Untrusted Data vulnerability in CRM Perks Connector for Gravity Forms and Google Sheets wp-gravity-forms-spreadsheets allows Object Injection.This issue affects Connector for Gravity Forms and Google Sheets: from n/a through <= 1.2.6.	9.8	More Details
CVE-2025-60210	Deserialization of Untrusted Data vulnerability in wpeverest Everest Forms - Frontend Listing everest-forms-frontend-listing allows Object Injection.This issue affects Everest Forms - Frontend Listing: from n/a through <= 1.0.5.	9.8	More Details
CVE-2025-60213	Deserialization of Untrusted Data vulnerability in Whitebox-Studio Scape scape allows Object Injection.This issue affects Scape: from n/a through <= 1.5.13.	9.8	More Details
CVE-2025-60214	Deserialization of Untrusted Data vulnerability in BoldThemes Goldenblatt goldenblatt allows Object Injection.This issue affects Goldenblatt: from n/a through <= 1.2.1.	9.8	More Details

CVE-2025-60238	Deserialization of Untrusted Data vulnerability in universam UNIVERSAM universam-demo allows Object Injection.This issue affects UNIVERSAM: from n/a through <= 8.72.34.	9.8	More Details
CVE-2025-60220	Incorrect Privilege Assignment vulnerability in pebas CouponXxL couponxxl allows Privilege Escalation.This issue affects CouponXxL: from n/a through <= 3.0.0.	9.8	More Details
CVE-2025-60216	Deserialization of Untrusted Data vulnerability in BoldThemes Addison addison allows Object Injection.This issue affects Addison: from n/a through <= 1.4.2.	9.8	More Details
CVE-2025-60224	Deserialization of Untrusted Data vulnerability in wpshuffle Subscribe to Download subscribe-to-download allows Object Injection.This issue affects Subscribe to Download: from n/a through <= 2.0.9.	9.8	More Details
CVE-2025-60226	Deserialization of Untrusted Data vulnerability in axiomthemes White Rabbit whiterabbit allows Object Injection.This issue affects White Rabbit: from n/a through <= 1.5.2.	9.8	More Details
CVE-2025-60225	Deserialization of Untrusted Data vulnerability in AncoraThemes BugsPatrol bugspatrol allows Object Injection.This issue affects BugsPatrol: from n/a through <= 1.5.0.	9.8	More Details
CVE-2025-60232	Deserialization of Untrusted Data vulnerability in quantumcloud KBx Pro Ultimate knowledgebase-helpdesk-pro allows Object Injection.This issue affects KBx Pro Ultimate: from n/a through <= 8.0.5.	9.8	More Details
CVE-2025-41723	The importFile SOAP method is vulnerable to a directory traversal attack. An unauthenticated remote attacker bypass the path restriction and upload files to arbitrary locations.	9.8	More Details
CVE-2025-55754	Improper Neutralization of Escape, Meta, or Control Sequences vulnerability in Apache Tomcat. Tomcat did not escape ANSI escape sequences in log messages. If Tomcat was running in a console on a Windows operating system, and the console supported ANSI escape sequences, it was possible for an attacker to use a specially crafted URL to inject ANSI escape sequences to manipulate the console and the clipboard and attempt to trick an administrator into running an attacker controlled command. While no attack vector was found, it may have been possible to mount this attack on other operating systems. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.10, from 10.1.0-M1 through 10.1.44, from 9.0.40 through 9.0.108. The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.60 though 8.5.100. Other, older, EOL versions may also be affected. Users are recommended to upgrade to version 11.0.11 or later, 10.1.45 or later or 9.0.109 or later, which fix the issue.	9.6	More Details
CVE-2025-61385	SQL injection vulnerability in tlocke pg8000 1.31.4 allows remote attackers to execute arbitrary SQL commands via a specially crafted Python list input to function pg8000.native.literal.	9.6	More Details
CVE-2025-59557	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ThemeMove Learts Addons learts-addons allows SQL Injection.This issue affects Learts Addons: from n/a through < 1.7.5.	9.3	More Details
CVE-2025-49915	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cozy Vision SMS Alert Order Notifications sms-alert allows SQL Injection.This issue affects SMS Alert Order Notifications: from n/a through <= 3.8.5.	9.3	More Details
CVE-2025-49931	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CrocoBlock JetSearch jet-search allows Blind SQL Injection.This issue affects JetSearch: from n/a through <= 3.5.10.	9.3	More Details
CVE-2025-10561	The device is running an outdated operating system, which may be susceptible to known vulnerabilities.	9.3	More Details
CVE-2025-62892	Missing Authorization vulnerability in sunshinephotocart Sunshine Photo Cart sunshine-photo-cart allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Sunshine Photo Cart: from n/a through <= 3.5.3.	9.1	More Details
CVE-2025-62919	Missing Authorization vulnerability in themeshopy TS Demo Importer ts-demo-importer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects TS Demo Importer: from n/a through <= 0.1.2.	9.1	More Details
CVE-2025-62959	Improper Control of Generation of Code ('Code Injection') vulnerability in videowhisper Paid Videochat Turnkey Site ppv-live-webcams allows Remote Code Inclusion.This issue affects Paid Videochat Turnkey Site: from n/a through <= 7.3.22.	9.1	More Details
CVE-2025-62717	Emlog is an open source website building system. In version 2.5.23, Emlog Pro is vulnerable to a session verification code error due to a clearing logic error. This means the verification code could be reused anywhere an email verification code is required. This issue has been fixed in commit 1f726df.	9.1	More Details
CVE-2025-60291	An issue was discovered in eTimeTrackLite Web thru 12.0 (20250704). There is a permission control flaw that allows unauthorized attackers to access specific routes and modify database connection configurations.	9.1	More Details
CVE-2025-52758	Unrestricted Upload of File with Dangerous Type vulnerability in Gesundheit Bewegt GmbH Zippy zippy allows Using Malicious Files.This issue affects Zippy: from n/a through <= 1.7.0.	9.1	More Details
CVE-2025-52741	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Barry Kooij Post Connector post-connector allows Reflected XSS.This issue affects Post Connector: from n/a through <= 1.0.11.	9.0	More Details
CVE-2025-62368	Taiga is an open source project management platform. In versions 6.8.3 and earlier, a remote code execution vulnerability exists in the Taiga API due to unsafe deserialization of untrusted data. This issue is fixed in version 6.9.0.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE-2025-62929	Missing Authorization vulnerability in PickPlugins Testimonial Slider testimonial allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Testimonial Slider: from n/a through <= 2.0.15.	8.8	More Details
CVE-2025-62924	Missing Authorization vulnerability in PickPlugins Post Grid and Gutenberg Blocks post-grid allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Post Grid and Gutenberg Blocks: from n/a through <= 2.3.17.	8.8	More Details
CVE-2025-12239	A weakness has been identified in TOTOLINK A3300R 17.0.0cu.557_B20221024. The impacted element is the function setDdnsCfg of the file /cgi-bin/cstecgi.cgi. Executing manipulation can lead to buffer overflow. The attack may be performed from remote. The exploit has been made available to the public and could be exploited.	8.8	More Details
CVE-2025-12240	A security vulnerability has been detected in TOTOLINK A3300R 17.0.0cu.557_B20221024. This affects the function setDmzCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ip leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2025-12241	A vulnerability was detected in TOTOLINK A3300R 17.0.0cu.557_B20221024. This impacts the function setLanguageCfg of the file /cgi-bin/cstecgi.cgi of the component POST Parameter Handler. The manipulation of the argument lang results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2025-62931	Missing Authorization vulnerability in microsoftstart MSN Partner Hub microsoft-start allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MSN Partner Hub: from n/a through <= 2.8.7.	8.8	More Details
CVE-2025-52737	Deserialization of Untrusted Data vulnerability in Tijmen Smit WP Store Locator wp-store-locator allows Object Injection.This issue affects WP Store Locator: from n/a through <= 2.2.260.	8.8	More Details
CVE-2025-52740	Deserialization of Untrusted Data vulnerability in Hernan Villanueva Boldermail boldermail allows Object Injection.This issue affects Boldermail: from n/a through <= 2.4.0.	8.8	More Details
CVE-2025-12258	A vulnerability was detected in TOTOLINK A3300R 17.0.0cu.557_B20221024. Impacted is the function setOpModeCfg of the file /cgi-bin/cstecgi.cg of the component POST Parameter Handler. The manipulation of the argument opmode results in stack-based buffer overflow. The attack may be performed from remote.	8.8	More Details
CVE-2025-12259	A flaw has been found in TOTOLINK A3300R 17.0.0cu.557_B20221024. The affected element is the function setScheduleCfg of the file /cgi-bin/cstecgi.cgi of the component POST Parameter Handler. This manipulation of the argument recHour causes stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2025-12260	A vulnerability has been found in TOTOLINK A3300R 17.0.0cu.557_B20221024. The impacted element is the function setSyslogCfg of the file /cgi-bin/cstecgi.cgi of the component POST Parameter Handler. Such manipulation of the argument enable leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-12265	A weakness has been identified in Tenda CH22 1.0.0.1. Affected by this issue is the function fromVirtualSer of the file /goform/VirtualSer. This manipulation of the argument page causes buffer overflow. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	8.8	More Details
CVE-2025-12271	A vulnerability was identified in Tenda CH22 1.0.0.1. This affects the function fromRouteStatic of the file /goform/RouteStatic. Such manipulation of the argument page leads to buffer overflow. The attack can be launched remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2025-60208	Cross-Site Request Forgery (CSRF) vulnerability in Tusko Trush Advanced Custom Fields : CPT Options Pages acf-cpt-options-pages allows Object Injection.This issue affects Advanced Custom Fields : CPT Options Pages: from n/a through <= 2.0.9.	8.8	More Details
CVE-2025-12272	A security flaw has been discovered in Tenda CH22 1.0.0.1. This impacts the function fromAddressNat of the file /goform/addressNat. Performing manipulation of the argument page results in buffer overflow. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	8.8	More Details
CVE-2025-12273	A weakness has been identified in Tenda CH22 1.0.0.1. Affected is the function fromwebExcptypemanFilter of the file /goform/webExcptypemanFilter. Executing manipulation of the argument page can lead to buffer overflow. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	8.8	More Details
CVE-2025-12274	A security vulnerability has been detected in Tenda CH22 1.0.0.1. Affected by this vulnerability is the function fromP2pListFilter of the file /goform/P2pListFilter. The manipulation of the argument page leads to buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2025-53428	Incorrect Privilege Assignment vulnerability in N-Media Simple User Registration wp-registration allows Privilege Escalation.This issue affects Simple User Registration: from n/a through <= 6.4.	8.8	More Details
CVE-2025-48082	Incorrect Privilege Assignment vulnerability in Progress Planner Progress Planner progress-planner allows Privilege Escalation.This issue affects Progress Planner: from n/a through <= 1.8.0.	8.8	More Details
CVE-2025-62918	Missing Authorization vulnerability in ignitionwp IgnitionDeck ignitiondeck allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects IgnitionDeck: from n/a through <= 2.0.10.	8.8	More Details
CVE-2025-	Incorrect Privilege Assignment vulnerability in GoodLayers Goodlayers Core goodlayers-core allows Privilege Escalation.This issue affects Goodlayers Core: from n/a through < 2.1.7.	8.8	More Details

59580			
CVE-2025-62916	Missing Authorization vulnerability in adivaha® Flights & Hotels Booking WP Plugin adiaha-hotel allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Flights & Hotels Booking WP Plugin: from n/a through <= 3.1.	8.8	More Details
CVE-2025-60041	Authentication Bypass Using an Alternate Path or Channel vulnerability in Iulia Cazan Emails Catch All emails-catch-all allows Password Recovery Exploitation.This issue affects Emails Catch All: from n/a through <= 3.5.3.	8.8	More Details
CVE-2025-54968	An issue was discovered in BAE SOCET GXP before 4.6.0.2. The SOCET GXP Job Service does not require authentication. In some configurations, this may allow remote users to submit jobs, or local users to submit jobs that will execute with the permissions of other users.	8.8	More Details
CVE-2025-62932	Missing Authorization vulnerability in wprio Table Block by RioVizual riovizual allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Table Block by RioVizual: from n/a through <= 2.3.2.	8.8	More Details
CVE-2025-12236	A vulnerability was determined in Tenda CH22 1.0.0.1. This issue affects the function fromDhcpListClient of the file /goform/DhcpListClient. This manipulation of the argument page causes buffer overflow. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2025-12234	A vulnerability has been found in Tenda CH22 1.0.0.1. This affects the function fromSafeMacFilter of the file /goform/SafeMacFilter. The manipulation of the argument page leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-12233	A flaw has been found in Tenda CH22 1.0.0.1. Affected by this issue is the function fromSafeUrlFilter of the file /goform/SafeUrlFilter. Executing manipulation of the argument page can lead to buffer overflow. The attack can be launched remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2025-31634	Deserialization of Untrusted Data vulnerability in designthemes Insurance insurance allows Object Injection.This issue affects Insurance: from n/a through <= 3.5.	8.8	More Details
CVE-2025-62962	Cross-Site Request Forgery (CSRF) vulnerability in Andrea Landonio CloudSearch cloud-search allows Stored XSS.This issue affects CloudSearch: from n/a through <= 3.0.0.	8.8	More Details
CVE-2025-62958	Cross-Site Request Forgery (CSRF) vulnerability in Clifton Griffin Simple Content Templates for Blog Posts & Pages simple-post-template allows Cross Site Request Forgery.This issue affects Simple Content Templates for Blog Posts & Pages: from n/a through <= 2.2.61.	8.8	More Details
CVE-2025-62957	Cross-Site Request Forgery (CSRF) vulnerability in NikanWP NikanWP WooCommerce Reporting wc-reports-lite allows Stored XSS.This issue affects NikanWP WooCommerce Reporting: from n/a through <= 1.0.0.	8.8	More Details
CVE-2025-62956	Cross-Site Request Forgery (CSRF) vulnerability in iseremet Reloadly reloadly-topup-widget allows Stored XSS.This issue affects Reloadly: from n/a through <= 2.0.1.	8.8	More Details
CVE-2025-62954	Missing Authorization vulnerability in Codeinwp Revive Old Posts tweet-old-post allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Revive Old Posts: from n/a through <= 9.3.3.	8.8	More Details
CVE-2025-62953	Missing Authorization vulnerability in nanbu Welcart e-Commerce usc-e-shop allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Welcart e-Commerce: from n/a through <= 2.11.24.	8.8	More Details
CVE-2025-62980	Missing Authorization vulnerability in MDZ Persian Admnin Fonts persian-admin-fonts allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Persian Admnin Fonts: from n/a through <= 4.1.03.	8.8	More Details
CVE-2025-62952	Missing Authorization vulnerability in QuantumCloud ChatBot chatbot allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ChatBot: from n/a through <= 7.3.0.	8.8	More Details
CVE-2025-62946	Missing Authorization vulnerability in everestthemes Everest Backup everest-backup allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Everest Backup: from n/a through <= 2.3.8.	8.8	More Details
CVE-2025-62945	Cross-Site Request Forgery (CSRF) vulnerability in Eduard Pinuaga Linares Did Prestashop Display did-prestashop-display allows Stored XSS.This issue affects Did Prestashop Display: from n/a through <= 1.0.30.	8.8	More Details
CVE-2025-12209	A vulnerability was determined in Tenda O3 1.0.0.10(2478). Affected is the function SetValue/GetValue of the file /goform/setDhcpConfig. Executing manipulation of the argument dhcpEn can lead to stack-based buffer overflow. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2025-12210	A vulnerability was identified in Tenda O3 1.0.0.10(2478). Affected by this vulnerability is the function SetValue/GetValue of the file /goform/AdvSetLanip. The manipulation of the argument lanIp leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-	A security flaw has been discovered in Tenda O3 1.0.0.10(2478). Affected by this issue is the function SetValue/GetValue of the		

2025-12211	file /goform/setDmzInfo. The manipulation of the argument dmzIP results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	8.8	More Details
CVE-2025-12212	A weakness has been identified in Tenda O3 1.0.0.10(2478). This affects the function SetValue/GetValue of the file /goform/setNetworkService. This manipulation of the argument upnpEn causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	8.8	More Details
CVE-2025-12213	A security vulnerability has been detected in Tenda O3 1.0.0.10(2478). This vulnerability affects the function SetValue/GetValue of the file /goform/setVlanConfig. Such manipulation of the argument lan leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2025-12214	A vulnerability was detected in Tenda O3 1.0.0.10(2478). This issue affects the function SetValue/GetValue of the file /goform/sysAutoReboot. Performing manipulation of the argument enable results in stack-based buffer overflow. The attack may be initiated remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2025-62934	Cross-Site Request Forgery (CSRF) vulnerability in Mejar WP Business Hours wp-business-hours allows Stored XSS.This issue affects WP Business Hours: from n/a through <= 1.4.	8.8	More Details
CVE-2025-12225	A vulnerability has been found in Tenda AC6 15.03.06.50. This issue affects some unknown processing of the file /goform/WifiGuestSet of the component HTTP Request Handler. Such manipulation of the argument shareSpeed leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-62933	Cross-Site Request Forgery (CSRF) vulnerability in Prakash Awesome Testimonials awesome-testimonials allows Stored XSS.This issue affects Awesome Testimonials: from n/a through <= 2.2.1.	8.8	More Details
CVE-2025-12232	A vulnerability was detected in Tenda CH22 1.0.0.1. Affected by this vulnerability is the function fromSafeClientFilter of the file /goform/SafeClientFilter. Performing manipulation of the argument page results in buffer overflow. The attack can be initiated remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2025-62896	Cross-Site Request Forgery (CSRF) vulnerability in digitaldonkey Multilang Contact Form multilang-contact-form allows Stored XSS.This issue affects Multilang Contact Form: from n/a through <= 1.5.	8.8	More Details
CVE-2025-32283	Deserialization of Untrusted Data vulnerability in designthemes Solar Energy solar allows Object Injection.This issue affects Solar Energy: from n/a through <= 3.5.	8.8	More Details
CVE-2025-62007	Incorrect Privilege Assignment vulnerability in bPlugins Voice Feedback voice-feedback allows Privilege Escalation.This issue affects Voice Feedback: from n/a through <= 1.0.3.	8.8	More Details
CVE-2025-12095	The Simple Registration for WooCommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5.8. This is due to missing nonce validation on the role requests admin page handler in the includes/display-role-admin.php file. This makes it possible for unauthenticated attackers to approve pending role requests and escalate user privileges via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2025-12028	The IndieAuth plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.5.4. This is due to missing nonce verification on the `login_form_indieauth()` function and the authorization endpoint at wp-login.php?action=indieauth. This makes it possible for unauthenticated attackers to force authenticated users to approve OAuth authorization requests for attacker-controlled applications via a forged request granted they can trick a user into performing an action such as clicking on a link or visiting a malicious page while logged in. The attacker can then exchange the stolen authorization code for an access token, effectively taking over the victim's account with the granted scopes (create, update, delete).	8.8	More Details
CVE-2025-60211	Incorrect Privilege Assignment vulnerability in extendons WooCommerce Registration Fields Plugin - Custom Signup Fields extendons-registration-fields allows Privilege Escalation.This issue affects WooCommerce Registration Fields Plugin - Custom Signup Fields: from n/a through <= 3.2.3.	8.8	More Details
CVE-2025-12322	A flaw has been found in Tenda CH22 1.0.0.1. Affected by this issue is the function fromNatStaticSetting of the file /goform/NatStaticSetting. Executing manipulation of the argument page can lead to buffer overflow. It is possible to launch the attack remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2025-62886	Cross-Site Request Forgery (CSRF) vulnerability in wpdevart Pricing Table builder wpdevart-pricing-table allows Stored XSS.This issue affects Pricing Table builder: from n/a through <= 1.5.1.	8.8	More Details
CVE-2025-10680	OpenVPN 2.7_alpha1 through 2.7_beta1 on POSIX based platforms allows a remote authenticated server to inject shell commands via DNS variables when --dns-updown is in use	8.8	More Details
CVE-2025-62498	A relative path traversal (ZipSlip) vulnerability was discovered in Productivity Suite software version 4.4.1.19. The vulnerability allows an attacker who can tamper with a productivity project to execute arbitrary code on the machine where the project is opened.	8.8	More Details
CVE-2025-62889	Missing Authorization vulnerability in KingAddons.com King Addons for Elementor king-addons allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects King Addons for Elementor: from n/a through <= 51.1.37.	8.8	More Details
CVE-2025-	Deserialization of Untrusted Data vulnerability in acowebs Product Table For WooCommerce product-table-for-	8.8	More

62008	woocommerce.This issue affects Product Table For WooCommerce: from n/a through <= 1.2.4.		Details
CVE-2025-62606	my little forum is a PHP and MySQL based internet forum that displays the messages in classical threaded view. Prior to version 2.5.12, an authenticated SQL injection vulnerability in the bookmark reordering feature allows any logged-in user to execute arbitrary SQL commands. This can lead to a full compromise of the application's database, including reading, modifying, or deleting all data. This issue has been patched in version 2.5.12.	8.8	More Details
CVE-2025-62890	Cross-Site Request Forgery (CSRF) vulnerability in Premmerce Premmerce Brands for WooCommerce premmerce-woocommerce-brands allows Cross Site Request Forgery.This issue affects Premmerce Brands for WooCommerce: from n/a through <= 1.2.13.	8.8	More Details
CVE-2025-60234	Deserialization of Untrusted Data vulnerability in designthemes Single Property single-property allows Object Injection.This issue affects Single Property: from n/a through <= 2.8.	8.8	More Details
CVE-2025-11893	The Charitable – Donation Plugin for WordPress – Fundraising with Recurring Donations & More plugin for WordPress is vulnerable to SQL Injection via the donation_ids parameter in all versions up to, and including, 1.8.8.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation of the vulnerability requires a paid donation.	8.8	More Details
CVE-2025-41719	A low privileged remote attacker can corrupt the webserver users storage on the device by setting a sequence of unsupported characters which leads to deletion of all previously configured users and the creation of the default Administrator with a known default password.	8.8	More Details
CVE-2025-62891	Cross-Site Request Forgery (CSRF) vulnerability in Jory Hogeveen Off-Canvas Sidebars & Menus (Slidebars) off-canvas-sidebars allows Cross Site Request Forgery.This issue affects Off-Canvas Sidebars & Menus (Slidebars): from n/a through <= 0.5.8.5.	8.8	More Details
CVE-2025-60212	Deserialization of Untrusted Data vulnerability in designthemes VEDA veda allows Object Injection.This issue affects VEDA: from n/a through <= 4.2.	8.8	More Details
CVE-2025-6979	Captive Portal can allow authentication bypass	8.8	More Details
CVE-2025-60215	Deserialization of Untrusted Data vulnerability in designthemes Kriya kriya allows Object Injection.This issue affects Kriya: from n/a through <= 3.4.	8.8	More Details
CVE-2025-60222	Incorrect Privilege Assignment vulnerability in FantasticPlugins SUMO Memberships for WooCommerce sumomemberships allows Privilege Escalation.This issue affects SUMO Memberships for WooCommerce: from n/a through <= 7.6.0.	8.8	More Details
CVE-2025-60425	Nagios Fusion v2024R1.2 and v2024R2 does not invalidate already existing session tokens when the two-factor authentication mechanism is enabled, allowing attackers to perform a session hijacking attack.	8.6	More Details
CVE-2025-27222	TRUfusion Enterprise through 7.10.4.0 uses the /trufusionPortal/getCobrandingData endpoint to retrieve files. However, the application doesn't properly sanitize the input to this endpoint, ultimately allowing path traversal sequences to be included. This can be used to read any local server file that is accessible by the TRUfusion user and can also be used to leak cleartext passwords of TRUfusion Enterprise itself.	8.6	More Details
CVE-2025-40780	In specific circumstances, due to a weakness in the Pseudo Random Number Generator (PRNG) that is used, it is possible for an attacker to predict the source port and query ID that BIND will use. This issue affects BIND 9 versions 9.16.0 through 9.16.50, 9.18.0 through 9.18.39, 9.20.0 through 9.20.13, 9.21.0 through 9.21.12, 9.16.8-S1 through 9.16.50-S1, 9.18.11-S1 through 9.18.39-S1, and 9.20.9-S1 through 9.20.13-S1.	8.6	More Details
CVE-2025-49916	Missing Authorization vulnerability in MultiVendorX MultiVendorX dc-woocommerce-multi-vendor allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects MultiVendorX: from n/a through <= 4.2.23.	8.6	More Details
CVE-2025-60227	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ThimPress WP Pipes wp-pipes allows Path Traversal.This issue affects WP Pipes: from n/a through <= 1.4.3.	8.6	More Details
CVE-2025-40778	Under certain circumstances, BIND is too lenient when accepting records from answers, allowing an attacker to inject forged data into the cache. This issue affects BIND 9 versions 9.11.0 through 9.16.50, 9.18.0 through 9.18.39, 9.20.0 through 9.20.13, 9.21.0 through 9.21.12, 9.11.3-S1 through 9.16.50-S1, 9.18.11-S1 through 9.18.39-S1, and 9.20.9-S1 through 9.20.13-S1.	8.6	More Details
CVE-2025-43994	Dell Storage Center - Dell Storage Manager, version(s) DSM 20.1.21, contain(s) a Missing Authentication for Critical Function vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	8.6	More Details
CVE-2025-48091	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Alexander AnyComment anycomment allows SQL Injection.This issue affects AnyComment: from n/a through <= 0.3.6.	8.5	More Details
CVE-2025-49378	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themefic Hydra Booking hydra-booking allows SQL Injection.This issue affects Hydra Booking: from n/a through <= 1.1.10.	8.5	More Details

CVE-2025-11957	Improper authorization in the temporary access workflow of Devolutions Server 2025.2.12.0 and earlier allows an authenticated basic user to self-approve or approve the temporary access requests of other users and gain unauthorized access to vaults and entries via crafted API requests.	8.4	More Details
CVE-2025-8432	Incorrect Default Permissions vulnerability in Centreon Infra Monitoring (MBI modules) allows Embedding Scripts within Scripts by CentreonBI user account on the MBI server This issue affects Infra Monitoring: from 24.10.0 before 24.10.6, from 24.04.0 before 24.04.9, from 23.10.0 before 23.10.15.	8.4	More Details
CVE-2025-54964	An issue was discovered in BAE SOCET GXP before 4.6.0.2. An attacker with the ability to interact with the GXP Job Service may inject arbitrary executables. If the Job Service is configured for local-only access, this may allow for privilege escalation in certain situations. If the Job Service is network accessible, this may allow remote command execution.	8.4	More Details
CVE-2025-60954	Microweber CMS 2.0 has Weak Password Requirements. The application does not enforce minimum password length or complexity during password resets. Users can set extremely weak passwords, including single-character passwords, which can lead to account compromise, including administrative accounts.	8.3	More Details
CVE-2023-53691	Hikvision CSMP (Comprehensive Security Management Platform) iSecure Center through 2023-06-25 allows file upload via /center/api/files directory traversal, as exploited in the wild in 2024 and 2025.	8.3	More Details
CVE-2024-58274	Hikvision CSMP (Comprehensive Security Management Platform) iSecure Center through 2024-08-01 allows execution of a command within $( ) in /center/api/installation/detection JSON data, as exploited in the wild in 2024 and 2025.	8.3	More Details
CVE-2025-46183	The Utils.deserialize function in pgCodeKeeper 10.12.0 processes serialized data from untrusted sources. If an attacker provides a specially crafted .ser file, deserialization may result in unintended code execution or other malicious behavior on the target system.	8.2	More Details
CVE-2025-60801	jshERP up to commit fbda24da was discovered to contain an unauthenticated remote code execution (RCE) vulnerability via the jsh_erp function.	8.2	More Details
CVE-2025-59151	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level advertisement and internet tracker blocking application. Pi-hole Admin Interface before 6.3 is vulnerable to Carriage Return Line Feed (CRLF) injection. When a request is made to a file ending with the .lp extension, the application performs a redirect without properly sanitizing the input. An attacker can inject carriage return and line feed characters (%0d%0a) to manipulate both the headers and the content of the HTTP response. This enables the injection of arbitrary HTTP response headers, potentially leading to session fixation, cache poisoning, and the weakening or bypassing of browser-based security mechanisms such as Content Security Policy or X-XSS-Protection. This vulnerability is fixed in 6.3.	8.2	More Details
CVE-2025-49910	Missing Authorization vulnerability in AmentoTech Private Limited WPGuppy wpguppy-lite allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WPGuppy: from n/a through <= 1.1.4.	8.2	More Details
CVE-2025-58958	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove SmilePure smilepure allows PHP Local File Inclusion.This issue affects SmilePure: from n/a through < 1.8.5.	8.2	More Details
CVE-2025-58967	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove Businext businext allows PHP Local File Inclusion.This issue affects Businext: from n/a through < 2.4.4.	8.2	More Details
CVE-2025-61247	indieka900 online-shopping-system-php 1.0 is vulnerable to SQL Injection in the password parameter of login.php.	8.2	More Details
CVE-2025-62935	Missing Authorization vulnerability in ilmosys Open Close WooCommerce Store woc-open-close allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Open Close WooCommerce Store: from n/a through <= 4.9.8.	8.1	More Details
CVE-2025-62938	Missing Authorization vulnerability in Reoon Technology Reoon Email Verifier reoon-email-verifier allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Reoon Email Verifier: from n/a through <= 2.0.1.	8.1	More Details
CVE-2025-62868	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Edge-Themes Edge CPT allows PHP Local File Inclusion.This issue affects Edge CPT: from n/a through 1.4.	8.1	More Details
CVE-2025-62610	Hono is a Web application framework that provides support for any JavaScript runtime. In versions from 1.1.0 to before 4.10.2, Hono’s JWT Auth Middleware does not provide a built-in aud (Audience) verification option, which can cause confused-deputy / token-mix-up issues: an API may accept a valid token that was issued for a different audience (e.g., another service) when multiple services share the same issuer/keys. This can lead to unintended cross-service access. Hono’s docs list verification options for iss/nbf/iat/exp only, with no aud support; RFC 7519 requires that when an aud claim is present, tokens MUST be rejected unless the processing party identifies itself in that claim. This issue has been patched in version 4.10.2.	8.1	More Details
CVE-2025-59048	OpenBao's AWS Plugin generates AWS access credentials based on IAM policies. Prior to version 0.1.1, the AWS Plugin is vulnerable to cross-account IAM role Impersonation in the AWS auth method. The vulnerability allows an IAM role from an untrusted AWS account to authenticate by impersonating a role with the same name in a trusted account, leading to unauthorized access. This impacts all users of the auth-aws plugin who operate in a multi-account AWS environment where IAM role names may not be unique across accounts. This vulnerability has been patched in version 0.1.1 of the auth-aws plugin. A workaround for this issue involves guaranteeing that IAM role names are unique across all AWS accounts that could potentially interact with your OpenBao environment, and to audit for any duplicate IAM roles.	8.1	More Details

CVE-2025-62169	OctoPrint-SpoolManager is a plugin for managing spools and all their usage metadata. In versions 1.8.0a2 and older of the testing branch and versions 1.7.7 and older of the stable branch, the APIs of the OctoPrint-SpoolManager plugin do not correctly enforce authentication or authorization checks. This issue has been patched in versions 1.8.0a3 of the testing branch and 1.7.8 of the stable branch. The impact of this vulnerability is greatly reduced when using OctoPrint version 1.11.2 and newer.	8.1	More Details
CVE-2025-62964	Missing Authorization vulnerability in RealMag777 MDTF wp-meta-data-filter-and-taxonomy-filter allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MDTF: from n/a through <= 1.3.4.	8.1	More Details
CVE-2025-62893	Authorization Bypass Through User-Controlled Key vulnerability in mediavine Create by Mediavine mediavine-create allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Create by Mediavine: from n/a through <= 1.9.14.	8.1	More Details
CVE-2025-59558	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove Billey billey allows PHP Local File Inclusion.This issue affects Billey: from n/a through < 2.1.6.	8.1	More Details
CVE-2025-62925	Missing Authorization vulnerability in Conversios Conversios.io enhanced-e-commerce-for-woocommerce-store allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Conversios.io: from n/a through <= 7.2.10.	8.1	More Details
CVE-2025-62915	Missing Authorization vulnerability in clicksend SMS Contact Form 7 Notifications by ClickSend clicksend-contactform7 allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SMS Contact Form 7 Notifications by ClickSend: from n/a through <= 1.4.0.	8.1	More Details
CVE-2025-59564	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove EduMall edumall allows PHP Local File Inclusion.This issue affects EduMall: from n/a through < 4.4.5.	8.1	More Details
CVE-2025-59555	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove Medizin medizin allows PHP Local File Inclusion.This issue affects Medizin: from n/a through < 1.9.7.	8.1	More Details
CVE-2025-59550	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in designervily Xcare xcare allows PHP Local File Inclusion.This issue affects Xcare: from n/a through < 6.5.	8.1	More Details
CVE-2025-59007	Deserialization of Untrusted Data vulnerability in themesflat TF Woo Product Grid Addon For Elementor tf-woo-product-grid allows Object Injection.This issue affects TF Woo Product Grid Addon For Elementor: from n/a through <= 1.0.1.	8.1	More Details
CVE-2025-62716	Plane is open-source project management software. Prior to version 1.1.0, an open redirect vulnerability in the ?next_path query parameter allows attackers to supply arbitrary schemes (e.g., javascript:) that are passed directly to router.push. This results in a cross-site scripting (XSS) vulnerability, enabling attackers to execute arbitrary JavaScript in the victim's browser. The issue can be exploited without authentication and has severe impact, including information disclosure, and privilege escalation and modifications of administrative settings. This issue has been patched in version 1.1.0.	8.1	More Details
CVE-2025-58955	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in designervily Karzo karzo allows PHP Local File Inclusion.This issue affects Karzo: from n/a through < 2.6.	8.1	More Details
CVE-2025-62922	Missing Authorization vulnerability in Shambhu Patnaik Export Categories export-categories allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Export Categories: from n/a through <= 1.0.	8.1	More Details
CVE-2025-11086	The Academy LMS – WordPress LMS Plugin for Complete eLearning Solution plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 3.3.7. This is due to the plugin not properly validating a user's role prior to registering a user via the Social Login addon. This makes it possible for unauthenticated attackers to update their role to Administrator when registering on the site.	8.1	More Details
CVE-2025-62927	Missing Authorization vulnerability in Nelio Software Nelio Content nelio-content allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Nelio Content: from n/a through <= 4.0.5.	8.1	More Details
CVE-2025-62909	Missing Authorization vulnerability in mrityunjay Smart WeTransfer smart-wetransfer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Smart WeTransfer: from n/a through <= 1.3.	8.1	More Details
CVE-2025-62029	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in themesion Grevo grevo.This issue affects Grevo: from n/a through <= 2.4.	8.1	More Details
CVE-2025-62928	Missing Authorization vulnerability in Joby Joseph SEO Meta Description Updater seo-meta-description-updater allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SEO Meta Description Updater: from n/a through <= 1.2.0.	8.1	More Details
CVE-2025-11621	Vault and Vault Enterprise's ("Vault") AWS Auth method may be susceptible to authentication bypass if the role of the configured bound_principal_iam is the same across AWS accounts, or uses a wildcard. This vulnerability, CVE-2025-11621, is fixed in Vault Community Edition 1.21.0 and Vault Enterprise 1.21.0, 1.20.5, 1.19.11, and 1.16.27	8.1	More Details
CVE-	The Directorist: AI-Powered Business Directory Plugin with Classified Ads Listings plugin for WordPress is vulnerable to arbitrary file move due to insufficient file path validation in the add_listing_action AJAX action in all versions up to, and including, 8.4.8.		

2025-10488	This makes it possible for unauthenticated attackers to move arbitrary files on the server, which can easily lead to remote code execution when the right file is moved (such as wp-config.php).	8.1	More Details
CVE-2025-52263	An issue in the Web Configuration module of Startcharge Artemis AC Charger 7-22 kW v1.0.4 allows authenticated network-adjacent attackers to upload crafted firmware, leading to arbitrary code execution.	8.0	More Details
CVE-2025-62775	Mercku M6a devices through 2.1.0 allow root TELNET logins via the web admin password.	8.0	More Details
CVE-2025-12235	A vulnerability was found in Tenda CH22 1.0.0.1. This vulnerability affects the function fromSetIpBind of the file /goform/SetIpBind. The manipulation of the argument page results in buffer overflow. The attack must originate from the local network. The exploit has been made public and could be used.	8.0	More Details
CVE-2025-62526	OpenWrt Project is a Linux operating system targeting embedded devices. Prior to version 24.10.4, ubusd contains a heap buffer overflow in the event registration parsing code. This allows an attacker to modify the head and potentially execute arbitrary code in the context of the ubus daemon. The affected code is executed before running the ACL checks, all ubus clients are able to send such messages. In addition to the heap corruption, the crafted subscription also results in a bypass of the listen ACL. This is fixed in OpenWrt 24.10.4. There are no workarounds.	7.9	More Details
CVE-2025-62525	OpenWrt Project is a Linux operating system targeting embedded devices. Prior to version 24.10.4, local users could read and write arbitrary kernel memory using the ioctls of the ltq-ptm driver which is used to drive the datapath of the DSL line. This only effects the lantiq target supporting xrx200, danube and amazon SoCs from Lantiq/Intel/MaxLinear with the DSL in PTM mode. The DSL driver for the VRX518 is not affected. ATM mode is also not affected. Most VDSL lines use PTM mode and most ADSL lines use ATM mode. OpenWrt is normally running as a single user system, but some services are sandboxed. This vulnerability could allow attackers to escape a ujail sandbox or other contains. This is fixed in OpenWrt 24.10.4. There are no workarounds.	7.9	More Details
CVE-2025-11575	Incorrect Default Permissions vulnerability in MongoDB Atlas SQL ODBC driver on Windows allows Privilege Escalation.This issue affects MongoDB Atlas SQL ODBC driver: from 1.0.0 through 2.0.0.	7.8	More Details
CVE-2025-23352	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager, where a malicious guest could cause uninitialized pointer access. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2025-54808	Oxford Nanopore Technologies' MinKNOW software at or prior to version 24.11 stores authentication tokens in a file located in the system's temporary directory (/tmp) on the host machine. This directory is typically world-readable, allowing any local user or application to access the token. If the token is leaked (e.g., via malware infection or other local exploit), and remote access is enabled, it can be used to establish unauthorized remote connections to the sequencer. Remote access must be enabled for remote exploitation to succeed. This may occur either because the user has enabled remote access for legitimate operational reasons or because malware with elevated privileges (e.g., sudo access) enables it without user consent. This vulnerability can be chained with remote access capabilities to generate a developer token from a remote device. Developer tokens can be created with arbitrary expiration dates, enabling persistent access to the sequencer and bypassing standard authentication mechanisms.	7.8	More Details
CVE-2025-12198	A vulnerability has been found in dnsmasq up to 2.73rc6. Affected is the function parse_hex of the file src/util.c of the component Config File Handler. The manipulation of the argument i leads to heap-based buffer overflow. Local access is required to approach this attack. 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.	7.8	More Details
CVE-2025-12100	Incorrect Default Permissions vulnerability in MongoDB BI Connector ODBC driver allows Privilege Escalation.This issue affects BI Connector ODBC driver: from 1.0.0 through 1.4.6.	7.8	More Details
CVE-2025-23347	NVIDIA Project G-Assist contains a vulnerability where an attacker might be able to escalate permissions. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	7.8	More Details
CVE-2025-53855	An out-of-bounds write vulnerability exists in the XML parser functionality of GCC Productions Inc. Fade In 4.2.0. A specially crafted .fadein file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2025-36007	IBM QRadar SIEM 7.5 through 7.5.0 Update Pack 13 Independent Fix 02 is vulnerable to privilege escalation due to improper privilege assignment to an update script.	7.8	More Details
CVE-2025-12341	A vulnerability was detected in ermig1979 AntiDupl up to 2.3.12. Impacted is an unknown function of the file AntiDupl.NET.WinForms.exe of the component Delete Duplicate Image Handler. The manipulation results in link following. The attack is only possible with local access. The vendor was contacted early about this disclosure but did not respond in any way.	7.8	More Details
CVE-2025-53814	A use-after-free vulnerability exists in the XML parser functionality of GCC Productions Inc. Fade In 4.2.0. A specially crafted .xml file can lead to heap-based memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2025-59500	Improper access control in Azure Notification Service allows an authorized attacker to elevate privileges over a network.	7.7	More Details
CVE-2025-	The seffaflik thru 0.0.9 is vulnerable to symlink attacks due to incorrect default permissions given to the .kimlik file and .seffaflik file, which is created with mode 0777 and 0775 respectively, exposing secrets to other local users. Additionally, the	7.7	More

61035	.kimlik file is written without symlink checks, allowing local attackers to overwrite arbitrary files. This can result in information disclosure and denial of service.		Details
CVE-2025-10145	The Auto Featured Image (Auto Post Thumbnail) plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.1.7 via the upload_to_library function. This makes it possible for authenticated attackers, with Author-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. On Cloud instances, this issue allows for metadata retrieval.	7.7	More Details
CVE-2025-60217	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ypromo PT Luxa Addons pt-luxa-addons allows Path Traversal.This issue affects PT Luxa Addons: from n/a through <= 1.2.2.	7.7	More Details
CVE-2025-46582	A private key disclosure vulnerability exists in ZTE's ZXMP M721 product. A low-privileged user can bypass authorization checks to view the device's communication private key, resulting in key exposure and impacting communication security.	7.7	More Details
CVE-2025-59461	A remote unauthenticated attacker may use the unauthenticated C++ API to access or modify sensitive data and disrupt services.	7.6	More Details
CVE-2025-53425	Incorrect Privilege Assignment vulnerability in Dokan, Inc. Dokan dokan-lite allows Privilege Escalation.This issue affects Dokan: from n/a through <= 4.1.2.	7.6	More Details
CVE-2025-60730	PerfreeBlog v4.0.11 has an arbitrary file deletion vulnerability in the unInstallTheme function	7.6	More Details
CVE-2025-62015	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Josh Kohlbach Advanced Coupons for WooCommerce Coupons advanced-coupons-for-woocommerce-free.This issue affects Advanced Coupons for WooCommerce Coupons: from n/a through <= 4.6.8.	7.6	More Details
CVE-2025-60731	PerfreeBlog v4.0.11 has a File Upload vulnerability in the installTheme function	7.6	More Details
CVE-2025-10914	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Proliz Software Ltd. Co. OBS (Student Affairs Information System) allows Reflected XSS.This issue affects OBS (Student Affairs Information System): before V26.0401.	7.6	More Details
CVE-2025-60424	A lack of rate limiting in the OTP verification component of Nagios Fusion v2024R1.2 and v2024R2 allows attackers to bypass authentication via a bruteforce attack.	7.6	More Details
CVE-2025-59566	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in AmentoTech Workreap (theme's plugin) workreap allows Path Traversal.This issue affects Workreap (theme's plugin): from n/a through <= 3.3.5.	7.6	More Details
CVE-2025-58959	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in AmentoTech Taskbot taskbot allows Path Traversal.This issue affects Taskbot: from n/a through <= 6.4.	7.6	More Details
CVE-2025-60735	PerfreeBlog v4.0.11 has a File Upload vulnerability in the installPlugin function	7.6	More Details
CVE-2025-11735	The HUSKY – Products Filter Professional for WooCommerce plugin for WordPress is vulnerable to blind SQL Injection via the `phrase` parameter in all versions up to, and including, 1.3.7.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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-2025-8677	Querying for records within a specially crafted zone containing certain malformed DNSKEY records can lead to CPU exhaustion. This issue affects BIND 9 versions 9.18.0 through 9.18.39, 9.20.0 through 9.20.13, 9.21.0 through 9.21.12, 9.18.11-S1 through 9.18.39-S1, and 9.20.9-S1 through 9.20.13-S1.	7.5	More Details
CVE-2025-60562	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formWISiteSurvey.	7.5	More Details
CVE-2025-52099	Integer Overflow vulnerability in SQLite SQLite3 v.3.50.0 allows a remote attacker to cause a denial of service via the setupLookaside function	7.5	More Details
CVE-2025-60336	A NULL pointer dereference in the sub_41773C function of TOTOLINK N600R v4.3.0cu.7866_B20220506 allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details
CVE-2025-60337	Tenda AC6 V2.0 15.03.06.50 was discovered to contain a buffer overflow in the speed_dir parameter in the SetSpeedWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-	Multiple buffer overflows in the SetClientState function of Tenda AC6 v.15.03.06.50 allows attackers to cause a Denial of Service (DoS) via injecting a crafted payload into the limitSpeed, deviceId, and limitSpeedUp parameters.	7.5	More Details

60340			
CVE-2025-60339	Multiple buffer overflow vulnerabilities in the openSchedWifi function of Tenda AC6 v.15.03.06.50 allows attackers to cause a Denial of Service (DoS) via injecting a crafted payload into the schedStartTime and schedEndTime parameters.	7.5	More Details
CVE-2025-59460	The system is deployed in its default state, with configuration settings that do not comply with the latest best practices for restricting access. This increases the risk of unauthorised connections.	7.5	More Details
CVE-2025-62513	OpenBao is an open source identity-based secrets management system. In versions 2.2.0 to 2.4.1, OpenBao's audit log experienced a regression wherein raw HTTP bodies used by few endpoints were not correctly redacted (HMAC'd). This impacts those using the ACME functionality of PKI, resulting in short-lived ACME verification challenge codes being leaked in the audit logs. Additionally, this impacts those using the OIDC issuer functionality of the identity subsystem, auth and token response codes along with claims could be leaked in the audit logs. ACME verification codes are not usable after verification or challenge expiry so are of limited long-term use. This issue has been patched in OpenBao 2.4.2.	7.5	More Details
CVE-2025-60341	Tenda AC6 V2.0 15.03.06.50 was discovered to contain a stack overflow in the ssid parameter in the fast_setting_wifi_set function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-60563	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formSetPortTr.	7.5	More Details
CVE-2025-60564	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formSetLog.	7.5	More Details
CVE-2025-60342	Tenda AC6 V2.0 15.03.06.50 was discovered to contain a stack overflow in the page parameter in the addressNat function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-60343	Multiple buffer overflows in the AdvSetMacMtuWan function of Tenda AC6 v.15.03.06.50 allows attackers to cause a Denial of Service (DoS) via injecting a crafted payload into the wanMTU, wanSpeed, cloneType, mac, serviceName, serverName, wanMTU2, wanSpeed2, cloneType2, mac2, serviceName2, and serverName2 parameters.	7.5	More Details
CVE-2025-60565	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formSchedule.	7.5	More Details
CVE-2025-61100	FRRouting/frr from v2.0 through v10.4.1 was discovered to contain a NULL pointer dereference via the ospf_opaque_lsa_dump function at ospf_opaque.c. This vulnerability allows attackers to cause a Denial of Service (DoS) under specific malformed LSA conditions.	7.5	More Details
CVE-2025-60547	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formSetWAN_Wizard7.	7.5	More Details
CVE-2025-60334	TOTOLINK N600R v4.3.0cu.7866_B20220506 was discovered to contain a stack overflow in the ssid parameter in the setWiFiBasicConfig function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-60338	Tenda AC6 V2.0 15.03.06.50 was discovered to contain a stack overflow in the page parameter in the DhcpListClient function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-41067	Reachable Assertion vulnerability in Open5GS up to version 2.7.5 allows attackers with connectivity to the NRF to cause a denial of service. An SBI request that deletes the NRF's own registry causes a check that ends up crashing the NRF process and renders the discovery service unavailable.	7.5	More Details
CVE-2025-60332	A NULL pointer dereference in the SetWLanRadioSettings function of D-Link DIR-823G A1 v1.0.2B05 allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details
CVE-2025-60331	D-Link DIR-823G A1 v1.0.2B05 was discovered to contain a buffer overflow in the FillMacCloneMac parameter in the /EXCU_SHELL endpoint. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-32657	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in RadiusTheme Testimonial Slider And Showcase Pro testimonial-slider-showcase-pro allows PHP Local File Inclusion.This issue affects Testimonial Slider And Showcase Pro: from n/a through <= 2.1.7.	7.5	More Details
CVE-2025-61099	FRRouting/frr from v2.0 through v10.4.1 was discovered to contain a NULL pointer dereference via the opaque_info_detail function at ospf_opaque.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted LS Update packet.	7.5	More Details
CVE-2025-61102	FRRouting/frr from v4.0 through v10.4.1 was discovered to contain a NULL pointer dereference via the show_vty_ext_link_adj_sid function at ospf_ext.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted OSPF packet.	7.5	More Details
CVE-2025-	FRRouting/frr from v4.0 through v10.4.1 was discovered to contain a NULL pointer dereference via the show_vty_link_info function at ospf_ext.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted OSPF packet.	7.5	More Details

61105			
CVE-2025-55752	Relative Path Traversal vulnerability in Apache Tomcat. The fix for bug 60013 introduced a regression where the rewritten URL was normalized before it was decoded. This introduced the possibility that, for rewrite rules that rewrite query parameters to the URL, an attacker could manipulate the request URI to bypass security constraints including the protection for /WEB-INF/ and /META-INF/. If PUT requests were also enabled then malicious files could be uploaded leading to remote code execution. PUT requests are normally limited to trusted users and it is considered unlikely that PUT requests would be enabled in conjunction with a rewrite that manipulated the URI. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.10, from 10.1.0-M1 through 10.1.44, from 9.0.0.M11 through 9.0.108. The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.6 though 8.5.100. Other, older, EOL versions may also be affected. Users are recommended to upgrade to version 11.0.11 or later, 10.1.45 or later or 9.0.109 or later, which fix the issue.	7.5	More Details
CVE-2025-62895	Insertion of Sensitive Information Into Sent Data vulnerability in Vito Peleg Atarim atarim-visual-collaboration allows Retrieve Embedded Sensitive Data.This issue affects Atarim: from n/a through <= 4.2.	7.5	More Details
CVE-2025-62902	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in ThemeHunk WP Popup Builder wp-popup-builder allows Retrieve Embedded Sensitive Data.This issue affects WP Popup Builder: from n/a through <= 1.3.6.	7.5	More Details
CVE-2025-27225	TRUfusion Enterprise through 7.10.4.0 exposes the /trufusionPortal/jsp/internal_admin_contact_login.jsp endpoint to unauthenticated users. This endpoint discloses sensitive internal information including PII to unauthenticated attackers.	7.5	More Details
CVE-2025-27223	TRUfusion Enterprise through 7.10.4.0 exposes the encrypted COOKIEID as an authentication mechanism for some endpoints such as /trufusionPortal/getProjectList. However, the application uses a static key to create the encrypted cookie, ultimately allowing anyone to forge cookies and gain access to sensitive internal information.	7.5	More Details
CVE-2025-62022	Missing Authorization vulnerability in BuddyPress BuddyPress buddypress.This issue affects BuddyPress: from n/a through <= 14.3.4.	7.5	More Details
CVE-2025-59579	Insertion of Sensitive Information Into Sent Data vulnerability in PressTigers Simple Job Board simple-job-board allows Retrieve Embedded Sensitive Data.This issue affects Simple Job Board: from n/a through <= 2.13.7.	7.5	More Details
CVE-2025-11447	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 11.0 before 18.3.5, 18.4 before 18.4.3, and 18.5 before 18.5.1 that could have allowed an unauthenticated attacker to cause a denial of service condition by sending GraphQL requests with crafted JSON payloads.	7.5	More Details
CVE-2025-52268	StarCharge Artemis AC Charger 7-22 kW v1.0.4 was discovered to contain a hardcoded AES key which allows attackers to forge or decrypt valid login tokens.	7.5	More Details
CVE-2025-62054	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in favethemes Houzez Theme - Functionality houzez-theme-functionality.This issue affects Houzez Theme - Functionality: from n/a through <= 4.1.8.	7.5	More Details
CVE-2025-10497	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.10 before 18.3.5, 18.4 before 18.4.3, and 18.5 before 18.5.1 that could have allowed an unauthenticated attacker to cause a denial of service condition by sending specially crafted payloads.	7.5	More Details
CVE-2025-9322	The Stripe Payment Forms by WP Full Pay – Accept Credit Card Payments, Donations & Subscriptions plugin for WordPress is vulnerable to SQL Injection via the 'wpfs-form-name' parameter in all versions up to, and including, 8.3.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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-2025-8416	The Product Filter by WBW plugin for WordPress is vulnerable to SQL Injection via the 'filtersDataBackend' parameter in all versions up to, and including, 2.9.7. This is 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-2025-4203	The wpForo Forum plugin for WordPress is vulnerable to error-based or time-based SQL Injection via the get_members() function in all versions up to, and including, 2.4.8 due to missing integer validation on the 'offset' and 'row_count' parameters. The function blindly interpolates 'row_count' into a 'LIMIT offset,row_count' clause using esc_sql() rather than enforcing numeric values. MySQL 5.x's grammar allows a 'PROCEDURE ANALYSE' clause immediately after a LIMIT clause. Unauthenticated attackers controlling 'row_count' can append a stored-procedure call, enabling error-based or time-based blind SQL injection that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2025-62604	MeterSphere is an open source continuous testing platform. Prior to version 2.10.25-lts, a logic flaw allows retrieval of arbitrary user information. This allows an unauthenticated attacker to log in to the system as any user. This issue has been patched in version 2.10.25-lts.	7.5	More Details
CVE-2025-60333	TOTOLINK N600R v4.3.0cu.7866_B20220506 was discovered to contain a stack overflow in the wepkey2 parameter in the setWiFiMultipleConfig function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-41068	Reachable Assertion vulnerability in Open5GS up to version 2.7.5 allows attackers with connectivity to the NRF to cause a denial of service. This is achieved by sending the creation of an NF with an invalid type via SBI and then requesting its data. The NRF executes a check that crashes the process, leaving the discovery service unresponsive.	7.5	More Details
CVE-	pypdf is a free and open-source pure-python PDF library. Prior to version 6.1.3, an attacker who uses this vulnerability can craft		

2025-62708	a PDF which leads to large memory usage. This requires parsing the content stream of a page using the LZWDecode filter. This has been fixed in pypdf version 6.1.3.	7.5	More Details
CVE-2025-60335	A NULL pointer dereference in the main function of TOTOLINK N600R v4.3.0cu.7866_B20220506 allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details
CVE-2025-62707	pypdf is a free and open-source pure-python PDF library. Prior to version 6.1.3, an attacker who uses this vulnerability can craft a PDF which leads to an infinite loop. This requires parsing the content stream of a page which has an inline image using the DCTDecode filter. This has been fixed in pypdf version 6.1.3.	7.5	More Details
CVE-2025-60566	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formSetMACFilter.	7.5	More Details
CVE-2025-60561	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formSetEmail.	7.5	More Details
CVE-2025-61106	FRRouting/frr from v4.0 through v10.4.1 was discovered to contain a NULL pointer dereference via the show_vty_ext_pref_pref_sid function at ospf_ext.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted OSPF packet.	7.5	More Details
CVE-2025-41722	The wsc server uses a hard-coded certificate to check the authenticity of SOAP messages. An unauthenticated remote attacker can extract private keys from the Software of the affected devices.	7.5	More Details
CVE-2025-11145	Observable Discrepancy, Exposure of Sensitive Information to an Unauthorized Actor, Exposure of Private Personal Information to an Unauthorized Actor vulnerability in CBK Soft Software Hardware Electronic Computer Systems Industry and Trade Inc. EnVision allows Account Footprinting.This issue affects enVision: before 250566.	7.5	More Details
CVE-2025-12105	A flaw was found in the asynchronous message queue handling of the libsoup library, widely used by GNOME and WebKit-based applications to manage HTTP/2 communications. When network operations are aborted at specific timing intervals, an internal message queue item may be freed twice due to missing state synchronization. This leads to a use-after-free memory access, potentially crashing the affected application. Attackers could exploit this behavior remotely by triggering specific HTTP/2 read and cancel sequences, resulting in a denial-of-service condition.	7.5	More Details
CVE-2025-10861	The Popup builder with Gamification, Multi-Step Popups, Page-Level Targeting, and WooCommerce Triggers plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.1.4. This is due to insufficient validation on the URLs supplied via the URL parameter. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services, as well as conduct network reconnaissance. The vulnerability was partially patched in version 2.1.4.	7.5	More Details
CVE-2025-61103	FRRouting/frr from v4.0 through v10.4.1 was discovered to contain a NULL pointer dereference via the show_vty_ext_link_lan_adj_sid function at ospf_ext.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted OSPF packet.	7.5	More Details
CVE-2025-11504	The Quickcreator – AI Blog Writer plugin for WordPress is vulnerable to Sensitive Information Exposure in versions 0.0.9 to 0.1.17 through the /wp-content/plugins/quickcreator/dupasrala.txt file. This makes it possible for unauthenticated attackers to view the plugin's API key and subsequently use that to perform actions on the site like creating new posts and injecting XSS payloads.	7.5	More Details
CVE-2025-62947	Insertion of Sensitive Information Into Sent Data vulnerability in publitio Publitio publitio allows Retrieve Embedded Sensitive Data.This issue affects Publitio: from n/a through <= 2.2.3.	7.5	More Details
CVE-2025-61104	FRRouting/frr from v4.0 through v10.4.1 was discovered to contain a NULL pointer dereference via the show_vty_unknown_tlv function at ospf_ext.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted OSPF packet.	7.5	More Details
CVE-2025-62399	Moodle’s mobile and web service authentication endpoints did not sufficiently restrict repeated password attempts, making them susceptible to brute-force attacks.	7.5	More Details
CVE-2025-58429	A relative path traversal vulnerability was discovered in Productivity Suite software version 4.4.1.19. The vulnerability allows an unauthenticated remote attacker to interact with the ProductivityService PLC simulator and delete arbitrary files on the target machine.	7.5	More Details
CVE-2025-58078	A relative path traversal vulnerability was discovered in Productivity Suite software version 4.4.1.19. The vulnerability allows an unauthenticated remote attacker to interact with the ProductivityService PLC simulator and write files with arbitrary data on the target machine.	7.5	More Details
CVE-2025-60569	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formSetRoute.	7.5	More Details
CVE-2025-61107	FRRouting/frr from v4.0 through v10.4.1 was discovered to contain a NULL pointer dereference via the show_vty_ext_pref_pref_sid function at ospf_ext.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted LSA Update packet.	7.5	More Details
CVE-2025-	Missing Authorization vulnerability in Themefic Hydra Booking hydra-booking allows Exploiting Incorrectly Configured Access	7.5	More

49377	Control Security Levels.This issue affects Hydra Booking: from n/a through <= 1.1.9.		Details
CVE-2025-49376	Missing Authorization vulnerability in DELUCKS DELUCKS SEO delucks-seo allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects DELUCKS SEO: from n/a through <= 2.5.9.	7.5	More Details
CVE-2025-12044	Vault and Vault Enterprise (“Vault”) are vulnerable to an unauthenticated denial of service when processing JSON payloads. This occurs due to a regression from a previous fix for [+HCSEC-2025-24+|https://discuss.hashicorp.com/t/hcsec-2025-24-vault-denial-of-service-though-complex-json-payloads/76393] which allowed for processing JSON payloads before applying rate limits. This vulnerability, CVE-2025-12044, is fixed in Vault Community Edition 1.21.0 and Vault Enterprise 1.16.27, 1.19.11, 1.20.5, and 1.21.0.	7.5	More Details
CVE-2025-48338	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Kevon Adonis WP Abstracts wp-abstracts-manuscripts-manager allows PHP Local File Inclusion.This issue affects WP Abstracts: from n/a through <= 2.7.4.	7.5	More Details
CVE-2025-50950	Audiofile v0.3.7 was discovered to contain a NULL pointer dereference via the ModuleState::setup function.	7.5	More Details
CVE-2025-6980	Captive Portal can expose sensitive information	7.5	More Details
CVE-2025-62727	Starlette is a lightweight ASGI framework/toolkit. Prior to 0.49.1 , an unauthenticated attacker can send a crafted HTTP Range header that triggers quadratic-time processing in Starlette's FileResponse Range parsing/merging logic. This enables CPU exhaustion per request, causing denial-of-service for endpoints serving files (e.g., StaticFiles or any use of FileResponse). This vulnerability is fixed in 0.49.1.	7.5	More Details
CVE-2025-62771	Mercku M6a devices through 2.1.0 allow password changes via intranet CSRF attacks.	7.5	More Details
CVE-2025-30944	Missing Authorization vulnerability in Essekia Tablesome Table Premium tablesome-premium allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Tablesome Table Premium: from n/a through <= 1.1.23.	7.5	More Details
CVE-2025-60568	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formAdvFirewall.	7.5	More Details
CVE-2025-61101	FRRouting/frr from v4.0 through v10.4.1 was discovered to contain a NULL pointer dereference via the show_vty_ext_link_rmt_itf_addr function at ospf_ext.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted OSPF packet.	7.5	More Details
CVE-2025-60570	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formLogDnsquery.	7.5	More Details
CVE-2025-41724	An unauthenticated remote attacker can crash the wscserver by sending incomplete SOAP requests. The wscserver process will not be restarted by a watchdog and a device reboot is necessary to make it work again.	7.5	More Details
CVE-2025-60559	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formSetDomainFilter.	7.5	More Details
CVE-2025-60558	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formVirtualServ.	7.5	More Details
CVE-2025-60557	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formSetEasy_Wizard.	7.5	More Details
CVE-2025-60556	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formSetWizard1.	7.5	More Details
CVE-2025-60555	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formSetWizardSelectMode.	7.5	More Details
CVE-2025-60552	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formTcpipSetup.	7.5	More Details
CVE-2025-60571	D-Link DIR600LAx FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formSetQoS.	7.5	More Details
CVE-			

2025-60550	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formEasySetTimezone.	7.5	More Details
CVE-2025-12055	HYDRA X, MIP 2 and FEDRA 2 of MPDV Mikrolab GmbH suffer from an unauthenticated local file disclosure vulnerability in all releases until Maintenance Pack 36 with Servicepack 8 (week 36/2025), which allows an attacker to read arbitrary files from the Windows operating system. The "Filename" parameter of the public $SCHEMAS$ ressource is vulnerable and can be exploited easily.	7.5	More Details
CVE-2025-60549	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formAutoDetecWAN_wizard4.	7.5	More Details
CVE-2025-60551	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the next_page parameter in the function formDeviceReboot.	7.5	More Details
CVE-2025-60938	Emoncms 11.7.3 has a remote code execution vulnerability in the firmware upload feature that allows authenticated users to execute arbitrary commands on the target system. The vulnerability stems from insufficient input validation of user-controlled parameters including filename, port, baud_rate, core, and autoreset within the /admin/upload-custom-firmware endpoint.	7.5	More Details
CVE-2025-60572	D-Link DIR600L Ax FW116WWb01 was discovered to contain a buffer overflow via the curTime parameter in the function formAdvNetwork.	7.5	More Details
CVE-2025-52756	Improper Control of Generation of Code ('Code Injection') vulnerability in Sayan Datta WP Last Modified Info wp-last-modified-info allows Remote Code Inclusion.This issue affects WP Last Modified Info: from n/a through <= 1.9.2.	7.4	More Details
CVE-2025-53427	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chibueze Okechukwu SEO Pyramid seo-pyramid allows Reflected XSS.This issue affects SEO Pyramid: from n/a through <= 1.9.8.	7.4	More Details
CVE-2025-49935	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in xtemos WoodMart woodmart allows PHP Local File Inclusion.This issue affects WoodMart: from n/a through < 8.3.2.	7.4	More Details
CVE-2025-12306	A vulnerability was determined in code-projects Nero Social Networking Site 1.0. Affected is an unknown function of the file /acceptoffres.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-12339	A security vulnerability has been detected in Campcodes Retro Basketball Shoes Online Store 1.0. This issue affects some unknown processing of the file /admin/admin_football.php. The manipulation of the argument pid leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-12301	A security vulnerability has been detected in code-projects Simple Food Ordering System 1.0. Impacted is an unknown function of the file /editproduct.php. Such manipulation of the argument photo leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-12342	A flaw has been found in Serdar Bayram Ghost Hot Spot up to 20251014. The affected element is an unknown function of the file /Auth.php of the component Login. This manipulation causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-12316	A vulnerability was identified in code-projects Courier Management System 1.0. This impacts an unknown function of the file /courier/edit-courier.php. The manipulation of the argument OfficeName leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-12253	A vulnerability was determined in AMTT Hotel Broadband Operation System 1.0. Affected by this vulnerability is an unknown functionality of the file /user/portal/get_expiredtime.php. This manipulation of the argument uid 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-2025-12257	A security vulnerability has been detected in SourceCodester Online Student Result System 1.0. This issue affects some unknown processing of the file /view_result.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-12326	A vulnerability was found in shawon100 RUET OJ up to 18fa45b0a669fa1098a0b8fc629cf6856369d9a5. This vulnerability affects unknown code of the file /process.php of the component POST Request Handler. The manipulation of the argument un results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-12307	A vulnerability was identified in code-projects Nero Social Networking Site 1.0. Affected by this vulnerability is an unknown functionality of the file /addfriend.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-12308	A security flaw has been discovered in code-projects Nero Social Networking Site 1.0. Affected by this issue is some unknown functionality of the file /deletemessage.php. Performing manipulation of the argument message_id results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-	A weakness has been identified in code-projects Nero Social Networking Site 1.0. This affects an unknown part of the file /friendprofile.php. Executing manipulation of the argument ID can lead to sql injection. It is possible to launch the attack	7.3	More

12309	remotely. The exploit has been made available to the public and could be exploited.		Details
CVE-2025-12215	A flaw has been found in projectworlds Online Shopping System 1.0. Impacted is an unknown function of the file /login_submit.php. Executing manipulation of the argument keywords can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-12248	A security vulnerability has been detected in CLTPHP 3.0. The affected element is an unknown function of the file /home/search.html. Such manipulation of the argument keyword leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-52735	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in XLPlugins NextMove Lite woo-thank-you-page-nextmove-lite allows Reflected XSS.This issue affects NextMove Lite: from n/a through <= 2.21.0.	7.3	More Details
CVE-2025-52734	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ERA404 CropRefine croprefine allows Reflected XSS.This issue affects CropRefine: from n/a through <= 1.2.1.	7.3	More Details
CVE-2025-12325	A vulnerability has been found in SourceCodester Best Salon Management System 1.0. This affects an unknown part of the file /panel/forgot-password.php. The manipulation of the argument email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-49925	Missing Authorization vulnerability in VibeThemes WPLMS wplms_plugin allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WPLMS: from n/a through <= 1.9.9.7.	7.3	More Details
CVE-2025-59273	Improper access control in Azure Event Grid allows an unauthorized attacker to elevate privileges over a network.	7.3	More Details
CVE-2025-12338	A weakness has been identified in Campcodes Retro Basketball Shoes Online Store 1.0. This vulnerability affects unknown code of the file /admin/admin_product.ph. Executing manipulation of the argument pid can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-49926	Improper Control of Generation of Code ('Code Injection') vulnerability in Laborator Kalium kalium allows Code Injection.This issue affects Kalium: from n/a through <= 3.25.	7.3	More Details
CVE-2025-12378	A security flaw has been discovered in code-projects Simple Food Ordering System 1.0. This issue affects some unknown processing of the file /addproduct.php. Performing manipulation of the argument photo results in unrestricted upload. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-49924	Incorrect Privilege Assignment vulnerability in Josh Kohlbach Wholesale Suite woocommerce-wholesale-prices allows Privilege Escalation.This issue affects Wholesale Suite: from n/a through <= 2.2.4.2.	7.3	More Details
CVE-2025-12208	A vulnerability was found in SourceCodester Best House Rental Management System 1.0. This impacts the function login2 of the file /admin_class.php. Performing manipulation of the argument Username results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-12336	A vulnerability was identified in Campcodes Retro Basketball Shoes Online Store 1.0. Affected by this issue is some unknown functionality of the file /admin/admin_index.php. Such manipulation of the argument Username leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-49921	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CrocoBlock JetReviews jet-reviews allows PHP Local File Inclusion.This issue affects JetReviews: from n/a through <= 3.0.0.	7.3	More Details
CVE-2025-12293	A vulnerability was identified in SourceCodester Point of Sales 1.0. This issue affects some unknown processing of the file /category.php. Such manipulation of the argument Category leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-49950	Missing Authorization vulnerability in billingo Official Integration for Billingo billingo allows Privilege Escalation.This issue affects Official Integration for Billingo: from n/a through <= 4.2.5.	7.3	More Details
CVE-2025-12337	A security flaw has been discovered in Campcodes Retro Basketball Shoes Online Store 1.0. This affects an unknown part of the file /admin/admin_feature.php. Performing manipulation of the argument pid results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-12237	A vulnerability was identified in projectworlds Advanced Library Management System 1.0. Impacted is an unknown function of the file /index.php. Such manipulation of the argument keywords leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-12277	A flaw has been found in Abdullah-Hasan-Sajjad Online-School up to f09dda77b4c29aa083ff57f4b1eb991b98b68883. This affects an unknown part of the file /studentLogin.php. This manipulation of the argument Email causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used. This product adopts a rolling release strategy to maintain continuous delivery The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-12292	A vulnerability was determined in SourceCodester Point of Sales 1.0. This vulnerability affects unknown code of the file /index.php. This manipulation of the argument Username causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details

CVE-2025-61482	Improper handling of OTP/TOTP/HOTP values in NetKnights GmbH privacyIDEA Authenticator v.4.3.0 on Android allows local attackers with root access to bypass two factor authentication. By hooking into app crypto routines and intercepting decryption paths, attacker can recover plaintext secrets, enabling generation of valid one-time passwords, and bypassing authentication for enrolled accounts.	7.2	More Details
CVE-2025-11889	The AIO Forms – Craft Complex Forms Easily plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the import functionality in all versions up to, and including, 1.3.15. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2025-62965	Missing Authorization vulnerability in wpseek Admin Management Xtended admin-management-xtended allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Admin Management Xtended : from n/a through <= 2.5.1.	7.2	More Details
CVE-2025-59837	Astro is a web framework that includes an image proxy. In versions 5.13.4 and later before 5.13.10, the image proxy domain validation can be bypassed by using backslashes in the href parameter, allowing server-side requests to arbitrary URLs. This can lead to server-side request forgery (SSRF) and potentially cross-site scripting (XSS). This vulnerability exists due to an incomplete fix for CVE-2025-58179. Fixed in 5.13.10.	7.2	More Details
CVE-2025-6978	Diagnostics command injection vulnerability	7.2	More Details
CVE-2025-62617	Admidio is an open-source user management solution. Prior to version 4.3.17, an authenticated SQL injection vulnerability exists in the member assignment data retrieval functionality of Admidio. Any authenticated user with permissions to assign members to a role (such as an administrator) can exploit this vulnerability to execute arbitrary SQL commands. This can lead to a full compromise of the application's database, including reading, modifying, or deleting all data. This issue has been patched in version 4.3.17.	7.2	More Details
CVE-2025-11238	The Watu Quiz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the HTTP Referer header in versions less than, or equal to, 3.4.4 due to insufficient input sanitization and output escaping when the "Save source URL" option is enabled. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an user accesses an injected page.	7.2	More Details
CVE-2025-62688	An incorrect permission assignment for a critical resource vulnerability was discovered in Productivity Suite software version 4.4.1.19. The vulnerability allows an attacker with low-privileged credentials to change their role, gaining full control access to the project.	7.1	More Details
CVE-2025-61136	A Host Header Injection vulnerability in the password reset component in axewater sharewarez v2.4.3 allows remote attackers to conduct password reset poisoning and account takeover via manipulation of the Host header when Flask's url_for(_external=True) generates reset links without a fixed SERVER_NAME.	7.1	More Details
CVE-2025-62020	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Infomaniak Network VOD Infomaniak vod-infomaniak.This issue affects VOD Infomaniak: from n/a through <= 1.5.11.	7.1	More Details
CVE-2025-61132	A Host Header Injection vulnerability in the password reset component in levlaz braindump v0.4.14 allows remote attackers to conduct password reset poisoning and account takeover via manipulation of the Host header when Flask's url_for(_external=True) generates reset links without a fixed SERVER_NAME.	7.1	More Details
CVE-2025-55067	The TLS4B ATG system is vulnerable to improper handling of Unix time values that exceed the 2038 epoch rollover. When the system clock reaches January 19, 2038, it resets to December 13, 1901, causing authentication failures and disrupting core system functionalities such as login access, history visibility, and leak detection termination. This vulnerability could allow an attacker to manipulate the system time to trigger a denial of service (DoS) condition, leading to administrative lockout, operational timer failures, and corrupted log entries.	7.1	More Details
CVE-2025-39534	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Somonator Terms Dictionary terms-dictionary allows Reflected XSS.This issue affects Terms Dictionary: from n/a through <= 1.5.1.	7.1	More Details
CVE-2025-62005	Cross-Site Request Forgery (CSRF) vulnerability in FantasticPlugins SUMO Memberships for WooCommerce sumomemberships allows Cross Site Request Forgery.This issue affects SUMO Memberships for WooCommerce: from n/a through < 7.8.0.	7.1	More Details
CVE-2025-52754	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in selloio Sello ChannelConnector sello-channelconnector allows Reflected XSS.This issue affects Sello ChannelConnector: from n/a through <= 1.6.3.	7.1	More Details
CVE-2025-52736	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Daman Jeet Finale Lite finale-woocommerce-sales-countdown-timer-discount allows Reflected XSS.This issue affects Finale Lite: from n/a through <= 2.20.0.	7.1	More Details
CVE-2025-52742	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Igor Benic Pets pets allows Reflected XSS.This issue affects Pets: from n/a through <= 1.4.1.	7.1	More Details
CVE-2025-52743	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bobbingwide oik-privacy-policy oik-privacy-policy allows Reflected XSS.This issue affects oik-privacy-policy: from n/a through <= 1.4.9.	7.1	More Details
CVE-2025-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins Directory Pro directory-pro allows Reflected XSS.This issue affects Directory Pro: from n/a through <= 2.5.5.	7.1	More Details

52748			
CVE-2025-52749	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Activity Track Uji Countdown uji-countdown allows Reflected XSS.This issue affects Uji Countdown: from n/a through <= 2.3.3.	7.1	More Details
CVE-2025-52750	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juergen Schulze Emu2 emu2-email-users-2 allows Reflected XSS.This issue affects Emu2: from n/a through <= 0.83b.	7.1	More Details
CVE-2025-52751	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in colome Slide Puzzle slide-puzzle allows Reflected XSS.This issue affects Slide Puzzle: from n/a through <= 1.0.0.	7.1	More Details
CVE-2025-52753	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in supsystic Contact Form by Supsystic contact-form-by-supsystic allows Reflected XSS.This issue affects Contact Form by Supsystic: from n/a through <= 1.7.35.	7.1	More Details
CVE-2025-52755	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chris Taylor Child Themes child-themes allows Reflected XSS.This issue affects Child Themes: from n/a through <= 1.0.1.	7.1	More Details
CVE-2025-49962	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in useStrict bbPress Notify bbpress-notify-nospam allows Reflected XSS.This issue affects bbPress Notify: from n/a through <= 2.19.4.	7.1	More Details
CVE-2025-52763	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NickDuncan Nifty Backups nifty-backups allows Reflected XSS.This issue affects Nifty Backups: from n/a through <= 1.08.	7.1	More Details
CVE-2025-52770	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in appscreo Hello Followers hellofollowers allows Reflected XSS.This issue affects Hello Followers: from n/a through <= 2.5.	7.1	More Details
CVE-2025-53229	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kamleshyadav RockON DJ rockon allows Reflected XSS.This issue affects RockON DJ: from n/a through <= 3.3.	7.1	More Details
CVE-2025-53234	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AndonDesign UDesign Core u-design-core allows Reflected XSS.This issue affects UDesign Core: from n/a through <= 4.14.0.	7.1	More Details
CVE-2025-53238	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Toast Plugins Toast Mobile Menu toast-responsive-menu allows Stored XSS.This issue affects Toast Mobile Menu: from n/a through <= 1.0.7.	7.1	More Details
CVE-2025-53297	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AA-Team Woocommerce Envato Affiliates wooenvato allows Reflected XSS.This issue affects Woocommerce Envato Affiliates: from n/a through <= 1.2.1.	7.1	More Details
CVE-2025-53350	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webjunk Calendar Plus calendar-plus allows Reflected XSS.This issue affects Calendar Plus: from n/a through <= 1.2.4.	7.1	More Details
CVE-2025-53351	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fidelo Software GmbH Fidelo Snippet thebing-snippet allows Reflected XSS.This issue affects Fidelo Snippet: from n/a through <= 1.12.	7.1	More Details
CVE-2025-49963	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in growniche Simple Stripe Checkout simple-stripe-checkout allows Reflected XSS.This issue affects Simple Stripe Checkout: from n/a through <= 1.1.28.	7.1	More Details
CVE-2025-49959	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pascal Casier bbPress Move Topics bbp-move-topics allows Reflected XSS.This issue affects bbPress Move Topics: from n/a through <= 1.1.6.	7.1	More Details
CVE-2025-53420	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VibeThemes WPLMS wplms_plugin allows Reflected XSS.This issue affects WPLMS: from n/a through <= 1.9.9.8.	7.1	More Details
CVE-2025-49945	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kylegetson Shortcode Generator shortcode-generator allows Reflected XSS.This issue affects Shortcode Generator: from n/a through <= 1.1.	7.1	More Details
CVE-2025-48092	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jurajpuchky Fix Multiple Redirects fix-multiple-redirects allows Reflected XSS.This issue affects Fix Multiple Redirects: from n/a through <= 1.2.3.	7.1	More Details
CVE-2025-48093	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Calvaweb Password only login password-only-login allows Reflected XSS.This issue affects Password only login: from n/a through <= 0.2.	7.1	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shiva WSAnalytics		More

2025-48097	wsanalytics-google-analytics-and-dashboards allows Reflected XSS.This issue affects WSAnalytics: from n/a through <= 1.1.2.	7.1	Details
CVE-2025-48098	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Survey Maker survey-maker allows Stored XSS.This issue affects Survey Maker: from n/a through <= 5.1.8.8.	7.1	More Details
CVE-2025-49911	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpinstinct WooCommerce Vehicle Parts Finder woo-vehicle-parts-finder allows Reflected XSS.This issue affects WooCommerce Vehicle Parts Finder: from n/a through <= 3.7.	7.1	More Details
CVE-2025-62986	Cross-Site Request Forgery (CSRF) vulnerability in FanBridge FanBridge signup fanbridge-signup allows Stored XSS.This issue affects FanBridge signup: from n/a through <= 0.6.	7.1	More Details
CVE-2025-49930	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrocoBlock JetSearch jet-search allows Reflected XSS.This issue affects JetSearch: from n/a through <= 3.5.10.	7.1	More Details
CVE-2025-49944	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jonatan Jumbert WPCode Content Ratio wpcode-content-ratio allows Reflected XSS.This issue affects WPCode Content Ratio: from n/a through <= 2.0.	7.1	More Details
CVE-2025-49946	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cynob IT Consultancy Auto Login After Registration auto-login-after-registration allows Reflected XSS.This issue affects Auto Login After Registration: from n/a through <= 1.0.0.	7.1	More Details
CVE-2025-49958	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in robokassa Robokassa payment gateway for Woocommerce robokassa allows Reflected XSS.This issue affects Robokassa payment gateway for Woocommerce: from n/a through <= 1.8.1.	7.1	More Details
CVE-2025-49947	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in extendons WooCommerce Registration Fields Plugin - Custom Signup Fields extendons-registration-fields allows Reflected XSS.This issue affects WooCommerce Registration Fields Plugin - Custom Signup Fields: from n/a through <= 3.2.3.	7.1	More Details
CVE-2025-49948	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ahmad Awais WP Super Edit wp-super-edit allows Reflected XSS.This issue affects WP Super Edit: from n/a through <= 2.5.4.	7.1	More Details
CVE-2025-49951	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpcrunch gAppointments gAppointments allows Reflected XSS.This issue affects gAppointments: from n/a through <= 1.14.1.	7.1	More Details
CVE-2025-49953	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themeinity ShareBang, Ultimate Social Share Buttons for WordPress sharebang allows Reflected XSS.This issue affects ShareBang, Ultimate Social Share Buttons for WordPress: from n/a through <= 1.4.	7.1	More Details
CVE-2025-49954	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mithra62 WP-Click-Tracker wp-click-track allows Reflected XSS.This issue affects WP-Click-Tracker: from n/a through <= 0.7.3.	7.1	More Details
CVE-2025-49955	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rajan Vijayan WP Smart Flexslider wp-smart-flexslider allows Reflected XSS.This issue affects WP Smart Flexslider: from n/a through <= 2.5.	7.1	More Details
CVE-2025-49956	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Anandaraj Balu Fade Slider fade-slider allows Reflected XSS.This issue affects Fade Slider: from n/a through <= 2.5.	7.1	More Details
CVE-2025-49957	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Weboccult Technologies Pvt Ltd Email Attachment by Order Status & Products email-attachment-by-order-status-products allows Reflected XSS.This issue affects Email Attachment by Order Status & Products: from n/a through <= 1.0.1.	7.1	More Details
CVE-2025-53352	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in G5Theme Grid Plus grid-plus allows Reflected XSS.This issue affects Grid Plus: from n/a through <= 3.3.	7.1	More Details
CVE-2025-49992	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThimPress LearnPress Export Import learnpress-import-export allows Reflected XSS.This issue affects LearnPress Export Import: from n/a through <= 4.0.9.	7.1	More Details
CVE-2025-60246	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in weissmike Simple Finance Calculator simple-finance-calculator allows Reflected XSS.This issue affects Simple Finance Calculator: from n/a through <= 1.0.	7.1	More Details
CVE-2025-58971	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AmentoTech Doctreat doctreat allows Reflected XSS.This issue affects Doctreat: from n/a through <= 1.6.7.	7.1	More Details
CVE-2025-53422	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeWarriors WhatsApp Chat for WordPress and WooCommerce tw-whatsapp-chat-rotator allows Reflected XSS.This issue affects WhatsApp Chat for WordPress and WooCommerce: from n/a through <= 1.2.1.	7.1	More Details

CVE-2025-60168	Cross-Site Request Forgery (CSRF) vulnerability in integrationshotelrunner HotelRunner Booking Widget hotelrunner allows Stored XSS.This issue affects HotelRunner Booking Widget: from n/a through <= 1.6.	7.1	More Details
CVE-2025-53423	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in designthemes Triss triss allows Reflected XSS.This issue affects Triss: from n/a through <= 2.6.	7.1	More Details
CVE-2025-58966	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Basix NEX-Forms LITE nex-forms-lite allows Reflected XSS.This issue affects NEX-Forms LITE: from n/a through < 8.2.	7.1	More Details
CVE-2025-59004	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pco_58 WC Return products wc-return-product allows Reflected XSS.This issue affects WC Return products: from n/a through <= 1.5.	7.1	More Details
CVE-2025-59571	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in purethemes WorkScout-Core workscout-core allows Reflected XSS.This issue affects WorkScout-Core: from n/a through < 1.7.06.	7.1	More Details
CVE-2025-59006	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themebon Easy Woocommerce Customizer easy-woocommerce-customizer allows Reflected XSS.This issue affects Easy Woocommerce Customizer: from n/a through <= 1.0.2.	7.1	More Details
CVE-2025-53426	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bob Likert Survey Master likert-survey-master allows Reflected XSS.This issue affects Likert Survey Master: from n/a through <= 0.8.0.1.	7.1	More Details
CVE-2025-58961	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kamleshyadav CF7 Auto Responder Addon CF7-autoresponder-addon allows DOM-Based XSS.This issue affects CF7 Auto Responder Addon: from n/a through <= 2.4.	7.1	More Details
CVE-2025-58916	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Munzir Author: Munzir myshouts-shoutbox allows Reflected XSS.This issue affects Author: Munzir: from n/a through <= 0.9.	7.1	More Details
CVE-2025-58921	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Arevico WP Tactical Popup wp-tactical-popup allows Reflected XSS.This issue affects WP Tactical Popup: from n/a through <= 1.1.	7.1	More Details
CVE-2025-12286	A weakness has been identified in VeePN up to 1.6.2. This affects an unknown function of the file C:\Program Files (x86)\VeePN\avservice\avservice.exe of the component AVService. This manipulation causes unquoted search path. The attack requires local access. A high degree of complexity is needed for the attack. The exploitability is reported as difficult. The vendor was contacted early about this disclosure but did not respond in any way.	7.0	More Details
CVE-2025-12247	A weakness has been identified in Hasleo Backup Suite up to 5.2. Impacted is an unknown function of the component HasleoImageMountService/HasleoBackupSuiteService. This manipulation causes unquoted search path. The attack is restricted to local execution. The attack's complexity is rated as high. The exploitability is considered difficult. The exploit has been made available to the public and could be exploited. Upgrading the affected component is advised.	7.0	More Details
CVE-2025-61977	A weak password recovery mechanism for forgotten password vulnerability was discovered in Productivity Suite software version v4.4.1.19. The vulnerability allows an attacker to decrypt an encrypted project by answering just one recovery question.	7.0	More Details
CVE-2025-62793	eLabFTW is an open source electronic lab notebook for research labs. The application served uploaded SVG files inline. Because SVG supports active content, an attacker could upload a crafted SVG that executes script when viewed, resulting in stored XSS under the application origin. A victim who opens the SVG URL or any page embedding it could have their session hijacked, data exfiltrated, or actions performed on their behalf. This vulnerability is fixed n 5.3.0.	6.8	More Details
CVE-2025-9978	The Jeg Kit for Elementor WordPress plugin before 2.7.0 does not sanitize SVG file contents when uploaded via xmlrpc.php, leading to a cross site scripting vulnerability.	6.8	More Details
CVE-2025-58456	A relative path traversal vulnerability was discovered in Productivity Suite software version 4.4.1.19. The vulnerability allows an unauthenticated remote attacker to interact with the ProductivityService PLC simulator and read arbitrary files on the target machine.	6.8	More Details
CVE-2025-56438	An issue in the firmware update mechanism of Nous W3 Smart WiFi Camera v1.33.50.82 allows unauthenticated and physically proximate attackers to escalate privileges to root via supplying a crafted update.tar archive file stored on a FAT32-formatted SD card.	6.8	More Details
CVE-2025-12136	The Real Cookie Banner: GDPR & ePrivacy Cookie Consent plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.2.4. This is due to insufficient validation on the user-supplied URL in the '/scanner/scan-without-login' REST API endpoint. This makes it possible for authenticated attackers, with administrator-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 via the `url` parameter.	6.8	More Details
CVE-2025-12351	Honeywell S35 Series Cameras contains an authorization bypass Vulnerability through User controller key. An attacker could potentially exploit this vulnerability, leading to Privilege Escalation to admin privileged functionalities . Honeywell also recommends updating to the most recent version of this product, service or offering (S35 Pinhole/Kit Camera to version 2025.08.28, S35 AI Fisheye & Dual Sensor/Micro Dome/Full Color Eyeball & Bullet Camera to version 2025.08.22, S35 Thermal Camera to version 2025.08.26).	6.8	More Details

CVE-2025-23299	NVIDIA Bluefield and ConnectX contain a vulnerability in the management interface that could allow a malicious actor with high privilege access to execute arbitrary code.	6.7	More Details
CVE-2025-48428	Cleartext Storage of Sensitive Information (CWE-312) in the Gallagher Morpho integration could allow an authenticated user with access to the Command Centre Server to export a specific signing key while in use allowing them to deploy a compromised or counterfeit device on that site. This issue affects Command Centre Server: 9.20 prior to vEL9.20.2819 (MR4), 9.10 prior to vEL9.10.3672 (MR7), 9.00 prior to vEL9.00.3831 (MR8), all versions of 8.90 and prior.	6.7	More Details
CVE-2025-12295	A weakness has been identified in D-Link DAP-2695 2.00RC13. The affected element is the function sub_40C6B8 of the component Firmware Update Handler. Executing manipulation can lead to improper verification of cryptographic signature. The attack can be launched remotely. Attacks of this nature are highly complex. The exploitability is described as difficult. The exploit has been made available to the public and could be exploited. This vulnerability only affects products that are no longer supported by the maintainer.	6.6	More Details
CVE-2025-62969	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in XLPlugins NextMove Lite woo-thank-you-page-nextmove-lite allows Stored XSS.This issue affects NextMove Lite: from n/a through <= 2.21.0.	6.5	More Details
CVE-2025-54967	An issue was discovered in BAE SOCET GXP before 4.6.0.3. It permits external entities in certain XML-based files. An attacker who is able to social engineer a SOCET GXP user into opening a malicious file can trigger a variety of outbound requests, potentially compromising sensitive information in the process.	6.5	More Details
CVE-2025-49929	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ultimate Blocks Ultimate Blocks ultimate-blocks allows Stored XSS.This issue affects Ultimate Blocks: from n/a through <= 3.3.6.	6.5	More Details
CVE-2025-61464	gnuboard gnuboard4 v4.36.04 and before is vulnerable to Second-order SQL Injection via the search_table in bbs/search.php.	6.5	More Details
CVE-2025-49928	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrocoBlock JetWooBuilder jet-woo-builder allows DOM-Based XSS.This issue affects JetWooBuilder: from n/a through <= 2.1.20.	6.5	More Details
CVE-2025-62963	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Estatik Estatik estatik allows DOM-Based XSS.This issue affects Estatik: from n/a through <= 4.1.13.	6.5	More Details
CVE-2025-49927	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrocoBlock JetWooBuilder jet-woo-builder allows Stored XSS.This issue affects JetWooBuilder: from n/a through <= 2.1.20.1.	6.5	More Details
CVE-2025-62987	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Builderall Builderall Builder for WordPress builderall-cheetah-for-wp allows Stored XSS.This issue affects Builderall Builder for WordPress: from n/a through <= 3.0.1.	6.5	More Details
CVE-2025-62885	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RexTheme WP VR wpvr allows DOM-Based XSS.This issue affects WP VR: from n/a through <= 8.5.42.	6.5	More Details
CVE-2025-10748	The RapidResult plugin for WordPress is vulnerable to SQL Injection via the 's' parameter in all versions up to, and including, 1.2. This is 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 contributor-level permissions and above to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-62985	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in llamaman Simple Pull Quote simple-pull-quote allows Stored XSS.This issue affects Simple Pull Quote: from n/a through <= 1.6.3.	6.5	More Details
CVE-2025-11375	Consul and Consul Enterprise's ("Consul") event endpoint is vulnerable to denial of service (DoS) due to lack of maximum value on the Content Length header. This vulnerability, CVE-2025-11375, is fixed in Consul Community Edition 1.22.0 and Consul Enterprise 1.22.0, 1.21.6, 1.20.8 and 1.18.12.	6.5	More Details
CVE-2025-62948	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Konstantin Pankratov Date counter date-counter allows Stored XSS.This issue affects Date counter: from n/a through <= 2.0.3.	6.5	More Details
CVE-2025-48096	Missing Authorization vulnerability in FRESHFACE Custom CSS custom-css-editor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Custom CSS: from n/a through <= 1.4.0.	6.5	More Details
CVE-2025-11374	Consul and Consul Enterprise's ("Consul") key/value endpoint is vulnerable to denial of service (DoS) due to incorrect Content Length header validation. This vulnerability, CVE-2025-11374, is fixed in Consul Community Edition 1.22.0 and Consul Enterprise 1.22.0, 1.21.6, 1.20.8 and 1.18.12.	6.5	More Details
CVE-2025-62949	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BuddyDev Activity Plus Reloaded for BuddyPress bp-activity-plus-reloaded allows Stored XSS.This issue affects Activity Plus Reloaded for BuddyPress: from n/a through <= 1.1.2.	6.5	More Details
CVE-2025-62984	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPeka WP AdCenter wpadcenter allows Stored XSS.This issue affects WP AdCenter: from n/a through <= 2.6.1.	6.5	More Details

CVE-2025-54963	An issue was discovered in BAE SOCET GXP before 4.6.0.2. An attacker with the ability to interact with the GXP Job Service may submit a crafted job request that grants read access to files on the filesystem with the permissions of the GXP Job Service process. The path to a file is not sanitized for directory traversal, potentially allowing an attacker to read sensitive files in some configurations.	6.5	More Details
CVE-2025-54970	An issue was discovered in BAE SOCET GXP before 4.6.0.2. The SOCET GXP Job Status Service fails to authenticate requests. In some configurations, this may allow remote or local users to abort jobs or read information without the permissions of the job owner.	6.5	More Details
CVE-2025-50951	FontForge v20230101 was discovered to contain a memory leak via the utf7toutf8_copy function at /fontforge/sfd.c.	6.5	More Details
CVE-2025-49908	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPClever WPC Countdown Timer for WooCommerce wpc-countdown-timer allows Stored XSS.This issue affects WPC Countdown Timer for WooCommerce: from n/a through <= 3.1.4.	6.5	More Details
CVE-2025-62019	Missing Authorization vulnerability in WPZOOM Recipe Card Blocks for Gutenberg & Elementor recipe-card-blocks-by-wpzoom.This issue affects Recipe Card Blocks for Gutenberg & Elementor: from n/a through <= 3.4.8.	6.5	More Details
CVE-2025-62951	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in icc0rz Interactive Content – H5P h5p allows Stored XSS.This issue affects Interactive Content – H5P: from n/a through <= 1.16.0.	6.5	More Details
CVE-2025-50949	FontForge v20230101 was discovered to contain a memory leak via the component DlgCreate8.	6.5	More Details
CVE-2025-62983	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sudar Muthu Posts By Tag posts-by-tag allows Stored XSS.This issue affects Posts By Tag: from n/a through <= 3.2.1.	6.5	More Details
CVE-2025-62967	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in designinvento DirectoryPress directorypress allows DOM-Based XSS.This issue affects DirectoryPress: from n/a through <= 3.6.25.	6.5	More Details
CVE-2025-60852	A CSV Injection vulnerability existed in Instant Developer Foundation versions prior to 25.0.9600. Applications built with affected versions of the framework did not properly sanitize user-controlled input before including it in CSV exports. This issue could lead to code execution on the system where the exported CSV file is opened.	6.5	More Details
CVE-2025-5983	The Meta Tag Manager WordPress plugin before 3.3 does not restrict which roles can create http-equiv refresh meta tags.	6.5	More Details
CVE-2025-62974	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CoSchedule Headline Analyzer headline-analyzer allows Stored XSS.This issue affects Headline Analyzer: from n/a through <= 1.3.7.	6.5	More Details
CVE-2025-46425	Dell Storage Center - Dell Storage Manager, version(s) 20.1.20, contain(s) an Improper Restriction of XML External Entity Reference vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	6.5	More Details
CVE-2025-62968	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sayan Datta WP Last Modified Info wp-last-modified-info allows Stored XSS.This issue affects WP Last Modified Info: from n/a through <= 1.9.2.	6.5	More Details
CVE-2025-62971	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrestaProject Attesa Extra attesa-extra allows Stored XSS.This issue affects Attesa Extra: from n/a through <= 1.4.5.	6.5	More Details
CVE-2025-56007	CRLF-injection in KeeneticOS before 4.3 at "/auth" API endpoint allows attackers to take over the device via adding additional users with full permissions by managing the victim to open page with exploit.	6.5	More Details
CVE-2025-49939	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrocoBlock JetElements For Elementor jet-elements allows Stored XSS.This issue affects JetElements For Elementor: from n/a through <= 2.7.8.	6.5	More Details
CVE-2025-49932	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrocoBlock JetBlog jet-blog allows Stored XSS.This issue affects JetBlog: from n/a through <= 2.4.4.1.	6.5	More Details
CVE-2025-33126	IBM DB2 High Performance Unload 6.1.0.3, 5.1.0.1, 6.1.0.2, 6.5, 6.5.0.0 IF1, 6.1.0.1, 6.1, 5.1, 6.1.0.3, 5.1.0.1, 6.1.0.2, 6.5, 6.5.0.0 IF1, 6.1.0.1, 6.1, 5.1, 6.1.0.3, 5.1.0.1, 6.1.0.2, 6.5, 6.5.0.0 IF1, 6.1.0.1, 6.1, 5.1, 6.1.0.3, 5.1.0.1, 6.1.0.2, 6.5, 6.5.0.0 IF1, 6.1.0.1, 6.1, and 5.1 could allow an authenticated user to cause the program to crash due to the incorrect calculation of a buffer size.	6.5	More Details
CVE-2025-49933	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrocoBlock JetBlog jet-blog allows Reflected XSS.This issue affects JetBlog: from n/a through <= 2.4.4.	6.5	More Details

CVE-2025-62068	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in E2Pdf e2pdf e2pdf.This issue affects e2pdf: from n/a through <= 1.28.09.	6.5	More Details
CVE-2025-62069	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 MDTF wp-meta-data-filter-and-taxonomy-filter.This issue affects MDTF: from n/a through <= 1.3.3.8.	6.5	More Details
CVE-2025-62706	Authlib is a Python library which builds OAuth and OpenID Connect servers. Prior to version 1.6.5, Authlib's JWE zip=DEF path performs unbounded DEFLATE decompression. A very small ciphertext can expand into tens or hundreds of megabytes on decrypt, allowing an attacker who can supply decryptable tokens to exhaust memory and CPU and cause denial of service. This issue has been patched in version 1.6.5. Workarounds for this issue involve rejecting or stripping zip=DEF for inbound JWEs at the application boundary, forking and add a bounded decompression guard via decompressobj().decompress(data, MAX_SIZE)) and returning an error when output exceeds a safe limit, or enforcing strict maximum token sizes and fail fast on oversized inputs; combine with rate limiting.	6.5	More Details
CVE-2025-52738	Missing Authorization vulnerability in Wikimedia Foundation Wikipedia Preview wikipedia-preview allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Wikipedia Preview: from n/a through <= 1.15.0.	6.5	More Details
CVE-2025-58970	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in AmentoTech Doctreat doctreat allows Code Injection.This issue affects Doctreat: from n/a through <= 1.6.7.	6.5	More Details
CVE-2025-33131	IBM DB2 High Performance Unload 6.1.0.3, 5.1.0.1, 6.1.0.2, 6.5, 6.5.0.0 IF1, 6.1.0.1, 6.1, and 5.1 could allow an authenticated user to cause the program to crash due to a buffer being overwritten when it is allocated on the stack.	6.5	More Details
CVE-2025-62060	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Tab Ultimate tabs-pro.This issue affects Tab Ultimate: from n/a through <= 1.8.	6.5	More Details
CVE-2025-52752	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in ThemeAtelier IDonatePro idonate-pro allows Retrieve Embedded Sensitive Data.This issue affects IDonatePro: from n/a through <= 2.1.9.	6.5	More Details
CVE-2025-33132	IBM DB2 High Performance Unload 6.1.0.3, 5.1.0.1, 6.1.0.2, 6.5, 6.5.0.0 IF1, 6.1.0.1, 6.1, and 5.1 could allow an authenticated user to cause the program to crash due to the incorrect calculation of the size of the data that is being pointed to.	6.5	More Details
CVE-2025-33133	IBM DB2 High Performance Unload 6.1.0.3, 5.1.0.1, 6.1.0.2, 6.5, 6.5.0.0 IF1, 6.1.0.1, 6.1, and 5.1 could allow an authenticated user to cause the program to crash due an out of bounds write.	6.5	More Details
CVE-2025-59462	An attacker who tampers with the C++ CLI client may crash the UpdateService during file transfers, disrupting updates and availability.	6.5	More Details
CVE-2025-53424	Missing Authorization vulnerability in vanquish WooCommerce Orders & Customers Exporter woocommerce-orders-ei allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WooCommerce Orders & Customers Exporter: from n/a through <= 5.4.	6.5	More Details
CVE-2025-11879	The GenerateBlocks plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'get_option_rest' function in all versions up to, and including, 2.1.1. This makes it possible for authenticated attackers, with contributor level access and above, to read arbitrary WordPress options, including sensitive information such as SMTP credentials, API keys, and other data stored by other plugins.	6.5	More Details
CVE-2025-62063	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Travel WP Travel Gutenberg Blocks wp-travel-blocks.This issue affects WP Travel Gutenberg Blocks: from n/a through <= 3.9.2.	6.5	More Details
CVE-2025-49960	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in leadbi LeadBI Plugin for WordPress leadbi allows Stored XSS.This issue affects LeadBI Plugin for WordPress: from n/a through <= 1.7.	6.5	More Details
CVE-2025-62058	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in favethemes Houzez Theme - Functionality houzez-theme-functionality.This issue affects Houzez Theme - Functionality: from n/a through < 4.2.0.	6.5	More Details
CVE-2025-11974	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 11.7 before 18.3.5, 18.4 before 18.4.3, and 18.5 before 18.5.1 that could have allowed an unauthenticated attacker to create a denial of service condition by uploading large files to specific API endpoints.	6.5	More Details
CVE-2025-48088	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force Ultimate Addons for WPBakery Page Builder allows Stored XSS.This issue affects Ultimate Addons for WPBakery Page Builder: from n/a before 3.21.1.	6.5	More Details
CVE-2025-49936	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in xtemos WoodMart woodmart allows DOM-Based XSS.This issue affects WoodMart: from n/a through < 8.3.2.	6.5	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrocoBlock JetEngine jet-		More

2025-49938	engine allows Stored XSS.This issue affects JetEngine: from n/a through <= 3.7.3.	6.5	Details
CVE-2025-62024	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jonathan Jernigan Pie Calendar pie-calendar.This issue affects Pie Calendar: from n/a through <= 1.2.9.	6.5	More Details
CVE-2025-62921	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pagup Bulk Auto Image Title Attribute bulk-image-title-attribute allows DOM-Based XSS.This issue affects Bulk Auto Image Title Attribute: from n/a through <= 2.0.1.	6.5	More Details
CVE-2025-49940	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeFusion Fusion Builder fusion-builder allows DOM-Based XSS.This issue affects Fusion Builder: from n/a through <= 3.13.2.	6.5	More Details
CVE-2025-11971	GitLab has remediated an issue in GitLab EE affecting all versions from 10.6 before 18.3.5, 18.4 before 18.4.3, and 18.5 before 18.5.1 that could have allowed an authenticated attacker to trigger unauthorized pipeline executions by manipulating commits.	6.5	More Details
CVE-2023-49440	AhnLab EPP 1.0.15 is vulnerable to SQL Injection via the "preview parameter."	6.5	More Details
CVE-2025-62042	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bastien Ho Event post event-post.This issue affects Event post: from n/a through <= 5.10.3.	6.5	More Details
CVE-2025-61430	Improper handling of DNS over TCP in Simple DNS Plus v9 allows a remote attacker with querying access to the DNS server to cause the server to return request payloads from other clients. This happens when the TCP length prefix is malformed (len differs from actual packet len), and due to a concurrency/buffering issue, even when the lengths match. A length prefix that is smaller than the actual packet size increases information leakage. In summary, this vulnerability allows an attacker to see DNS queries of other clients.	6.5	More Details
CVE-2025-36170	IBM QRadar SIEM 7.5 through 7.5.0 Update Pack 13 Independent Fix 02 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-2025-8413	The Listeo theme for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `soundcloud` shortcode in version less than, or equal to, 2.0.8 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-2025-36138	IBM QRadar SIEM 7.5 through 7.5.0 Update Pack 13 Independent Fix 02 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-2025-10737	The Open Source Genesis Framework theme for WordPress is vulnerable to Stored Cross-Site Scripting via the theme's shortcodes in all versions up to, and including, 3.6.0 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-2025-11823	The ShopLentor – WooCommerce Builder for Elementor & Gutenberg +21 Modules – All in One Solution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'button_exist_text' parameter in the 'wishsuite_button' shortcode in all versions up to, and including, 3.2.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11875	The SpendeOnline.org plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'spendeonline' shortcode in all versions up to, and including, 3.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-10580	The Widget Options – The #1 WordPress Widget & Block Control Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple functions in all versions up to, and including, 4.1.2 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-2025-12096	The Simple Excel Pricelist for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pricelist' shortcode in all versions up to, and including, 1.13 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-2025-8588	The Gutenberg Blocks – PublishPress Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Marker Title' and 'Marker Description' parameters for the Maps block in versions up to, and including, 3.3.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor-level access and above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11897	The The7 — Website and eCommerce Builder for WordPress theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘ the7_fancy_title_css’ parameter in all versions up to, and including, 12.9.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE-2025-7730	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘percentage’ parameter in all versions up to, and including, 5.4.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-10701	The Time Clock – A WordPress Employee & Volunteer Time Clock Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'data' parameter in all versions up to, and including, 1.3.1. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with Time Clock user credentials to inject arbitrary web scripts in pages that will execute whenever a user accesses an affected page.	6.4	More Details
CVE-2025-8666	The Testimonial Carousel For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters in versions less than, or equal to, 11.6.2 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-2025-64094	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to 10.1.1, sanitization of the content of uploaded SVG files was not covering all possible XSS scenarios. This vulnerability exists because of an incomplete fix for CVE-2025-48378. This vulnerability is fixed in 10.1.1.	6.4	More Details
CVE-2025-11825	The Playerzbr plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'urlmeta' post meta field in all versions up to, and including, 1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11866	The Photographers galleries plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple shortcode attributes (`w`, `h`, `raw_css`, `look`, etc.) in all versions up to, and including, 1.1.8. This is due to the plugin not properly sanitizing user input or escaping output when inserting these values into HTML attributes and inline styles. 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-2025-11810	The Print Button Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'print-button' shortcode in all versions up to, and including, 1.0.1. This is due to insufficient input sanitization and output escaping on the 'target' attribute. 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-2025-11811	The Simple Youtube Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'embed_youtube' shortcode in all versions up to, and including, 1.1.3. This is due to insufficient input sanitization and output escaping on the 'id' attribute. 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-2025-11813	The Responsive iframe GoogleMap plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'responsive_map' shortcode in all versions up to, and including, 1.0.2. This is due to insufficient input sanitization and output escaping on the 'width' and 'height' 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-2025-11817	The Simple Tableau Viz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tableau' shortcode in all versions up to, and including, 2.0. This is 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-2025-11818	The WP Responsive Meet The Team plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wprm_team' shortcode in all versions up to, and including, 1.0.1. This is 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-2025-11819	The WP-Thumbnail plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'roboshot' shortcode in all versions up to, and including, 1.1. This is 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-2025-8427	The Beaver Builder Plugin (Starter Version) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘auto_play’ parameter in all versions up to, and including, 2.9.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11824	The Cinza Grid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cgrid_skin_content' post meta field in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11880	The SM CountDown Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's smcountdown shortcode in versions less than, or equal to, 1.2 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-2025-11827	The Oboxmedia Ads plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'before_widget' and 'after_widget' parameters of the oboxads-ad-widget shortcode in all versions up to, and including, 1.9.8. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-	The ST Categories Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's st-categories shortcode in versions less than, or equal to, 1.0.0. This is due to insufficient input sanitization and output escaping on user	6.4	More

11878	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.		Details
CVE-2025-11872	The Material Design Iconic Font Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mdiconic' shortcode in all versions up to, and including, 2 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-2025-11870	The Simple Business Data plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'simple_business_data' shortcode attributes in all versions up to, and including, 1.0.1. This is due to the plugin not properly sanitizing user input or escaping output when embedding the `type` attribute into the `class` attribute in rendered HTML. 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-2025-11867	The Bg Book Publisher plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `book_author` post meta, rendered through the `[book_author]` shortcode, in all versions up to, and including, 1.25. This is due to the plugin not properly escaping the meta value before output. 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-2025-11830	The WP Restaurant Listings plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'align' parameter of the restaurant_summary shortcode in all versions up to, and including, 1.0.2. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11809	The WP-Force Images Download plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpfid' shortcode in all versions up to, and including, 1.8. This is due to insufficient input sanitization and output escaping on the 'class' attribute. 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-2025-11807	The Mixlr Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mixlr' shortcode in all versions up to, and including, 1.0.1. This is due to insufficient input sanitization and output escaping on the 'url' attribute. 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-2025-11883	The Responsive Progress Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's rprogress shortcode in versions less than, or equal to, 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-2025-11804	The JB News Ticker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' shortcode attribute of the 'jbticker' shortcode in all versions up to, and including, 1.0. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-10138	The This-or-That plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'thisorthat' shortcode in all versions up to, and including, 1.0.4 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-2025-11834	The WP AD Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'startindex' parameter of the ad-gallery shortcode in all versions up to, and including, 1.3. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12242	A vulnerability has been found in CodeAstro Gym Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/actions/check-attendance.php. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-12223	A vulnerability was detected in Bdtask Flight Booking Software up to 3.1. This affects an unknown part of the file /b2c/package-information of the component Package Information Module. The manipulation results in unrestricted upload. 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.	6.3	More Details
CVE-2025-12305	A vulnerability was found in quequnlong shiyi-blog up to 1.2.1. This impacts an unknown function of the file src/main/java/com/mojian/controller/SysJobController.java of the component Job Handler. The manipulation results in deserialization. The attack can be executed remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-12243	A vulnerability was found in code-projects Client Details System 1.0. Affected by this issue is some unknown functionality of the file clientdetails/welcome.php of the component GET Parameter Handler. Performing manipulation of the argument ID results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-12249	A vulnerability was detected in Axosoft Scrum and Bug Tracking 22.1.1.11545. The impacted element is an unknown function of the component Edit Ticket Page. Performing manipulation of the argument Title results in csv injection. It is possible to initiate the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-12313	A vulnerability has been found in D-Link DI-7001 MINI 19.09.19A1/24.04.18B1. The affected element is an unknown function of the file /msp_info.htm. Such manipulation of the argument cmd leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-	The URL Shortener Plugin For WordPress plugin for WordPress is vulnerable to unauthorized access to functionality provided by the API due to a missing capability check on the verifyRequest function in all versions up to, and including, 3.0.7. This makes it	6.3	More Details

10740	possible for authenticated attackers, with Subscriber-level access and above, to modify links.		
CVE-2025-12268	A vulnerability has been found in LearnHouse up to 98dfad76aad70711a8113f6c1fdabfccf10509ca. Impacted is an unknown function of the file /api/v1/courses/ of the component Course Thumbnail Handler. The manipulation of the argument thumbnail leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-12254	A vulnerability was identified in code-projects Online Event Judging System 1.0. Affected by this issue is some unknown functionality of the file /add_judge.php. Such manipulation of the argument fullname leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-12266	A vulnerability was detected in Zytec Dalian Zhuoyun Technology Central Authentication Service up to 20251009. This vulnerability affects the function _empty of the file /index.php/auth/widget. Performing manipulation of the argument get.layer/get.widget/get.action results in code injection. 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-2025-12263	A vulnerability was identified in code-projects Online Event Judging System 1.0. Affected is an unknown function of the file /edit_judge.php. The manipulation of the argument judge_id leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-12262	A vulnerability was determined in code-projects Online Event Judging System 1.0. This impacts an unknown function of the file /edit_criteria.php. Executing manipulation of the argument crit_id can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-12261	A vulnerability was found in CodeAstro Gym Management System 1.0. This affects an unknown function of the file /admin/actions/remove-announcement.php. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-12252	A vulnerability was found in code-projects Online Event Judging System 1.0. Affected is an unknown function of the file /ajax/action.php. The manipulation of the argument content results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-12238	A security flaw has been discovered in code-projects Automated Voting System 1.0. The affected element is an unknown function of the file /admin/user.php. Performing manipulation of the argument Username results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-12327	A vulnerability was determined in shawon100 RUET OJ up to 18fa45b0a669fa1098a0b8fc629cf6856369d9a5. This issue affects some unknown processing of the file /description.php. 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. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-62523	PILOS (Platform for Interactive Live-Online Seminars) is a frontend for BigBlueButton. PILOS before 4.8.0 includes a Cross-Origin Resource Sharing (CORS) misconfiguration in its middleware: it reflects the Origin request header back in the Access-Control-Allow-Origin response header without proper validation or a whitelist, while Access-Control-Allow-Credentials is set to true. This behavior could allow a malicious website on a different origin to send requests (including credentials) to the PILOS API. This may enable exfiltration or actions using the victim's credentials if the server accepts those cross-origin requests as authenticated. Laravel's session handling applies additional origin checks such that cross-origin requests are not authenticated by default. Because of these session-origin protections, and in the absence of any other unknown vulnerabilities that would bypass Laravel's origin/session checks, this reflected-Origin CORS misconfiguration is not believed to be exploitable in typical PILOS deployments. This vulnerability has been patched in PILOS in v4.8.0	6.3	More Details
CVE-2025-27093	Sliver is a command and control framework that uses a custom Wireguard netstack. In versions 1.5.43 and earlier, and in development version 1.6.0-dev, the netstack does not limit traffic between Wireguard clients. This allows clients to communicate with each other unrestrictedly, potentially enabling leaked or recovered keypairs to be used to attack operators or allowing port forwardings to be accessible from other implants.	6.3	More Details
CVE-2025-8483	The The Discussion Board – WordPress Forum Plugin plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.5.5. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes.	6.3	More Details
CVE-2025-53421	Missing Authorization vulnerability in PickPlugins Accordion accordions allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Accordion: from n/a through <= 2.3.14.	6.3	More Details
CVE-2025-53236	Missing Authorization vulnerability in AndonDesign UDesign Core u-design-core allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects UDesign Core: from n/a through <= 4.14.0.	6.3	More Details
CVE-2025-52757	Missing Authorization vulnerability in FantasticPlugins SUMO Memberships for WooCommerce sumomemberships allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SUMO Memberships for WooCommerce: from n/a through <= 7.6.0.	6.3	More Details
CVE-2025-49961	Missing Authorization vulnerability in Breeze Team Breeze Checkout breeze-checkout allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Breeze Checkout: from n/a through <= 1.4.0.	6.3	More Details
CVE-2025-49952	Authorization Bypass Through User-Controlled Key vulnerability in favethemes Houzez houzez allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Houzez: from n/a through <= 4.1.1.	6.3	More Details

CVE-2025-36361	IBM App Connect Enterprise 13.0.1.0 through 13.0.4.2, and 12.0.1.0 through 12.0.12.17 could allow an authenticated user to perform unauthorized actions on customer defined resources due to missing authorization.	6.3	More Details
CVE-2025-12347	A flaw has been found in MaxSite CMS up to 109. This issue affects some unknown processing of the file application/maxsite/admin/plugins/editor_files/save-file-ajax.php. Executing manipulation of the argument file_path/content can lead to unrestricted upload. The attack can be executed 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.	6.3	More Details
CVE-2025-12203	A weakness has been identified in givanz Vvveb up to 1.0.7.3. This issue affects the function sanitizeFileName of the file system/functions.php of the component Code Editor. Executing manipulation of the argument File can lead to path traversal. The attack can be launched remotely. The exploit has been made available to the public and could be exploited. This patch is called b0fa7ff74a3539c6d37000db152caad572e4c39b. Applying a patch is advised to resolve this issue.	6.3	More Details
CVE-2025-12346	A vulnerability was detected in MaxSite CMS up to 109. This vulnerability affects unknown code of the file application/maxsite/admin/plugins/auto_post/uploads-require-maxsite.php of the component HTTP Header Handler. Performing manipulation of the argument X-Requested-FileName/X-Requested-FileUpDir results in unrestricted upload. Remote exploitation of the attack is possible. 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-2025-12344	A vulnerability has been found in Yonyou U8 Cloud up to 5.1sp. The impacted element is an unknown function of the file /service/NCloudGatewayServlet of the component Request Header Handler. Such manipulation of the argument ts/sign leads to unrestricted upload. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-12222	A security vulnerability has been detected in Bdtask Flight Booking Software up to 3.1. Affected by this issue is some unknown functionality of the file /admin/transaction/deposit of the component Deposit Handler. The manipulation leads to unrestricted upload. 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.	6.3	More Details
CVE-2025-12255	A security flaw has been discovered in code-projects Online Event Judging System 1.0. This affects an unknown part of the file /add_contestant.php. Performing manipulation of the argument fullname results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-12329	A security flaw has been discovered in shawon100 RUET OJ up to 18fa45b0a669fa1098a0b8fc629cf6856369d9a5. The affected element is an unknown function of the file /details.php. Performing 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 exploited. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-12328	A vulnerability was identified in shawon100 RUET OJ up to 18fa45b0a669fa1098a0b8fc629cf6856369d9a5. Impacted is an unknown function of the file /contestproblem.php. Such manipulation of the argument Name leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-12256	A weakness has been identified in code-projects Online Event Judging System 1.0. This vulnerability affects unknown code of the file /edit_contestant.php. Executing manipulation of the argument contestant_id can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-46185	An Insecure Permission vulnerability in pgcodekeeper 10.12.0 allows a local attacker to obtain sensitive information via the plaintext storage of passwords and usernames.	6.2	More Details
CVE-2025-60419	An issue was discovered in the NDIS Usermode IO driver (RtkIOAC60.sys, version 6.0.5600.16348) allowing local authenticated attackers to send a crafted IOCTL request to the driver to cause a denial of service.	6.2	More Details
CVE-2025-10023	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (Services Meta-services modules) allows Stored XSS by users with elevated privileges.This issue affects Infra Monitoring: from 24.10.0 before 24.10.9, from 24.04.0 before 24.04.16, from 23.10.0 before 23.10.26.	6.2	More Details
CVE-2025-36083	IBM Concert Software 1.0.0 through 2.0.0 could allow a local user to obtain sensitive information from buffers due to improper clearing of heap memory before release.	6.2	More Details
CVE-2025-60791	Easywork Enterprise 2.1.3.354 is vulnerable to Cleartext Storage of Sensitive Information in Memory. The application leaves valid device-bound license keys in process memory after a failed activation attempt. The keys can be obtained by attaching a debugger or analyzing the process/memory dump and then they can be used to activate the software on the same machine without purchasing.	6.2	More Details
CVE-2025-62936	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Jthemes xSmart xsmart allows Code Injection.This issue affects xSmart: from n/a through <= 1.2.9.4.	6.1	More Details
CVE-2025-61413	A stored cross-site scripting (XSS) vulnerability in the /manager/pages component of Piranha CMS v12.0 allows attackers to execute arbitrary web scripts or HTML via creating a page and injecting a crafted payload into the Markdown blocks.	6.1	More Details
CVE-2025-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RomanCode MapSVG mapsvg-lite-interactive-vector-maps allows DOM-Based XSS.This issue affects MapSVG: from n/a through <= 8.7.15.	6.1	More Details

62930			
CVE-2025-11992	The Multi Item Responsive Slider plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing or incorrect nonce validation on the 'mioptions.php' page. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-60837	A reflected cross-site scripting (XSS) vulnerability in MCMS v6.0.1 allows attackers to execute arbitrary Javascript in the context of a user's browser via a crafted payload.	6.1	More Details
CVE-2025-55757	A unauthenticated reflected XSS vulnerability in VirtueMart 1.0.0-4.4.10 for Joomla was discovered.	6.1	More Details
CVE-2025-49923	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Craig Hewitt Seriously Simple Podcasting seriously-simple-podcasting allows DOM-Based XSS.This issue affects Seriously Simple Podcasting: from n/a through <= 3.11.1.	6.1	More Details
CVE-2025-57240	Cross site scripting (XSS) vulnerability in 17gz International Student service system 1.0 allows attackers to execute arbitrary code via the registration step.	6.1	More Details
CVE-2025-62923	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Debuggers Studio Marquee Addons for Elementor marquee-addons-for-elementor allows DOM-Based XSS.This issue affects Marquee Addons for Elementor: from n/a through <= 3.7.12.	6.1	More Details
CVE-2025-60859	Cross Site Scripting (XSS) vulnerability in Gnuboard 5.6.15 allows authenticated attackers to execute arbitrary code via crafted c_id parameter in bbs/view_comment.php.	6.1	More Details
CVE-2025-52760	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Globalis MultiSite Clone Duplicator multisite-clone-duplicator allows Reflected XSS.This issue affects MultiSite Clone Duplicator: from n/a through <= 1.5.3.	6.1	More Details
CVE-2025-56008	Cross site scripting (XSS) vulnerability in KeeneticOS before 4.3 at "Wireless ISP" page allows attackers located near to the router to takeover the device via adding additional users with full permissions.	6.1	More Details
CVE-2025-54965	An XSS issue was discovered in BAE SOCET GXP before 4.6.0.2. The SOCET GXP Job Status Service does not properly sanitize the job ID parameter before using it in the job status page. An attacker who is able to social engineer a user into clicking a malicious link may be able to execute arbitrary JavaScript in the victim's browser.	6.1	More Details
CVE-2025-54969	An issue was discovered in BAE SOCET GXP before 4.6.0.2. The SOCET GXP Job Status Service does not implement CSRF protections. An attacker who social engineers a valid user into clicking a malicious link or visiting a malicious website may be able to submit requests to the Job Status Service without the user's knowledge.	6.1	More Details
CVE-2025-12017	The VNPAY Payment gateway plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'message' parameter in all versions up to, and including, 1.0.0 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-2025-60936	Emoncms 11.7.3 is vulnerable to Cross Site in the input handling mechanism. This vulnerability allows authenticated attackers with API access to inject malicious JavaScript code that executes when administrators view the application logs.	6.1	More Details
CVE-2025-41384	Cross-Site Scripting (XSS) vulnerability reflected in SuiteCRM v7.14.1. This vulnerability allows an attacker to execute JavaScript code by modifying the HTTP Referer header to include an arbitrary domain with malicious JavaScript code at the end. The server will attempt to block the arbitrary domain but will allow the JavaScript code to execute.	6.1	More Details
CVE-2025-12390	A flaw was found in Keycloak. In Keycloak where a user can accidentally get access to another user's session if both use the same device and browser. This happens because Keycloak sometimes reuses session identifiers and doesn’t clean up properly during logout when browser cookies are missing. As a result, one user may receive tokens that belong to another user.	6.0	More Details
CVE-2025-59593	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Extend Themes Colibri Page Builder colibri-page-builder allows Stored XSS.This issue affects Colibri Page Builder: from n/a through < 1.0.334.	5.9	More Details
CVE-2025-60135	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NIKITAS GEORGOPOULOS WeShare Buttons e-mailit allows Stored XSS.This issue affects WeShare Buttons: from n/a through <= 13.0.0.	5.9	More Details
CVE-2025-62710	Sakai is a Collaboration and Learning Environment. Prior to versions 23.5 and 25.0, EncryptionUtilityServiceImpl initialized an AES256TextEncryptor password (serverSecretKey) using RandomStringUtils with the default java.util.Random. java.util.Random is a non-cryptographic PRNG and can be predicted from limited state/seed information (e.g., start time window), substantially reducing the effective search space of the generated key. An attacker who can obtain ciphertexts (e.g., exported or at-rest strings protected by this service) and approximate the PRNG seed can feasibly reconstruct the serverSecretKey and decrypt affected data. SAK-49866 is patched in Sakai 23.5, 25.0, and trunk.	5.9	More Details
CVE-2025-40843	CodeChecker is an analyzer tooling, defect database and viewer extension for the Clang Static Analyzer and Clang Tidy. CodeChecker versions up to 6.26.1 contain a buffer overflow vulnerability in the internal ldlogger library, which is executed by the CodeChecker log command. This issue affects CodeChecker: through 6.26.1.	5.9	More Details

CVE-2025-49912	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nks Email Subscription Popup email-subscribe allows Stored XSS.This issue affects Email Subscription Popup: from n/a through <= 1.2.26.	5.9	More Details
CVE-2025-48095	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Survey Maker survey-maker allows Stored XSS.This issue affects Survey Maker: from n/a through <= 5.1.8.8.	5.9	More Details
CVE-2025-5350	SSRF and Reflected XSS Vulnerabilities exist in multiple WSO2 products within the deprecated Try-It feature, which was accessible only to administrative users. This feature accepted user-supplied URLs without proper validation, leading to server-side request forgery (SSRF). Additionally, the retrieved content was directly reflected in the HTTP response, enabling reflected cross-site scripting (XSS) in the admin user's browser context. By tricking an administrator into accessing a crafted link, an attacker could force the server to fetch malicious content and reflect it into the admin’s browser, leading to arbitrary JavaScript execution for UI manipulation or data exfiltration. While session cookies are protected with the HttpOnly flag, the XSS still poses a significant security risk. Furthermore, SSRF can be used by a privileged user to query internal services, potentially aiding in internal network enumeration if the target endpoints are reachable from the affected product.	5.9	More Details
CVE-2025-62517	Rollbar.js offers error tracking and logging from Javascript to Rollbar. In versions before 2.26.5 and from 3.0.0-alpha1 to before 3.0.0-beta5, there is a prototype pollution vulnerability in merge(). If application code calls rollbar.configure() with untrusted input, prototype pollution is possible. This issue has been fixed in versions 2.26.5 and 3.0.0-beta5. A workaround involves ensuring that values passed to rollbar.configure() do not contain untrusted input.	5.9	More Details
CVE-2025-60176	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tattersoftware WP Tesseract wp-tesseract allows Stored XSS.This issue affects WP Tesseract: from n/a through <= 1.0.2.	5.9	More Details
CVE-2025-53218	Insertion of Sensitive Information Into Sent Data vulnerability in Saad Iqbal AppExperts appexperts allows Retrieve Embedded Sensitive Data.This issue affects AppExperts: from n/a through <= 1.4.5.	5.8	More Details
CVE-2025-53232	Insertion of Sensitive Information Into Sent Data vulnerability in inkthemes WP Gmail SMTP wp-gmail-smtp allows Retrieve Embedded Sensitive Data.This issue affects WP Gmail SMTP: from n/a through <= 1.0.7.	5.8	More Details
CVE-2025-59578	Insertion of Sensitive Information Into Sent Data vulnerability in wpdesk ShopMagic shopmagic-for-woocommerce allows Retrieve Embedded Sensitive Data.This issue affects ShopMagic: from n/a through <= 4.5.6.	5.8	More Details
CVE-2025-62796	PrivateBin is an online pastebin where the server has zero knowledge of pasted data. Versions 1.7.7 through 2.0.1 allow persistent HTML injection via the unsanitized attachment filename (attachment_name) when attachments are enabled. An attacker can modify attachment_name before encryption so that, after decryption, arbitrary HTML is inserted unescaped into the page near the file size hint, enabling redirect (e.g., meta refresh) and site defacement and related phishing attacks. Script execution is normally blocked by the recommended Content Security Policy, limiting confidentiality impact. The issue was introduced in 1.7.7 and fixed in 2.0.2. Update to 2.0.2 or later. Workarounds include enforcing the recommended CSP, deploying PrivateBin on a separate domain, or disabling attachments.	5.8	More Details
CVE-2025-59459	An attacker that gains SSH access to an unprivileged account may be able to disrupt services (including SSH), causing persistent loss of availability.	5.5	More Details
CVE-2025-49949	Missing Authorization vulnerability in templazee Templazee templazee allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Templazee: from n/a through <= 1.0.2.	5.5	More Details
CVE-2025-23330	NVIDIA Display Driver for Linux contains a vulnerability where an attacker might be able to trigger a null pointer dereference. A successful exploit of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2025-35981	Exposure of Private Personal Information to an Unauthorized Actor (CWE-359) in the Command Centre Server allows a privileged Operator to view limited personal data about a Cardholder they would not normally have permissions to view. This issue affects Command Centre Server: 9.30.1874 (MR1), 9.20.2337 (MR3), 9.10.3194 (MR6).	5.5	More Details
CVE-2025-10651	The Welcart e-Commerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'order_mail' setting in versions up to, and including, 2.11.22. This is due to insufficient sanitization on the order_mail field and a lack of escaping on output. This makes it possible for authenticated attackers, with Editor-level permissions and above, to inject arbitrary web scripts via the General Setting page that will execute when an administrator accesses the E-mail Setting page.	5.5	More Details
CVE-2025-23300	NVIDIA Display Driver for Linux contains a vulnerability in the kernel driver, where a user could cause a null pointer dereference by allocating a specific memory resource. A successful exploit of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2025-10874	The Orbit Fox: Duplicate Page, Menu Icons, SVG Support, Cookie Notice, Custom Fonts & More WordPress plugin before 3.0.2 does not limit URLs which may be used for the stock photo import feature, allowing the user to specify arbitrary URLs. This leads to a server-side request forgery as the user may force the server to access any URL of their choosing.	5.5	More Details
CVE-2025-48430	Uncaught Exception (CWE-248) in the Command Centre Server allows an Authorized and Privileged Operator to crash the Command Centre Server at will. This issue affects Command Centre Server: 9.30 prior to vEL9.30.2482 (MR2), 9.20 prior to vEL9.20.2819 (MR4), 9.10 prior to vEL9.10.3672 (MR7), 9.00 prior to vEL9.00.3831 (MR8), all versions of 8.90 and prior.	5.5	More Details
CVE-2025-41402	Client-Side Enforcement of Server-Side Security (CWE-602) in the Command Centre Server allows a privileged operator to enter invalid competency data, bypassing expiry checks. This issue affects Command Centre Server: 9.30 prior to vEL9.30.2482 (MR2), 9.20 prior to vEL9.20.2819 (MR4), 9.10 prior to vEL9.10.3672 (MR7), all versions of 9.00 and prior.	5.5	More Details

CVE-2025-10937	Oxford Nanopore Technologies' MinKNOW software at or prior to version 24.11 creates a temporary file to store the local authentication token during startup, before copying it to its final location. This temporary file is created in a directory accessible to all users on the system. An unauthorized local user or process can exploit this behavior by placing a file lock on the temporary token file using the flock system call. This prevents MinKNOW from completing the token generation process. As a result, no valid local token is created, and the software is unable to execute commands on the sequencer. This leads to a denial-of-service (DoS) condition, blocking sequencing operations.	5.5	More Details
CVE-2025-62941	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dFactory Events Maker by dFactory events-maker allows Stored XSS.This issue affects Events Maker by dFactory: from n/a through <= 1.6.14.	5.4	More Details
CVE-2025-62940	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nick Diego Blox Lite blox-lite allows Stored XSS.This issue affects Blox Lite: from n/a through <= 1.2.8.	5.4	More Details
CVE-2025-62939	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Joe Open Currency Converter artiss-currency-converter allows Stored XSS.This issue affects Open Currency Converter: from n/a through <= 1.5.0.	5.4	More Details
CVE-2025-62937	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Johnny Post List Featured Image post-list-featured-image allows Stored XSS.This issue affects Post List Featured Image: from n/a through <= 0.5.9.	5.4	More Details
CVE-2025-49934	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrocoBlock JetBlocks For Elementor jet-blocks allows Stored XSS.This issue affects JetBlocks For Elementor: from n/a through <= 1.3.18.	5.4	More Details
CVE-2025-62917	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jamel.Z Tooltipy bluet-keywords-tooltip-generator allows Stored XSS.This issue affects Tooltipy: from n/a through <= 5.5.9.	5.4	More Details
CVE-2025-6639	The Tutor LMS Pro – eLearning and online course solution plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.8.3 due to missing validation on a user controlled key when viewing and editing assignments through the tutor_assignment_submit() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to view and edit assignment submissions of other students.	5.4	More Details
CVE-2025-62942	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tempranova WP Mapbox GL JS Maps wp-mapbox-gl-js allows Stored XSS.This issue affects WP Mapbox GL JS Maps: from n/a through <= 3.0.1.	5.4	More Details
CVE-2025-62943	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Matt McInvale Next Page, Not Next Post next-page-not-next-post allows Stored XSS.This issue affects Next Page, Not Next Post: from n/a through <= 0.3.0.	5.4	More Details
CVE-2025-10749	The Microsoft Azure Storage for WordPress plugin for WordPress is vulnerable to Unauthorized Arbitrary Media Deletion in all versions up to, and including, 4.5.1. This is due to missing capability checks on the 'azure-storage-media-replace' AJAX action. This makes it possible for authenticated attackers with subscriber-level access and above to delete arbitrary media files from the WordPress Media Library via the replace_attachment parameter granted they can access the nonce which is exposed to all authenticated users.	5.4	More Details
CVE-2025-10727	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ArkSigner Software and Hardware Inc. AcBakImzala allows Reflected XSS.This issue affects AcBakImzala: before v5.1.4.	5.4	More Details
CVE-2025-22169	Jira Align is vulnerable to an authorization issue. A low-privilege user can access unexpected endpoints that disclose a small amount of sensitive information. For example, a low-level user was able to subscribe to an item/object without having the expected permission level.	5.4	More Details
CVE-2025-62920	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webnique USERCENTRICS CMP usercentrics-consent-management-platform allows Stored XSS.This issue affects USERCENTRICS CMP: from n/a through <= 1.0.9.	5.4	More Details
CVE-2025-11429	A flaw was found in Keycloak. Keycloak does not immediately enforce the disabling of the "Remember Me" realm setting on existing user sessions. Sessions created while "Remember Me" was active retain their extended session lifetime until they expire, overriding the administrator's recent security configuration change. This is a logic flaw in session management increases the potential window for successful session hijacking or unauthorized long-term access persistence. The flaw lies in the session expiration logic relying on the session-local "remember-me" flag without validating the current realm-level configuration.	5.4	More Details
CVE-2025-62907	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in aviplugins.com Custom Post Type Attachment custom-post-type-pdf-attachment allows Stored XSS.This issue affects Custom Post Type Attachment: from n/a through <= 3.4.6.	5.4	More Details
CVE-2025-49920	Missing Authorization vulnerability in accessiBe Web Accessibility By accessiBe accessibe allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Web Accessibility By accessiBe: from n/a through <= 2.10.	5.4	More Details
CVE-2025-62912	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SiteGround SiteGround Email Marketing siteground-email-marketing allows Stored XSS.This issue affects SiteGround Email Marketing: from n/a through <= 1.7.1.	5.4	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rock Content Rock Convert		More

2025-62911	rock-convert allows Stored XSS.This issue affects Rock Convert: from n/a through <= 3.0.1.	5.4	Details
CVE-2025-62910	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in deshine Video Gallery by Huzzaz huzzaz-video-gallery allows Stored XSS.This issue affects Video Gallery by Huzzaz: from n/a through <= 10.5.	5.4	More Details
CVE-2025-62905	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Justin Tadlock Query Posts query-posts allows Stored XSS.This issue affects Query Posts: from n/a through <= 0.3.2.	5.4	More Details
CVE-2025-62904	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ben Huson WP Geo wp-geo allows Stored XSS.This issue affects WP Geo: from n/a through <= 3.5.1.	5.4	More Details
CVE-2025-62903	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPClever WPC Smart Messages for WooCommerce wpc-smart-messages allows Stored XSS.This issue affects WPC Smart Messages for WooCommerce: from n/a through <= 4.2.4.	5.4	More Details
CVE-2025-62900	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WeblineIndia Popular Posts by Webline popular-posts-by-webline allows Stored XSS.This issue affects Popular Posts by Webline: from n/a through <= 1.1.1.	5.4	More Details
CVE-2025-62899	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in THRIVE - Web Design Gold Coast Photospace Responsive photospace-responsive allows Stored XSS.This issue affects Photospace Responsive: from n/a through <= 2.2.0.	5.4	More Details
CVE-2025-62898	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Maarten Links shortcode links-shortcode allows Stored XSS.This issue affects Links shortcode: from n/a through <= 1.8.3.	5.4	More Details
CVE-2025-62894	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in magicoders ACF Recent Posts Widget acf-recent-posts-widget allows Stored XSS.This issue affects ACF Recent Posts Widget: from n/a through <= 5.9.3.	5.4	More Details
CVE-2025-36085	IBM Concert 1.0.0 through 2.0.0 Software is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	5.4	More Details
CVE-2025-62006	Missing Authorization vulnerability in VeronaLabs WP SMS wp-sms.This issue affects WP SMS: from n/a through <= 7.0.1.	5.4	More Details
CVE-2025-62887	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in KingAddons.com King Addons for Elementor king-addons allows DOM-Based XSS.This issue affects King Addons for Elementor: from n/a through <= 51.1.37.	5.4	More Details
CVE-2025-62027	Missing Authorization vulnerability in StellarWP Event Tickets event-tickets.This issue affects Event Tickets: from n/a through <= 5.26.3.	5.4	More Details
CVE-2025-62913	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpopal Opal Service opal-service allows Stored XSS.This issue affects Opal Service: from n/a through <= 1.9.1.	5.4	More Details
CVE-2025-22175	Jira Align is vulnerable to an authorization issue. A low-privilege user can access unexpected endpoints that disclose a small amount of sensitive information. For example, a low-level user was able to modify the steps of another user's private checklist.	5.4	More Details
CVE-2025-62982	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sarah Giles Dynamic User Directory dynamic-user-directory allows Stored XSS.This issue affects Dynamic User Directory: from n/a through <= 2.3.	5.4	More Details
CVE-2025-60982	IDOR vulnerability in Educare ERP 1.0 (2025-04-22) allows unauthorized access to sensitive data via manipulated object references. Affected endpoints do not enforce proper authorization checks, allowing authenticated users to access or modify data belonging to other users by changing object identifiers in API requests. Attackers can exploit this flaw to view or modify sensitive records without proper authorization.	5.4	More Details
CVE-2025-62398	A serious authentication flaw allowed attackers with valid credentials to bypass multi-factor authentication under certain conditions, potentially compromising user accounts.	5.4	More Details
CVE-2025-62401	An issue in Moodle’s timed assignment feature allowed students to bypass the time restriction, potentially giving them more time than allowed to complete an assessment.	5.4	More Details
CVE-2025-62798	Sharp is a content management framework built for Laravel as a package. Prior to 9.11.1, a Cross-Site Scripting (XSS) vulnerability was discovered in code16/sharp when rendering content using the SharpShowTextField component. In affected versions, expressions wrapped in {{ & }} were evaluated by Vue. This allowed attackers to inject arbitrary JavaScript or HTML that executes in the browser when the field is displayed. The issue has been fixed in v9.11.1 .	5.4	More Details
CVE-2025-	Multiple CSRF attack vectors in JDownloads component 1.0.0-4.0.47 for Joomla were discovered.	5.4	More Details

55758			
CVE-2025-36121	IBM OpenPages 9.1 and 9.0 is vulnerable to HTML injection. A remotely authenticated 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-2025-11154	The IDonate WordPress plugin before 2.1.13 does not have authorisation and CSRF when deleting users via an action handler, allowing unauthenticated attackers to delete arbitrary users.	5.4	More Details
CVE-2025-12110	A flaw was found in Keycloak. An offline session continues to be valid when the offline_access scope is removed from the client. The refresh token is accepted and you can continue to request new tokens for the session. As it can lead to a situation where an administrator removes the scope, and assumes that offline sessions are no longer available, but they are.	5.4	More Details
CVE-2025-24934	Software which sets SO_REUSEPORT_LB on a socket and then connects it to a host will not directly observe any problems. However, due to its membership in a load-balancing group, that socket will receive packets originating from any host. This breaks the contract of the connect(2) and implied connect via sendto(2), and may leave the application vulnerable to spoofing attacks. The kernel failed to check the connection state of sockets when adding them to load-balancing groups. Furthermore, when looking up the destination socket for an incoming packet, the kernel will match a socket belonging to a load-balancing group even if it is connected, in violation of the contract that connected sockets are only supposed to receive packets originating from the connected host.	5.4	More Details
CVE-2025-62048	Missing Authorization vulnerability in WPMU DEV - Your All-in-One WordPress Platform SmartCrawl smartcrawl-seo.This issue affects SmartCrawl: from n/a through <= 3.14.3.	5.4	More Details
CVE-2025-60983	Reflected Cross Site Scripting vulnerability in Rubikon Banking Solution 4.0.3 in the "Search For Customers Information" endpoints.	5.4	More Details
CVE-2025-62966	Missing Authorization vulnerability in Apiki GoCache gocache-cdn allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects GoCache: from n/a through <= 1.3.6.	5.4	More Details
CVE-2025-61080	A reflected Cross-Site Scripting (XSS) vulnerability has been identified in Clear2Pay Bank Visibility Application - Payment Execution 1.10.0.104 via the ID parameter in the URL.	5.4	More Details
CVE-2025-56009	Cross site request forgery (CSRF) vulnerability in KeeneticOS before 4.3 at "/rci" API endpoint allows attackers to take over the device via adding additional users with full permissions by managing the victim to open page with exploit.	5.3	More Details
CVE-2025-49903	Missing Authorization vulnerability in bdthemes ZoloBlocks zoloblocks allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ZoloBlocks: from n/a through <= 2.3.11.	5.3	More Details
CVE-2025-62884	Missing Authorization vulnerability in Elliot Sowersby / RelyWP Coupon Affiliates woo-coupon-usage allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Coupon Affiliates: from n/a through <= 7.0.3.	5.3	More Details
CVE-2025-49899	Missing Authorization vulnerability in jjlemstra Whydonate wp-whydonate allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Whydonate: from n/a through <= 4.0.15.	5.3	More Details
CVE-2023-37749	Incorrect access control in the REST API endpoint of HubSpot v1.29441 allows unauthenticated attackers to view users' data without proper authorization.	5.3	More Details
CVE-2025-49380	Deserialization of Untrusted Data vulnerability in wpinstinct WooCommerce Vehicle Parts Finder woo-vehicle-parts-finder allows Object Injection.This issue affects WooCommerce Vehicle Parts Finder: from n/a through <= 3.7.	5.3	More Details
CVE-2025-62897	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Brecht WP Recipe Maker wp-recipe-maker allows Code Injection.This issue affects WP Recipe Maker: from n/a through <= 10.1.1.	5.3	More Details
CVE-2025-49374	Server-Side Request Forgery (SSRF) vulnerability in captcha.eu Captcha.eu captcha-eu allows Server Side Request Forgery.This issue affects Captcha.eu: from n/a through <= 1.0.61.	5.3	More Details
CVE-2025-61795	Improper Resource Shutdown or Release vulnerability in Apache Tomcat. If an error occurred (including exceeding limits) during the processing of a multipart upload, temporary copies of the uploaded parts written to disc were not cleaned up immediately but left for the garbage collection process to delete. Depending on JVM settings, application memory usage and application load, it was possible that space for the temporary copies of uploaded parts would be filled faster than GC cleared it, leading to a DoS. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.11, from 10.1.0-M1 through 10.1.46, from 9.0.0.M1 through 9.0.109. The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected. Users are recommended to upgrade to version 11.0.12 or later, 10.1.47 or later or 9.0.110 or later which fixes the issue.	5.3	More Details
CVE-2025-12134	The ZoloBlocks – Gutenberg Block Editor Plugin with Advanced Blocks, Dynamic Content, Templates & Patterns plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the update_popup_status() function in all versions up to, and including, 2.3.11. This makes it possible for unauthenticated attackers to enable/disable	5.3	More Details

	popups.		
CVE-2025-60134	Cross-Site Request Forgery (CSRF) vulnerability in John James Jacoby WP Media Categories wp-media-categories allows Cross Site Request Forgery.This issue affects WP Media Categories: from n/a through <= 2.1.0.	5.3	More Details
CVE-2025-46583	There is a Denial of Service (DoS) vulnerability in the ZTE MC889A Pro product. Due to insufficient validation of the input parameters of the Short Message Service interface, allowing an attacker to exploit it to carry out a DoS attack.	5.3	More Details
CVE-2025-10705	The MxChat – AI Chatbot for WordPress plugin for WordPress is vulnerable to Blind Server-Side Request Forgery in all versions up to, and including, 2.4.6. This is due to insufficient validation of user-supplied URLs in the PDF processing functionality. This makes it possible for unauthenticated attackers to make the WordPress server perform HTTP requests to arbitrary destinations via the mxchat_handle_chat_request AJAX action.	5.3	More Details
CVE-2021-43768	In Malwarebytes For Teams v.1.0.990 and before and fixed in v.1.0.1003 and later a privilege escalation can occur via the COM interface running in mbamservice.exe.	5.3	More Details
CVE-2025-12245	A vulnerability was identified in chatwoot up to 4.7.0. This vulnerability affects the function initPostMessageCommunication of the file app/javascript/sdk/IFrameHelper.js of the component Widget. The manipulation of the argument baseUrl leads to origin validation error. Remote exploitation of the attack is possible. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-12205	A vulnerability was detected in Kamailio 5.5. The affected element is the function sr_push_yy_state of the file src/core/cfg.lex of the component Configuration File Handler. The manipulation results in use after free. The attack must be initiated from a local position. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-12204	A security vulnerability has been detected in Kamailio 5.5. Impacted is the function rve_destroy of the file src/core/rvalue.c of the component Configuration File Handler. The 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 vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-62236	The Frontier Airlines website has a publicly available endpoint that validates if an email addresses is associated with an account. An unauthenticated, remote attacker could determine valid email addresses, possibly aiding in further attacks.	5.3	More Details
CVE-2025-49906	Missing Authorization vulnerability in StellarWP WPComplete wpcomplete allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WPComplete: from n/a through <= 2.9.5.3.	5.3	More Details
CVE-2025-36081	IBM Concert Software 1.0.0 through 2.0.0 could allow a user to modify system logs due to improper neutralization of log input.	5.3	More Details
CVE-2025-62979	Insertion of Sensitive Information Into Sent Data vulnerability in airesvsg ACF to REST API acf-to-rest-api allows Retrieve Embedded Sensitive Data.This issue affects ACF to REST API: from n/a through <= 3.3.4.	5.3	More Details
CVE-2025-62977	Missing Authorization vulnerability in 沃之涛 百度站长SEO合集(支持百度/神马/Bing/头条推送) baiduseo allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects 百度站长SEO合集(支持百度/神马/Bing/头条推送): from n/a through <= 2.1.3.	5.3	More Details
CVE-2025-62976	Missing Authorization vulnerability in Joovii Sendle Shipping official-sendle-shipping-method allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Sendle Shipping: from n/a through <= 6.02.	5.3	More Details
CVE-2025-62973	Missing Authorization vulnerability in Themekraft BuddyForms buddyforms allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects BuddyForms: from n/a through <= 2.9.0.	5.3	More Details
CVE-2025-62970	Missing Authorization vulnerability in Spencer Haws Link Whisper Free link-whisper allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Link Whisper Free: from n/a through <= 0.8.8.	5.3	More Details
CVE-2025-49913	Missing Authorization vulnerability in CoSchedule CoSchedule coschedule-by-todaymade allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects CoSchedule: from n/a through <= 3.4.0.	5.3	More Details
CVE-2025-62524	PILOS (Platform for Interactive Live-Online Seminars) is a frontend for BigBlueButton. PILOS before 4.8.0 exposes the PHP version via the X-Powered-By header, enabling attackers to fingerprint the server and assess potential exploits. This information disclosure vulnerability originates from PHP's base image. Additionally, the PHP version can also be inferred through the PILOS version displayed in the footer and by examining the source code available on GitHub. This information disclosure vulnerability has been patched in PILOS in v4.8.0.	5.3	More Details
CVE-2025-10638	The NS Maintenance Mode for WP WordPress plugin through 1.3.1 lacks authorization in its subscriber export function allowing unauthenticated attackers to download a list of a site's subscribers containing their name and email address	5.3	More Details
CVE-2025-	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check while verifying webhook signatures on the "verifyAndCreateOrderData" function in all versions	5.3	More

11564	up to, and including, 3.8.3. This makes it possible for unauthenticated attackers to bypass payment verification and mark orders as paid by submitting forged webhook requests with `payment_type` set to 'recurring'.		Details
CVE-2025-62607	Nautobot Single Source of Truth (SSoT) is an app for Nautobot. Prior to version 3.10.0, an unauthenticated attacker could access this page to view the Service Now public instance name e.g. companyname.service-now.com. This is considered low-value information. This does not expose the Secret, the Secret Name, or the Secret Value for the Username/Password for Service-Now.com. An unauthenticated member would not be able to change the instance name, nor set a Secret. There is not a way to gain access to other pages Nautobot through the unauthenticated Configuration page. This issue has been patched in version 3.10.0.	5.3	More Details
CVE-2025-10637	The Social Feed Gallery plugin for WordPress is vulnerable to Information Exposure in versions less than, or equal to, 4.9.2. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to exfiltrate Instagram profile and media data from any account the site owner connected to their site.	5.3	More Details
CVE-2025-62396	An error-handling issue in the Moodle router (r.php) could cause the application to display internal directory listings when specific HTTP headers were not properly configured.	5.3	More Details
CVE-2025-12310	A security vulnerability has been detected in VirtFusion up to 6.0.2. This vulnerability affects unknown code of the file /account/_settings of the component Email Change Handler. The manipulation leads to improper restriction of excessive authentication attempts. 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.	5.3	More Details
CVE-2025-62397	The router’s inconsistent response to invalid course IDs allowed attackers to infer which course IDs exist, potentially aiding reconnaissance.	5.3	More Details
CVE-2025-60729	PerfreeBlog v4.0.11 has an arbitrary file read vulnerability in the validThemeFilePath function	5.3	More Details
CVE-2025-62062	Insertion of Sensitive Information Into Sent Data vulnerability in ThemeRuby Easy Post Submission easy-post-submission allows Retrieve Embedded Sensitive Data.This issue affects Easy Post Submission: from n/a through <= 1.7.0.	5.3	More Details
CVE-2025-11269	The Product Filter by WBW plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'approveNotice' action in all versions up to, and including, 3.0.0. This makes it possible for unauthenticated attackers to update the plugin's settings.	5.3	More Details
CVE-2025-10694	The User Feedback – Create Interactive Feedback Form, User Surveys, and Polls in Seconds plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the `maybe_load_onboarding_wizard` function in all versions up to, and including, 1.8.0. This makes it possible for unauthenticated attackers to access the onboarding wizard page and view configuration information including the administrator email address.	5.3	More Details
CVE-2025-10579	The BackWPup – WordPress Backup & Restore Plugin plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'backwpup_working' AJAX action in all versions up to, and including, 5.5.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve access to a back-up's filename while a backup is running. This information has little value on it's own, but could be used to aid in a brute force attack to retrieve back-up contents in limited environments (i.e. NGINX).	5.3	More Details
CVE-2025-11760	The eRoom – Webinar & Meeting Plugin for Zoom, Google Meet, Microsoft Teams plugin for WordPress is vulnerable to exposure of sensitive information in all versions up to, and including, 1.5.6. This is due to the plugin exposing Zoom SDK secret keys in client-side JavaScript within the meeting view template. This makes it possible for unauthenticated attackers to extract the sdk_secret value, which should remain server-side, compromising the security of the Zoom integration and allowing attackers to generate valid JWT signatures for unauthorized meeting access.	5.3	More Details
CVE-2025-58712	A container privilege escalation flaw was found in certain AMQ Broker images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.	5.2	More Details
CVE-2025-57848	A container privilege escalation flaw was found in certain Container-native Virtualization images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.	5.2	More Details
CVE-2025-62783	InventoryGui is a library for creating chest GUIs for Bukkit/Spigot plugins. Versions 1.6.1-SNAPSHOT and earlier contain a vulnerability where any plugin using the `GuiStorageElement can allow item duplication when the experimental Bundle item feature is enabled on the server. The vulnerability is resolved in version 1.6.2-SNAPSHOT.	5.0	More Details
CVE-2025-23332	NVIDIA Display Driver for Linux contains a vulnerability in a kernel module, where an attacker might be able to trigger a null pointer deference. A successful exploit of this vulnerability might lead to denial of service.	5.0	More Details
CVE-2025-62781	PILOS (Platform for Interactive Live-Online Seminars) is a frontend for BigBlueButton. Prior to 4.8.0, users with a local account can change their password while logged in. When doing so, all other active sessions are terminated, except for the currently active one. However, the current session’s token remains valid and is not refreshed. If an attacker has previously obtained this session token through another vulnerability, changing the password will not invalidate their access. As a result, the attacker can continue to act as the user even after the password has been changed. This vulnerability is fixed in 4.8.0.	5.0	More Details

CVE-2025-59575	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Stylemix MasterStudy LMS masterstudy-lms-learning-management-system allows Retrieve Embedded Sensitive Data.This issue affects MasterStudy LMS: from n/a through <= 3.6.20.	5.0	More Details
CVE-2025-12103	A flaw was found in Red Hat Openshift AI Service. The TrustyAI component is granting all service accounts and users on a cluster permissions to get, list, watch any pod in any namespace on the cluster. TrustyAI is creating a role `trustyai-service-operator-lmeval-user-role` and a CRB `trustyai-service-operator-default-lmeval-user-rolebinding` which is being applied to `system:authenticated` making it so that every single user or service account can get a list of pods running in any namespace on the cluster Additionally users can access all `persistentvolumeclaims` and `lmevaljobs`	5.0	More Details
CVE-2025-11128	The RSS Aggregator by Feedzy – Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.1.0 via the 'feedzy_sanitize_feeds' function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query information from internal services.	5.0	More Details
CVE-2025-10047	The Email Tracker – Email Log, Email Open Tracking, Email Analytics & Email Management for WordPress Emails plugin for WordPress is vulnerable to SQL Injection via the 'orderby' parameter in all versions up to, and including, 5.3.12 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-2025-62988	Server-Side Request Forgery (SSRF) vulnerability in Codeless Slider Templates slider-templates allows Server Side Request Forgery.This issue affects Slider Templates: from n/a through <= 1.0.3.	4.9	More Details
CVE-2025-62820	Slack Nebula before 1.9.7 mishandles CIDR in some configurations and thus accepts arbitrary source IP addresses within the Nebula network.	4.9	More Details
CVE-2025-62705	OpenBao is an open source identity-based secrets management system. Prior to version 2.4.2, OpenBao's audit log did not appropriately redact fields when relevant subsystems sent []byte response parameters rather than strings. This includes, but is not limited to sys/raw with use of encoding=base64, all data would be emitted unredacted to the audit log, and Transit, when performing a signing operation with a derived Ed25519 key, would emit public keys to the audit log. This issue has been patched in OpenBao 2.4.2.	4.9	More Details
CVE-2025-62367	Taiga is an open source project management platform. In versions 6.8.3 and earlier, Taiga API is vulnerable to time-based blind SQL injection allowing sensitive data disclosure via response timing. This issue is fixed in version 6.9.0.	4.8	More Details
CVE-2025-12287	A security vulnerability has been detected in Bdtask Wholesale Inventory Control and Inventory Management System up to 20251013. This impacts an unknown function of the file /Admin_dashboard/edit_profile. Such manipulation of the argument first_name/last_name leads to sql injection. The attack may be launched 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.	4.7	More Details
CVE-2025-62981	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CRM Perks WP Gravity Forms Zoho CRM and Bigin gf-zoho allows Phishing.This issue affects WP Gravity Forms Zoho CRM and Bigin: from n/a through <= 1.2.8.	4.7	More Details
CVE-2025-12331	A weakness has been identified in Willow CMS up to 1.4.0. Impacted is an unknown function of the file /admin/images/add. This manipulation causes unrestricted upload. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	4.7	More Details
CVE-2025-48099	Cross-Site Request Forgery (CSRF) vulnerability in Code Amp Search & Filter search-filter allows Cross Site Request Forgery.This issue affects Search & Filter: from n/a through <= 1.2.17.	4.7	More Details
CVE-2025-62594	ImageMagick is a software suite to create, edit, compose, or convert bitmap images. ImageMagick versions prior to 7.1.2-8 are vulnerable to denial-of-service due to unsigned integer underflow and division-by-zero in the CLAHEImage function. When tile width or height is zero, unsigned underflow occurs in pointer arithmetic, leading to out-of-bounds memory access, and division-by-zero causes immediate crashes. This issue has been patched in version 7.1.2-8.	4.7	More Details
CVE-2025-12201	A vulnerability was identified in ajayrandhawa User-Management-PHP-MYSQL up to fedcf58797bf2791591606f7b61fdad99ad8bff1. This affects an unknown part of the file /admin/edit-user.php of the component User Management Interface. Such manipulation of the argument image leads to unrestricted upload. It is possible to launch the attack remotely. The exploit is publicly available and might be used. 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.	4.7	More Details
CVE-2025-60151	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CRM Perks WP Gravity Forms HubSpot gf-hubspot allows Phishing.This issue affects WP Gravity Forms HubSpot: from n/a through <= 1.2.5.	4.7	More Details
CVE-2025-12294	A security flaw has been discovered in SourceCodester Point of Sales 1.0. Impacted is an unknown function of the file /delete_category.php. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	4.7	More Details
CVE-2025-12250	A flaw has been found in OpenWGA 7.11.12 Build 737. This affects an unknown function of the file WGA.File of the component TMLScript API. Executing manipulation can lead to path traversal. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-	A vulnerability was found in ashymuzuro Full-Ecommece-Website and Muzuro Ecommerce System up to 1.1.0. This affects an		

2025-12291	unknown part of the file /admin/index.php?add_product of the component Add Product Page. The manipulation results in unrestricted upload. The attack may be performed from remote. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-12315	A vulnerability was determined in code-projects Food Ordering System 1.0. This affects an unknown function of the file /admin/menu.php. Executing manipulation of the argument itemPrice can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2025-12226	A vulnerability was found in SourceCodester Best House Rental Management System 1.0. Impacted is the function save_house of the file /admin_class.php. Performing manipulation of the argument house_no results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	4.7	More Details
CVE-2025-12296	A security vulnerability has been detected in D-Link DAP-2695 2.00RC13. The impacted element is the function sub_4174B0 of the component Firmware Update Handler. The manipulation leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	4.7	More Details
CVE-2025-12314	A vulnerability was found in code-projects Food Ordering System 1.0. The impacted element is an unknown function of the file /admin/deleteitem.php. Performing manipulation of the argument itemID results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	4.7	More Details
CVE-2025-12016	The qnotsquiz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'qnotsquiz_custom_start_text' parameter in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with 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-2025-23345	NVIDIA Display Driver for Windows and Linux contains a vulnerability in a video decoder, where an attacker might cause an out-of-bounds read. A successful exploit of this vulnerability might lead to information disclosure or denial of service.	4.4	More Details
CVE-2025-46602	Dell SupportAssist OS Recovery, versions prior to 5.5.15.0, contain an Insertion of Sensitive Information into Externally-Accessible File or Directory vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure.	4.4	More Details
CVE-2025-49917	Server-Side Request Forgery (SSRF) vulnerability in Icegram Icegram Express Pro email-subscribers-premium allows Server Side Request Forgery.This issue affects Icegram Express Pro: from n/a through <= 5.9.5.	4.4	More Details
CVE-2025-60131	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zoefff Werk aan de Muur werk-aan-de-muur allows Stored XSS.This issue affects Werk aan de Muur: from n/a through <= 1.5.	4.4	More Details
CVE-2025-12033	The Simple Banner – Easily add multiple Banners/Bars/Notifications/Announcements to the top or bottom of your website plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pro_version_activation_code' parameter in all versions up to, and including, 3.0.10 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-2025-12034	The Fast Velocity Minify plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.5.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-11172	The Check Plagiarism plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the chk_plag_mine_plugin_wpse10500_admin_action() function in all versions up to, and including, 2.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the API key.	4.3	More Details
CVE-2025-5605	An authentication bypass vulnerability exists in the Management Console of multiple WSO2 products. A malicious actor with access to the console can manipulate the request URI to bypass authentication and access certain restricted resources, resulting in partial information disclosure. The known exposure from this issue is limited to memory statistics. While the vulnerability does not allow full account compromise, it still enables unauthorized access to internal system details.	4.3	More Details
CVE-2025-12246	A security flaw has been discovered in chatwoot up to 4.7.0. This issue affects some unknown processing of the file app/javascript/shared/components/IframeLoader.vue of the component Admin Interface. The manipulation of the argument Link results in cross site scripting. The attack can be executed remotely. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-62723	FlashMQ is a MQTT broker/server, designed for multi-CPU environments. Prior to version 1.23.2, any authenticated user can create sessions and have them collect QoS messages. When not sent to a client, these are then not released upon (eventual) session expiration. Version 1.23.2 fixes the issue.	4.3	More Details
CVE-2025-62972	Missing Authorization vulnerability in WPWebinarSystem WebinarPress wp-webinarsystem allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WebinarPress: from n/a through <= 1.33.28.	4.3	More Details
CVE-2025-22178	Jira Align is vulnerable to an authorization issue. A low-privilege user can access unexpected endpoints that disclose a small amount of sensitive information. For example, a low-level user was able to view items on the "Why" page.	4.3	More Details
CVE-2025-	A flaw was found in the course overview output function where user access permissions were not fully enforced. This could allow unauthorized users to view information about courses they should not have access to, potentially exposing limited course	4.3	More

62393	details.		Details
CVE-2025-62802	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to 10.1.1, the out-of-box experience for HTML editing allows unauthenticated users to upload files. This opens a potential vector to other security issues and is not needed on most implementations. This vulnerability is fixed in 10.1.1.	4.3	More Details
CVE-2025-10902	The Originality.ai AI Checker plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'ai_scan_result_remove' function in all versions up to, and including, 1.0.12. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete all data in the wp_originalityai_log database table, which can include post titles, scan scores, credits used, and other data.	4.3	More Details
CVE-2025-12072	The Disable Content Editor For Specific Template plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0. This is due to missing nonce validation on template configuration updates. This makes it possible for unauthenticated attackers to add or delete template configurations via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-22176	Jira Align is vulnerable to an authorization issue. A low-privilege user can access unexpected endpoints that disclose a small amount of sensitive information. For example, a low-level user was able to view audit log items.	4.3	More Details
CVE-2025-22177	Jira Align is vulnerable to an authorization issue. A low-privilege user can access unexpected endpoints that disclose a small amount of sensitive information. For example, a low-level user was able to view other team overviews.	4.3	More Details
CVE-2025-41720	A low privileged remote attacker can upload arbitrary data masked as a png file to the affected device using the webserver API because only the file extension is verified.	4.3	More Details
CVE-2025-12298	A vulnerability was identified in code-projects Simple Food Ordering System 1.0. This affects an unknown part of the file /editcategory.php. The manipulation of the argument pname leads to cross site scripting. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	4.3	More Details
CVE-2025-62400	Moodle exposed the names of hidden groups to users who had permission to create calendar events but not to view hidden groups. This could reveal private or restricted group information.	4.3	More Details
CVE-2025-62975	Cross-Site Request Forgery (CSRF) vulnerability in raychat Raychat raychat allows Cross Site Request Forgery.This issue affects Raychat: from n/a through <= 2.2.1.	4.3	More Details
CVE-2025-62978	Missing Authorization vulnerability in Kiotviet KiotViet Sync kiotvietsync allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects KiotViet Sync: from n/a through <= 1.8.5.	4.3	More Details
CVE-2025-12290	A vulnerability has been found in Sui Shang Information Technology Suishang Enterprise-Level B2B2C Multi-User Mall System 1.0. Affected by this issue is some unknown functionality of the file /i/359. The manipulation of the argument keywords leads to cross site scripting. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-11257	The LLM Hubspot Blog Import plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'process_save_blogs' AJAX endpoint in all versions up to, and including, 1.0.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to trigger an import of all Hubspot data.	4.3	More Details
CVE-2025-12276	A vulnerability was detected in LearnHouse up to 98dfad76aad70711a8113f6c1fdabfccf10509ca. Affected by this issue is some unknown functionality of the component Image Handler. The manipulation results in information disclosure. The attack can be executed remotely. The exploit is now public and may be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-58918	Cross-Site Request Forgery (CSRF) vulnerability in Waituk Entrada theme allows Cross Site Request Forgery.This issue affects Entrada: from n/a through 5.7.7.	4.3	More Details
CVE-2025-54966	An issue was discovered in BAE SOCET GXP before 4.6.0.2. Some endpoints on the SOCET GXP Job Status Service may return sensitive information in certain situations, including local file paths and SOCET GXP version information.	4.3	More Details
CVE-2025-49373	Cross-Site Request Forgery (CSRF) vulnerability in Evergreen Content Poster Evergreen Content Poster evergreen-content-poster allows Cross Site Request Forgery.This issue affects Evergreen Content Poster: from n/a through <= 1.4.5.	4.3	More Details
CVE-2025-12297	A vulnerability was detected in atjiu pybbs up to 6.0.0. This affects an unknown function of the file UserApiController.java. The manipulation results in information disclosure. The attack may be launched remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2025-12300	A weakness has been identified in code-projects Simple Food Ordering System 1.0. This issue affects some unknown processing of the file /addcategory.php. This manipulation of the argument cname causes cross site scripting. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	4.3	More Details
CVE-2025-62395	A flaw in the cohort search web service allowed users with permissions in lower contexts to access cohort information from the system context, revealing restricted administrative data.	4.3	More Details

CVE-2025-11887	The Supervisor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several AJAX functions in all versions up to, and including, 1.3.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update various plugin settings.	4.3	More Details
CVE-2025-12302	A vulnerability was detected in code-projects Simple Food Ordering System 1.0. The affected element is an unknown function of the file /editproduct.php. Performing manipulation of the argument pname/category/price results in cross site scripting. The attack may be initiated remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2025-62394	Moodle failed to verify enrolment status correctly when sending quiz notifications. As a result, suspended or inactive users might receive quiz-related messages, leaking limited course information.	4.3	More Details
CVE-2025-12289	A flaw has been found in Sui Shang Information Technology Suishang Enterprise-Level B2B2C Multi-User Mall System 1.0. Affected by this vulnerability is an unknown functionality of the file /Point/index/activity_state/1/category_id/1001. Executing manipulation of the argument category_id can lead to cross site scripting. The attack can be executed 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.	4.3	More Details
CVE-2025-12014	The NGINX Cache Optimizer plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'nginxcacheoptimizer-blacklist-update' AJAX action in all versions up to, and including, 1.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to add URLs to the Exclude URLs From Dynamic Caching setting.	4.3	More Details
CVE-2025-12299	A security flaw has been discovered in code-projects Simple Food Ordering System 1.0. This vulnerability affects unknown code of the file /addproduct.php. The manipulation of the argument pname/category/price results in cross site scripting. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	4.3	More Details
CVE-2025-10570	The Flexible Refund and Return Order for WooCommerce plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.0.38 via the save_refund_request() function. This makes it possible for authenticated attackers, with subscriber-level access and above, to submit refund requests for arbitrary orders that they do not own.	4.3	More Details
CVE-2025-49907	Missing Authorization vulnerability in RealMag777 MDTF wp-meta-data-filter-and-taxonomy-filter allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MDTF: from n/a through <= 1.3.3.9.	4.3	More Details
CVE-2025-12244	A vulnerability was determined in code-projects Simple E-Banking System 1.0. This affects an unknown part of the file /eBank/register.php. Executing manipulation of the argument Username can lead to cross site scripting. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	4.3	More Details
CVE-2025-11976	The FuseWP – WordPress User Sync to Email List & Marketing Automation (Mailchimp, Constant Contact, ActiveCampaign etc.) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.23.0. This is due to missing or incorrect nonce validation on the save_changes function. This makes it possible for unauthenticated attackers to add or edit sync rules via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-6680	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.8.3. This makes it possible for authenticated attackers, with tutor-level access and above, to view assignments for courses they don't teach which may contain sensitive information.	4.3	More Details
CVE-2025-22170	Jira Align is vulnerable to an authorization issue. A low-privilege user without sufficient privileges to perform an action could if they included a particular state-related parameter of a user with sufficient privileges to perform the action.	4.3	More Details
CVE-2025-22168	Jira Align is vulnerable to an authorization issue. A low-privilege user can access unexpected endpoints that disclose a small amount of sensitive information. For example, a low-level user was able to read the steps of another user's private checklist.	4.3	More Details
CVE-2025-12202	A security flaw has been discovered in ajayrandhawa User-Management-PHP-MYSQL web up to fedcf58797bf2791591606f7b61fdad99ad8bff1. This vulnerability affects unknown code. Performing manipulation results in cross-site request forgery. The attack can be initiated remotely. The exploit has been released to the public and may be exploited. 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.	4.3	More Details
CVE-2025-11255	The Password Policy Manager | Password Manager plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'moppm_ajax' AJAX endpoint in all versions up to, and including, 2.0.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to log out the site's connection to miniorange.	4.3	More Details
CVE-2025-11497	The Advanced Database Cleaner plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.1.6. This is due to missing or incorrect nonce validation on the aDBc_prepare_elements_to_clean() function. This makes it possible for unauthenticated attackers to alter the keep last setting via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-62026	Insertion of Sensitive Information Into Sent Data vulnerability in Blockspare Blockspare blockspare allows Retrieve Embedded Sensitive Data.This issue affects Blockspare: from n/a through <= 3.2.13.2.	4.3	More Details
CVE-2025-60132	Cross-Site Request Forgery (CSRF) vulnerability in johnh10 Video Blogster Lite video-blogster-lite allows Stored XSS.This issue affects Video Blogster Lite: from n/a through <= 1.2.	4.3	More Details
CVE-2025-	Missing Authorization vulnerability in Sovlix MeetingHub meetinghub.This issue affects MeetingHub: from n/a through <= 1.23.9.	4.3	More Details

62073			
CVE-2025-62072	Missing Authorization vulnerability in Rustaurius Front End Users front-end-only-users.This issue affects Front End Users: from n/a through <= 3.2.33.	4.3	More Details
CVE-2025-12335	A vulnerability was determined in code-projects E-Commerce Website 1.0. Affected by this vulnerability is an unknown functionality of the file /pages/supplier_update.php. This manipulation of the argument supp_name/supp_address causes cross site scripting. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	4.3	More Details
CVE-2025-62071	Missing Authorization vulnerability in Repuso Social proof testimonials and reviews by Repuso social-testimonials-and-reviews-widget.This issue affects Social proof testimonials and reviews by Repuso: from n/a through <= 5.29.	4.3	More Details
CVE-2025-62070	Missing Authorization vulnerability in WPXPO WowRevenue revenue.This issue affects WowRevenue: from n/a through <= 1.2.13.	4.3	More Details
CVE-2025-59463	An attacker may cause chunk-size mismatches that block file transfers and prevent subsequent transfers.	4.3	More Details
CVE-2025-12334	A vulnerability was found in code-projects E-Commerce Website 1.0. Affected is an unknown function of the file /pages/product_add.php. The manipulation of the argument prod_name/prod_desc/prod_cost results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used.	4.3	More Details
CVE-2025-62009	Cross-Site Request Forgery (CSRF) vulnerability in Dmitry V. (CEO of "UKR Solution") UPC/EAN/GTIN Code Generator upc-ean-barcode-generator allows Cross Site Request Forgery.This issue affects UPC/EAN/GTIN Code Generator: from n/a through <= 2.0.2.	4.3	More Details
CVE-2025-62013	Missing Authorization vulnerability in POSIMYTH UiChemy uichemy.This issue affects UiChemy: from n/a through <= 4.0.0.	4.3	More Details
CVE-2025-62021	Missing Authorization vulnerability in Made Neat Acknowledgify acknowledgify.This issue affects Acknowledgify: from n/a through <= 1.1.3.	4.3	More Details
CVE-2025-62883	Missing Authorization vulnerability in Premmerce Premmerce User Roles premmerce-user-roles allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Premmerce User Roles: from n/a through <= 1.0.13.	4.3	More Details
CVE-2025-62882	Missing Authorization vulnerability in Craig Hewitt Seriously Simple Podcasting seriously-simple-podcasting allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Seriously Simple Podcasting: from n/a through <= 3.13.0.	4.3	More Details
CVE-2025-22171	Jira Align is vulnerable to an authorization issue. A low-privilege user is able to alter the private checklists of other users.	4.3	More Details
CVE-2025-62881	Missing Authorization vulnerability in WP Lab WP-Lister Lite for eBay wp-lister-for-ebay allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP-Lister Lite for eBay: from n/a through <= 3.8.3.	4.3	More Details
CVE-2025-12005	The WP VR – 360 Panorama and Free Virtual Tour Builder For WordPress plugin for WordPress is vulnerable to unauthorized access of data in all versions up to, and including, 8.5.41. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor level access and above, to modify sensitive plugin options.	4.3	More Details
CVE-2025-49937	Missing Authorization vulnerability in Syed Balkhi Smash Balloon Social Post Feed custom-facebook-feed allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Smash Balloon Social Post Feed: from n/a through <= 4.3.2.	4.3	More Details
CVE-2025-49922	Missing Authorization vulnerability in etruel WPeMatico RSS Feed Fetcher wpematico allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPeMatico RSS Feed Fetcher: from n/a through <= 2.8.3.	4.3	More Details
CVE-2025-12304	A vulnerability has been found in dulaiduwang003 TIME-SEA-PLUS up to fb299162f18498dd9cf17da906886d80a077d53b. This affects the function alipayIsSucceed of the file PayController.java of the component Order Status Handler. The manipulation leads to improper authorization. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-12288	A vulnerability was detected in Bdtask Pharmacy Management System up to 9.4. Affected is an unknown function of the file /user/edit_user/ of the component User Profile Handler. Performing manipulation results in authorization bypass. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-10901	The Originality.ai AI Checker plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'ai_get_table' function in all versions up to, and including, 1.0.12. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read all data in the wp_originalityai_log database table, which can include post titles, scan scores, credits used, and other data.	4.3	More Details
CVE-	Jira Align is vulnerable to an authorization issue. A low-privilege user can access unexpected endpoints that disclose a small		

2025-22172	amount of sensitive information. For example, a low-level user was able to read external reports without the required permission.	4.3	More Details
CVE-2025-62061	Cross-Site Request Forgery (CSRF) vulnerability in impleCode Product Catalog Simple post-type-x.This issue affects Product Catalog Simple: from n/a through <= 1.8.4.	4.3	More Details
CVE-2025-10588	The PixelYourSite – Your smart PIXEL (TAG) & API Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 11.1.2. This is due to missing or incorrect nonce validation on the adminEnableGdprAjax() function. This makes it possible for unauthenticated attackers to modify GDPR settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-12267	A flaw has been found in abhicodebox ModernShop 20250922. This issue affects some unknown processing of the file /search. Executing manipulation of the argument q can lead to cross site scripting. The attack may be performed from remote. The exploit has been published and may be used.	4.3	More Details
CVE-2025-22174	Jira Align is vulnerable to an authorization issue. A low-privilege user can access unexpected endpoints that disclose a small amount of sensitive information. For example, a low-level user was able to view portfolio rooms without the required permission.	4.3	More Details
CVE-2025-11576	The AI Chatbot Free Models – Customer Support, Live Chat, Virtual Assistant plugin for WordPress is vulnerable to CSV Injection in all versions up to, and including, 1.6.5. This is due to insufficient sanitization in the 'newcodebyte_chatbot_export_messages' function. This makes it possible for unauthenticated attackers to embed untrusted input into exported CSV files, which can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration.	4.3	More Details
CVE-2025-12270	A vulnerability was determined in LearnHouse up to 98dfad76aad70711a8113f6c1fdabfccf10509ca. The impacted element is an unknown function of the file /api/v1/assignments/{assignment_id}/tasks/{task_id}/sub_file of the component Student Assignment Submission Handler. This manipulation causes improper control of resource identifiers. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. 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.	4.3	More Details
CVE-2025-12283	A security flaw has been discovered in code-projects Client Details System 1.0. The impacted element is an unknown function. The manipulation results in authorization bypass. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	4.3	More Details
CVE-2025-62052	Missing Authorization vulnerability in Horea Radu One Page Express Companion one-page-express-companion.This issue affects One Page Express Companion: from n/a through <= 1.6.43.	4.3	More Details
CVE-2025-6833	The All in One Time Clock Lite – Tracking Employee Time Has Never Been Easier plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.0 via the 'aio_time_clock_lite_js' AJAX action due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber access and above, to clock other users in and out.	4.3	More Details
CVE-2025-12333	A vulnerability has been found in code-projects E-Commerce Website 1.0. This impacts an unknown function of the file /pages/supplier_add.php. The manipulation of the argument supp_name/supp_address leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-22173	Jira Align is vulnerable to an authorization issue. A low-privilege user can access unexpected endpoints that disclose a small amount of sensitive information. For example, a low-level user was able to view certain sprint data without the required permission.	4.3	More Details
CVE-2025-11958	An improper input validation in the Security Dashboard ignored-tasks API of Devolutions Server 2025.2.15.0 and earlier allows an authenticated user to cause a denial of service to the Security Dashboard via a crafted request.	4.1	More Details
CVE-2025-59776	A relative path traversal vulnerability was discovered in Productivity Suite software version 4.4.1.19. The vulnerability allows an unauthenticated remote attacker to interact with the ProductivityService PLC simulator and create arbitrary directories on the target machine.	4.0	More Details
CVE-2025-60023	A relative path traversal vulnerability was discovered in Productivity Suite software version 4.4.1.19. The vulnerability allows an unauthenticated remote attacker to interact with the ProductivityService PLC simulator and delete arbitrary directories on the target machine.	4.0	More Details
CVE-2025-62794	GitHub Workflow Updater is a VS Code extension that automatically pins GitHub Actions to specific commits for enhanced security. Before 0.0.7, any provided Github token would be stored in plaintext in the editor configuration as json on disk, rather than through the more secure "securestorage" api. An attacker with read only access to your home directory could have read this token and used it to perform actions with that token. Update to 0.0.7.	3.8	More Details
CVE-2025-11244	The Password Protected plugin for WordPress is vulnerable to authorization bypass via IP address spoofing in all versions up to, and including, 2.7.11. This is due to the plugin trusting client-controlled HTTP headers (such as X-Forwarded-For, HTTP_CLIENT_IP, and similar headers) to determine user IP addresses in the `pp_get_ip_address()` function when the "Use transients" feature is enabled. This makes it possible for attackers to bypass authorization by spoofing these headers with the IP address of a legitimately authenticated user, granted the "Use transients" option is enabled (non-default configuration) and the site is not behind a CDN or reverse proxy that overwrites these headers.	3.7	More Details
CVE-2025-10939	A flaw was found in Keycloak. The Keycloak guides recommend to not expose /admin path to the outside in case the installation is using a proxy. The issue occurs at least via ha-proxy, as it can be tricked to using relative/non-normalized paths to access the /admin application path relative to /realms which is expected to be exposed.	3.7	More Details

CVE-2025-11989	GitLab has remediated an issue in GitLab EE affecting all versions from 17.6.0 before 18.3.5, 18.4 before 18.4.3, and 18.5 before 18.5.1 that could have allowed an authenticated attacker to execute unauthorized quick actions by including malicious commands in specific descriptions.	3.7	More Details
CVE-2025-12224	A flaw has been found in Iqbolshoh php-business-website up to 10677743a8dfc281f85291a27cf63a0bce043c24. This vulnerability affects unknown code of the file admin/contact.php. This manipulation of the argument twitter causes cross site scripting. The attack may be initiated remotely. The exploit has been published and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. Other parameters might be affected as well. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-12227	A vulnerability was determined in projectworlds Gate Pass Management System 1.0. The affected element is an unknown function of the file /add-pass.php. Executing manipulation can lead to cross site scripting. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	3.5	More Details
CVE-2025-12269	A vulnerability was found in LearnHouse up to 98dfad76aad70711a8113f6c1fdabfccf10509ca. The affected element is an unknown function of the file /dash/org/settings/previews of the component Account Setting Page. The manipulation results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used. 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.	3.5	More Details
CVE-2025-12264	A security flaw has been discovered in Wisencode up to 20251012. Affected by this vulnerability is an unknown functionality of the file /support-ticket/create of the component Create Support Ticket Handler. The manipulation of the argument Message results in cross site scripting. The attack may be launched remotely. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-12251	A vulnerability has been found in OpenWGA 7.11.12 Build 737. This impacts an unknown function of the component Admin UI. The manipulation leads to cross site scripting. 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.	3.5	More Details
CVE-2025-12199	A vulnerability was found in dnsmasq up to 2.73rc6. Affected by this vulnerability is the function check_servers of the file src/network.c of the component Config File Handler. The manipulation results in null pointer dereference. The attack needs to be approached locally. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.3	More Details
CVE-2025-12200	A vulnerability was determined in dnsmasq up to 2.73rc6. Affected by this issue is the function parse_dhcp_opt of the file src/option.c of the component Config File Handler. This manipulation of the argument m causes null pointer dereference. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	3.3	More Details
CVE-2025-12207	A vulnerability has been found in Kamailio 5.5. This affects the function yyerror_at of the file src/core/cfg.y of the component Grammar Rule Handler. Such manipulation leads to null pointer dereference. The attack needs to be performed locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.3	More Details
CVE-2025-12206	A flaw has been found in Kamailio 5.5. The impacted element is the function rve_is_constant of the file src/core/rvalue.c. This manipulation causes null pointer dereference. The attack needs to be launched locally. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.3	More Details
CVE-2025-11248	ZohoCorp ManageEngine Endpoint Central versions prior to 11.4.2528.05 are vulnerable to a sensitive information logging issue. An authenticated user with access to the logs could potentially obtain the sensitive agent token.	3.2	More Details
CVE-2025-62772	On Mercku M6a devices through 2.1.0, session tokens remain valid for at least months in some cases.	3.1	More Details
CVE-2025-62774	On Mercku M6a devices through 2.1.0, the authentication system uses predictable session tokens based on timestamps.	3.1	More Details
CVE-2025-10723	The PixelYourSite WordPress plugin before 11.1.2 does not validate some URL parameters before using them to generate paths passed to function/s, allowing any admins to perform LFI attacks	2.7	More Details
CVE-2025-6601	GitLab has remediated an issue in GitLab EE affecting all versions from 18.4 before 18.4.3, and 18.5 before 18.5.1 that under certain conditions could have allowed authenticated users to gain unauthorized project access by exploiting the access request approval workflow.	2.7	More Details
CVE-2025-11888	The ShopEngine Elementor WooCommerce Builder Addon – All in One WooCommerce Solution plugin for WordPress is vulnerable to unauthorized modification of data due to an insufficient capability check on the post_deactive() function and post_activate() function in all versions up to, and including, 4.8.4. This makes it possible for authenticated attackers, with Editor-level access and above, to activate and deactivate licenses.	2.7	More Details
CVE-2025-41721	A high privileged remote attacker can influence the parameters passed to the openssl command due to improper neutralization of special elements when adding a password protected self-signed certificate.	2.7	More Details
CVE-2025-12282	A vulnerability was identified in code-projects Client Details System 1.0. The affected element is an unknown function of the file /admin/manage-users.php. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit is publicly available and might be used.	2.4	More Details
CVE-	A vulnerability was determined in code-projects Client Details System 1.0. Impacted is an unknown function of the file		

2025-12281	/admin/clientview.php. Executing manipulation can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	2.4	More Details
CVE-2025-12280	A vulnerability was found in code-projects Client Details System 1.0. This issue affects some unknown processing of the file /update-clients.php. Performing manipulation results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	2.4	More Details
CVE-2025-12279	A vulnerability has been found in code-projects Client Details System 1.0. This vulnerability affects unknown code of the file /welcome.php. Such manipulation leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2025-12228	A vulnerability was identified in projectworlds Expense Management System 1.0. The impacted element is an unknown function of the file /public/admin/users/create of the component Users Page. The manipulation leads to cross site scripting. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	2.4	More Details
CVE-2025-12231	A security vulnerability has been detected in projectworlds Expense Management System 1.0. Affected is an unknown function of the file /public/admin/expense_categories/create of the component Expense Categories Page. Such manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	2.4	More Details
CVE-2025-12303	A flaw has been found in PHPGurukul Curfew e-Pass Management System 1.0. The impacted element is an unknown function of the file admin-profile.php. Executing manipulation of the argument adminname/email can lead to cross site scripting. The attack may be launched remotely. The exploit has been published and may be used.	2.4	More Details
CVE-2025-12311	A vulnerability was detected in PHPGurukul Curfew e-Pass Management System 1.0. This issue affects some unknown processing of the file edit-category-detail.php. The manipulation of the argument catname results in cross site scripting. The attack can be launched remotely. The exploit is now public and may be used.	2.4	More Details
CVE-2025-12312	A flaw has been found in PHPGurukul Curfew e-Pass Management System 1.0. Impacted is an unknown function of the file view-pass-detail.php. This manipulation of the argument Fullname/Category causes cross site scripting. The attack may be initiated remotely. The exploit has been published and may be used.	2.4	More Details
CVE-2025-12229	A security flaw has been discovered in projectworlds Expense Management System 1.0. This affects an unknown function of the file /public/admin/roles/create of the component Roles Page. The manipulation results in cross site scripting. The attack may be performed from remote. The exploit has been released to the public and may be exploited.	2.4	More Details
CVE-2025-12230	A weakness has been identified in projectworlds Expense Management System 1.0. This impacts an unknown function of the file /public/admin/currencies/create of the component Currency Page. This manipulation causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.	2.4	More Details
CVE-2025-12332	A flaw has been found in SourceCodester Student Grades Management System 1.0. This affects the function delete_user of the file /admin.php. Executing manipulation can lead to cross site scripting. The attack may be performed from remote. The exploit has been published and may be used.	2.4	More Details
CVE-2025-12330	A security flaw has been discovered in Willow CMS up to 1.4.0. This issue affects some unknown processing of the file /admin/articles/add of the component Add Post Page. The manipulation of the argument title/body results in cross site scripting. The attack may be launched remotely. The exploit has been released to the public and may be exploited.	2.4	More Details
CVE-2025-62773	Mercku M6a devices through 2.1.0 allow TELNET sessions via a router.telnet.enabled.update request by an administrator.	2.4	More Details
CVE-2025-62778	Frappe Learning is a learning management system. A security issue was identified in Frappe Learning 2.39.1 and earlier, where students were able to access the Quiz Form if they had the URL.	N/A	More Details
CVE-2025-62261	Liferay Portal 7.4.0 through 7.4.3.99, and older unsupported versions, and Liferay DXP 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 34, and older unsupported versions stores password reset tokens in plain text, which allows attackers with access to the database to obtain the token, reset a user's password and take over the user's account.	N/A	More Details
CVE-2025-62260	Liferay Portal 7.4.0 through 7.4.3.99, and Liferay DXP 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions does not limit the number of objects returned from Headless API requests, which allows remote attackers to perform denial-of-service (DoS) attacks on the application by executing a request that returns a large number of objects.	N/A	More Details
CVE-2025-40038	In the Linux kernel, the following vulnerability has been resolved: KVM: SVM: Skip fastpath emulation on VM-Exit if next RIP isn't valid Skip the WRMSR and HLT fastpaths in SVM's VM-Exit handler if the next RIP isn't valid, e.g. because KVM is running with nrips=false. SVM must decode and emulate to skip the instruction if the CPU doesn't provide the next RIP, and getting the instruction bytes to decode requires reading guest memory. Reading guest memory through the emulator can fault, i.e. can sleep, which is disallowed since the fastpath handlers run with IRQs disabled. BUG: sleeping function called from invalid context at ./include/linux/uaccess.h:106 in_atomic(): 1, irqs_disabled(): 1, non_block: 0, pid: 32611, name: qemu preempt_count: 1, expected: 0 INFO: lockdep is turned off. irq event stamp: 30580 hardirqs last enabled at (30579): [<ffffffffc08b2527>] vcpu_run+0x1787/0x1db0 [kvm] hardirqs last disabled at (30580): [<ffffffffb4f62e32>] __schedule+0x1e2/0xed0 softirqs last enabled at (30570): [<ffffffffb4247a64>] fpu_swap_kvm_fpstate+0x44/0x210 softirqs last disabled at (30568): [<ffffffffb4247a64>] fpu_swap_kvm_fpstate+0x44/0x210 CPU: 298 UID: 0 PID: 32611 Comm: qemu Tainted: G U 6.16.0-smp--e6c618b51cfe-sleep #782 NONE Tainted: [U]=USER Hardware name: Google Astoria-Turin/astoria, BIOS 0.20241223.2-0 01/17/2025 Call Trace: <TASK> dump_stack_lvl+0x7d/0xb0 __might_resched+0x271/0x290 __might_fault+0x28/0x80 kvm_vcpu_read_guest_page+0x8d/0xc0 [kvm] kvm_fetch_guest_virt+0x92/0xc0 [kvm] __do_insn_fetch_bytes+0xf3/0x1e0 [kvm] x86_decode_insn+0xd1/0x1010 [kvm] x86_emulate_instruction+0x105/0x810 [kvm] __svm_skip_emulated_instruction+0xc4/0x140 [kvm_amd] handle_fastpath_invd+0xc4/0x1a0 [kvm] vcpu_run+0x11a1/0x1db0 [kvm] kvm_arch_vcpu_ioctl_run+0x5cc/0x730 [kvm] kvm_vcpu_ioctl+0x578/0x6a0 [kvm] __se_sys_ioctl+0x6d/0xb0 do_syscall_64+0x8a/0x2c0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x7f479d57a94b </TASK> Note, this is essentially a reapply of commit 5c30e8101e8d ("KVM: SVM: Skip WRMSR fastpath on VM-Exit if next RIP isn't valid"), but with	N/A	More Details

	different justification (KVM now grabs SRCU when skipping the instruction for other reasons).		
CVE-2025-40037	In the Linux kernel, the following vulnerability has been resolved: fbdev: simplefb: Fix use after free in simplefb_detach_genpds() The pm_domain cleanup can not be devres managed as it uses struct simplefb_par which is allocated within struct fb_info by framebuffer_alloc(). This allocation is explicitly freed by unregister_framebuffer() in simplefb_remove(). Devres managed cleanup runs after the device remove call and thus can no longer access struct simplefb_par. Call simplefb_detach_genpds() explicitly from simplefb_destroy() like the cleanup functions for clocks and regulators. Fixes an use after free on M2 Mac mini during aperture_remove_conflicting_devices() using the downstream asahi kernel with Debian's kernel config. For unknown reasons this started to consistently dereference an invalid pointer in v6.16.3 based kernels. [6.736134] BUG: KASAN: slab-use-after-free in simplefb_detach_genpds+0x58/0x220 [6.743545] Read of size 4 at addr ffff8000304743f0 by task (udev-worker)/227 [6.750697] [6.752182] CPU: 6 UID: 0 PID: 227 Comm: (udev-worker) Tainted: G S 6.16.3-asahi+ #16 PREEMPTLAZY [6.752186] Tainted: [S]=CPU_OUT_OF_SPEC [6.752187] Hardware name: Apple Mac mini (M2, 2023) (DT) [6.752189] Call trace: [6.752190] show_stack+0x34/0x98 (C) [6.752194] dump_stack_lvl+0x60/0x80 [6.752197] print_report+0x17c/0x4d8 [6.752201] kasan_report+0xb4/0x100 [6.752206] __asan_report_load4_noabort+0x20/0x30 [6.752209] simplefb_detach_genpds+0x58/0x220 [6.752213] devm_action_release+0x50/0x98 [6.752216] release_nodes+0xd0/0x2c8 [6.752219] devres_release_all+0xfc/0x178 [6.752221] device_unbind_cleanup+0x28/0x168 [6.752224] device_release_driver_internal+0x34c/0x470 [6.752228] device_release_driver+0x20/0x38 [6.752231] bus_remove_device+0x1b0/0x380 [6.752234] device_del+0x314/0x820 [6.752238] platform_device_del+0x3c/0x1e8 [6.752242] platform_device_unregister+0x20/0x50 [6.752246] aperture_detach_platform_device+0x1c/0x30 [6.752250] aperture_detach_devices+0x16c/0x290 [6.752253] aperture_remove_conflicting_devices+0x34/0x50 ... [6.752343] [6.967409] Allocated by task 62: [6.970724] kasan_save_stack+0x3c/0x70 [6.974560] kasan_save_track+0x20/0x40 [6.978397] kasan_save_alloc_info+0x40/0x58 [6.982670] __kasan_kmalloc+0xd4/0xd8 [6.986420] __kmalloc_noprof+0x194/0x540 [6.990432] framebuffer_alloc+0xc8/0x130 [6.994444] simplefb_probe+0x258/0x2378 ... [7.054356] [7.055838] Freed by task 227: [7.058891] kasan_save_stack+0x3c/0x70 [7.062727] kasan_save_track+0x20/0x40 [7.066565] kasan_save_free_info+0x4c/0x80 [7.070751] __kasan_slab_free+0x6c/0xa0 [7.074675] kfree+0x10c/0x380 [7.077727] framebuffer_release+0x5c/0x90 [7.081826] simplefb_destroy+0x1b4/0x2c0 [7.085837] put_fb_info+0x98/0x100 [7.089326] unregister_framebuffer+0x178/0x320 [7.093861] simplefb_remove+0x3c/0x60 [7.097611] platform_remove+0x60/0x98 [7.101361] device_remove+0xb8/0x160 [7.105024] device_release_driver_internal+0x2fc/0x470 [7.110256] device_release_driver+0x20/0x38 [7.114529] bus_remove_device+0x1b0/0x380 [7.118628] device_del+0x314/0x820 [7.122116] platform_device_del+0x3c/0x1e8 [7.126302] platform_device_unregister+0x20/0x50 [7.131012] aperture_detach_platform_device+0x1c/0x30 [7.136157] aperture_detach_devices+0x16c/0x290 [7.140779] aperture_remove_conflicting_devices+0x34/0x50 ...	N/A	More Details
CVE-2025-62779	Frappe Learning is a learning system that helps users structure their content. In Frappe Learning 2.39.1 and earlier, users were able to add HTML through input fields in the Job Form.	N/A	More Details
CVE-2025-62254	The ComboServlet in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.2, 2023.Q3.1 through 2023.Q3.5, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions does not limit the number or size of the files it will combine, which allows remote attackers to create very large responses that lead to a denial of service attack via the URL query string.	N/A	More Details
CVE-2025-40036	In the Linux kernel, the following vulnerability has been resolved: misc: fastrpc: fix possible map leak in fastrpc_put_args copy_to_user() failure would cause an early return without cleaning up the fdlist, which has been updated by the DSP. This could lead to map leak. Fix this by redirecting to a cleanup path on failure, ensuring that all mapped buffers are properly released before returning.	N/A	More Details
CVE-2025-62258	CSRF vulnerability in Headless API in Liferay Portal 7.4.0 through 7.4.3.107, and Liferay DXP 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions allows remote attackers to execute any Headless API via the `endpoint` parameter.	N/A	More Details
CVE-2025-62784	InventoryGui is a library for creating chest GUIs for Bukkit/Spigot plugins. Versions before 1.6.5 contain a vulnerability where any plugin using a GUI with the GuiStorageElement and allows taking out items out of that element can allow item duplication when the experimental Bundle item feature is enabled on the server. The vulnerability is resolved in version 1.6.5.	N/A	More Details
CVE-2025-40035	In the Linux kernel, the following vulnerability has been resolved: Input: uinput - zero-initialize uinput_ff_upload_compat to avoid info leak Struct ff_effect_compat is embedded twice inside uinput_ff_upload_compat, contains internal padding. In particular, there is a hole after struct ff_replay to satisfy alignment requirements for the following union member. Without clearing the structure, copy_to_user() may leak stack data to userspace. Initialize ff_up_compat to zero before filling valid fields.	N/A	More Details
CVE-2025-40034	In the Linux kernel, the following vulnerability has been resolved: PCI/AER: Avoid NULL pointer dereference in aer_ratelimit() When platform firmware supplies error information to the OS, e.g., via the ACPI APEI GHES mechanism, it may identify an error source device that doesn't advertise an AER Capability and therefore dev->aer_info, which contains AER stats and ratelimiting data, is NULL. pci_dev_aer_stats_incr() already checks dev->aer_info for NULL, but aer_ratelimit() did not, leading to NULL pointer dereferences like this one from the URL below: {1}[Hardware Error]: Hardware error from APEI Generic Hardware Error Source: 0 {1}[Hardware Error]: event severity: corrected {1}[Hardware Error]: device_id: 0000:00:00.0 {1}[Hardware Error]: vendor_id: 0x8086, device_id: 0x2020 {1}[Hardware Error]: aer_cor_status: 0x00001000, aer_cor_mask: 0x00002000 BUG: kernel NULL pointer dereference, address: 0000000000000264 RIP: 0010:___ratelimit+0xc/0x1b0 pci_print_aer+0x141/0x360 aer_recover_work_func+0xb5/0x130 [8086:2020] is an Intel "Sky Lake-E DMI3 Registers" device that claims to be a Root Port but does not advertise an AER Capability. Add a NULL check in aer_ratelimit() to avoid the NULL pointer dereference. Note that this also prevents ratelimiting these events from GHES. [bhelgaas: add crash details to commit log]	N/A	More Details
CVE-2025-62259	Liferay Portal 7.4.0 through 7.4.3.109, and older unsupported versions, and Liferay DXP 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions does not limit access to APIs before a user has verified their email address, which allows remote users to access and edit content via the API.	N/A	More Details
CVE-2025-	microCLAUDIA in v3.2.0 and prior has an improper access control vulnerability. This flaw allows an authenticated user to perform unauthorized actions on other organizations' systems by sending direct API requests. To do so, the attacker can use organization identifiers obtained through a compromised endpoint or deduced manually. This vulnerability allows access	N/A	More Details

41090	between tenants, enabling an attacker to list and manage remote assets, uninstall agents, and even delete vaccines configurations.		
CVE-2025-53701	Vilar VS-IPC1002 IP cameras are vulnerable to Reflected XSS (Cross-site Scripting) attacks, because parameters in GET requests sent to /cgi-bin/action endpoint are not sanitized properly, making it possible to target logged in admin users. The vendor did not respond in any way. Only version 1.1.0.18 was tested, other versions might be vulnerable as well.	N/A	More Details
CVE-2025-43024	A GUI dialog of an application allows to view what files are in the file system without proper authorization.	N/A	More Details
CVE-2025-40031	In the Linux kernel, the following vulnerability has been resolved: tee: fix register_shm_helper() In register_shm_helper(), fix incorrect error handling for a call to iov_iter_extract_pages(). A case is missing for when iov_iter_extract_pages() only got some pages and return a number larger than 0, but not the requested amount. This fixes a possible NULL pointer dereference following a bad input from ioctl(TEE_IOC_SHM_REGISTER) where parts of the buffer isn't mapped.	N/A	More Details
CVE-2025-40027	In the Linux kernel, the following vulnerability has been resolved: net/9p: fix double req put in p9_fd_cancelled Syzkaller reports a KASAN issue as below: general protection fault, probably for non-canonical address 0xfbd59c0000000021: 0000 [#1] PREEMPT SMP KASAN NOPTI KASAN: maybe wild-memory-access in range [0xdead000000000108-0xdead00000000010f] CPU: 0 PID: 5083 Comm: syz-executor.2 Not tainted 6.1.134-syzkaller-00037-g855bd1d7d838 #0 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.12.0-1 04/01/2014 RIP: 0010:__list_del include/linux/list.h:114 [inline] RIP: 0010:__list_del_entry include/linux/list.h:137 [inline] RIP: 0010:list_del include/linux/list.h:148 [inline] RIP: 0010:p9_fd_cancelled+0xe9/0x200 net/9p/trans_fd.c:734 Call Trace: <TASK> p9_client_flush+0x351/0x440 net/9p/client.c:614 p9_client_rpc+0xb6b/0xc70 net/9p/client.c:734 p9_client_version net/9p/client.c:920 [inline] p9_client_create+0xb51/0x1240 net/9p/client.c:1027 v9fs_session_init+0x1f0/0x18f0 fs/9p/v9fs.c:408 v9fs_mount+0xba/0xcb0 fs/9p/vfs_super.c:126 legacy_get_tree+0x108/0x220 fs/fs_context.c:632 vfs_get_tree+0x8e/0x300 fs/super.c:1573 do_new_mount fs/namespace.c:3056 [inline] path_mount+0x6a6/0x1e90 fs/namespace.c:3386 do_mount fs/namespace.c:3399 [inline] __do_sys_mount fs/namespace.c:3607 [inline] __se_sys_mount fs/namespace.c:3584 [inline] __x64_sys_mount+0x283/0x300 fs/namespace.c:3584 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x35/0x80 arch/x86/entry/common.c:81 entry_SYSCALL_64_after_hwframe+0x6e/0xd8 This happens because of a race condition between: - The 9p client sending an invalid flush request and later cleaning it up; - The 9p client in p9_read_work() canceled all pending requests. Thread 1 Thread 2 ... p9_client_create() ... p9_fd_create() ... p9_conn_create() ... // start Thread 2 INIT_WORK(&m->rq, p9_read_work); p9_read_work() ... p9_client_rpc() ... ... p9_conn_cancel() ... spin_lock(&m->req_lock); ... p9_fd_cancelled() ... ... spin_unlock(&m->req_lock); // status rewrite p9_client_cb(m->client, req, REQ_STATUS_ERROR) // first remove list_del(&req->req_list); ... spin_lock(&m->req_lock) ... // second remove list_del(&req->req_list); spin_unlock(&m->req_lock) ... Commit 74d6a5d56629 ("9p/trans_fd: Fix concurrency del of req_list in p9_fd_cancelled/p9_read_work") fixes a concurrency issue in the 9p filesystem client where the req_list could be deleted simultaneously by both p9_read_work and p9_fd_cancelled functions, but for the case where req->status equals REQ_STATUS_RCVD. Update the check for req->status in p9_fd_cancelled to skip processing not just received requests, but anything that is not SENT, as whatever changed the state from SENT also removed the request from its list. Found by Linux Verification Center (linuxtesting.org) with Syzkaller. [updated the check from status == RECV || status == ERROR to status != SENT]	N/A	More Details
CVE-2025-40026	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: Don't (re)check L1 intercepts when completing userspace I/O When completing emulation of instruction that generated a userspace exit for I/O, don't recheck L1 intercepts as KVM has already finished that phase of instruction execution, i.e. has already committed to allowing L2 to perform I/O. If L1 (or host userspace) modifies the I/O permission bitmaps during the exit to userspace, KVM will treat the access as being intercepted despite already having emulated the I/O access. Pivot on EMULTYPE_NO_DECODE to detect that KVM is completing emulation. Of the three users of EMULTYPE_NO_DECODE, only complete_emulated_io() (the intended "recipient") can reach the code in question. gp_interception()'s use is mutually exclusive with is_guest_mode(), and complete_emulated_insn_gp() unconditionally pairs EMULTYPE_NO_DECODE with EMULTYPE_SKIP. The bad behavior was detected by a syzkaller program that toggles port I/O interception during the userspace I/O exit, ultimately resulting in a WARN on vcpu->arch.pio.count being non-zero due to KVM no completing emulation of the I/O instruction. WARNING: CPU: 23 PID: 1083 at arch/x86/kvm/x86.c:8039 emulator_pio_in_out+0x154/0x170 [kvm] Modules linked in: kvm_intel kvm irqbypass CPU: 23 UID: 1000 PID: 1083 Comm: repro Not tainted 6.16.0-rc5-c1610d2d66b1-next-vm #74 NONE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 0.0.0 02/06/2015 RIP: 0010:emulator_pio_in_out+0x154/0x170 [kvm] PKRU: 55555554 Call Trace: <TASK> kvm_fast_pio+0xd6/0x1d0 [kvm] vmx_handle_exit+0x149/0x610 [kvm_intel] kvm_arch_vcpu_ioctl_run+0xda8/0x1ac0 [kvm] kvm_vcpu_ioctl+0x244/0x8c0 [kvm] __x64_sys_ioctl+0x8a/0xd0 do_syscall_64+0x5d/0xc60 entry_SYSCALL_64_after_hwframe+0x4b/0x53 </TASK>	N/A	More Details
CVE-2025-40029	In the Linux kernel, the following vulnerability has been resolved: bus: fsl-mc: Check return value of platform_get_resource() platform_get_resource() returns NULL in case of failure, so check its return value and propagate the error in order to prevent NULL pointer dereference.	N/A	More Details
CVE-2025-40025	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to do sanity check on node footer for non inode dnode As syzbot reported below: ------------[cut here]------------ kernel BUG at fs/f2fs/file.c:1243! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI CPU: 0 UID: 0 PID: 5354 Comm: syz.0.0 Not tainted 6.17.0-rc1-syzkaller-00211-g90d970cade8e #0 PREEMPT(full) RIP: 0010:f2fs_truncate_hole+0x69e/0x6c0 fs/f2fs/file.c:1243 Call Trace: <TASK> f2fs_punch_hole+0x2db/0x330 fs/f2fs/file.c:1306 f2fs_fallocate+0x546/0x990 fs/f2fs/file.c:2018 vfs_fallocate+0x666/0x7e0 fs/open.c:342 ksys_fallocate fs/open.c:366 [inline] __do_sys_fallocate fs/open.c:371 [inline] __se_sys_fallocate fs/open.c:369 [inline] __x64_sys_fallocate+0xc0/0x110 fs/open.c:369 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0x3b0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f1e65f8ebe9 w/ a fuzzed image, f2fs may encounter panic due to it detects inconsistent truncation range in direct node in f2fs_truncate_hole(). The root cause is: a non-inode dnode may has the same footer.ino and footer.nid, so the dnode will be parsed as an inode, then ADDRS_PER_PAGE() may return wrong blkaddr count which may be 923 typically, by chance, dn.ofs_in_node is equal to 923, then count can be calculated to 0 in below statement, later it will trigger panic w/ f2fs_bug_on(, count == 0 || ...). count = min(end_offset - dn.ofs_in_node, pg_end - pg_start); This patch introduces a new node_type NODE_TYPE_NON_INODE, then allowing passing the new_type to sanity_check_node_footer in f2fs_get_node_folio() to detect corruption that a non-inode dnode has the same footer.ino and footer.nid. Scripts to reproduce: mkfs.f2fs -f /dev/vdb mount /dev/vdb /mnt/f2fs touch /mnt/f2fs/foo touch /mnt/f2fs/bar dd if=/dev/zero of=/mnt/f2fs/foo bs=1M count=8 umount /mnt/f2fs inject.f2fs --node --mb i_nid --nid 4 --idx 0 --val 5 /dev/vdb mount /dev/vdb /mnt/f2fs xfs_io /mnt/f2fs/foo -c "fpunch 6984k 4k"	N/A	More Details

CVE-2025-10151	Improper locking vulnerability in Softing Industrial Automation GmbH gateways allows infected memory and/or resource leak exposure.This issue affects smartLink HW-PN: from 1.02 through 1.03 smartLink HW-DP: 1.31	N/A	More Details
CVE-2025-10150	Webserver crash caused by scanning on TCP port 80 in Softing Industrial Automation GmbH gateways and switch.This issue affects smartLink HW-PN: from 1.02 through 1.03 smartLink HW-DP: 1.31	N/A	More Details
CVE-2025-40030	In the Linux kernel, the following vulnerability has been resolved: pinctrl: check the return value of pinmux_ops::get_function_name() While the API contract in docs doesn't specify it explicitly, the generic implementation of the get_function_name() callback from struct pinmux_ops - pinmux_generic_get_function_name() - can fail and return NULL. This is already checked in pinmux_check_ops() so add a similar check in pinmux_func_name_to_selector() instead of passing the returned pointer right down to strcmp() where the NULL can get dereferenced. This is normal operation when adding new pinfunctions.	N/A	More Details
CVE-2025-40032	In the Linux kernel, the following vulnerability has been resolved: PCI: endpoint: pci-epf-test: Add NULL check for DMA channels before release The fields dma_chan_tx and dma_chan_rx of the struct pci_epf_test can be NULL even after EPF initialization. Then it is prudent to check that they have non-NULL values before releasing the channels. Add the checks in pci_epf_test_clean_dma_chan(). Without the checks, NULL pointer dereferences happen and they can lead to a kernel panic in some cases: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000050 Call trace: dma_release_channel+0x2c/0x120 (P) pci_epf_test_epc_deinit+0x94/0xc0 [pci_epf_test] pci_epc_deinit_notify+0x74/0xc0 tegra_pcie_ep_pex_rst_irq+0x250/0x5d8 irq_thread_fn+0x34/0xb8 irq_thread+0x18c/0x2e8 kthread+0x14c/0x210 ret_from_fork+0x10/0x20 [mani: trimmed the stack trace]	N/A	More Details
CVE-2025-1680	An acceptance of extraneous untrusted data with trusted data vulnerability has been identified in Moxa’s Ethernet switches, which allows attackers with administrative privileges to manipulate HTTP Host headers by injecting a specially crafted Host header into HTTP requests sent to an affected device’s web service. This vulnerability is classified as Host Header Injection, where invalid Host headers can manipulate to redirect users, forge links, or phishing attacks. There is no impact to the confidentiality, integrity, and availability of the affected device; no loss of confidentiality, integrity, and availability within any subsequent systems.	N/A	More Details
CVE-2025-40033	In the Linux kernel, the following vulnerability has been resolved: remoteproc: pru: Fix potential NULL pointer dereference in pru_rproc_set_ctable() pru_rproc_set_ctable() accessed rproc->priv before the IS_ERR_OR_NULL check, which could lead to a null pointer dereference. Move the pru assignment, ensuring we never dereference a NULL rproc pointer.	N/A	More Details
CVE-2025-34155	Tibbo AggreGate Network Manager < 6.40.05 contains an observable response discrepancy in its login functionality. Authentication failure messages differ based on whether a supplied username exists or not, allowing an unauthenticated remote attacker to infer valid account identifiers. This can facilitate user enumeration and increase the likelihood of targeted brute-force or credential-stuffing attacks.	N/A	More Details
CVE-2025-12114	Enabled serial console could potentially leak information that might help attacker to find vulnerabilities.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-62777	Use of Hard-Coded Credentials issue exists in MZK-DP300N version 1.07 and earlier, which may allow an attacker within the local network to log in to the affected device via Telnet and execute arbitrary commands.	N/A	More Details
CVE-2025-62256	Liferay Portal 7.4.0 through 7.4.3.109, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.7, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions does not properly restrict access to OpenAPI in certain circumstances, which allows remote attackers to access the OpenAPI YAML file via a crafted URL.	N/A	More Details
CVE-2025-53702	Vilar VS-IPC1002 IP cameras are vulnerable to DoS (Denial-of-Service) attacks. An unauthenticated attacker on the same local network might send a crafted request to /cgi-bin/action endpoint and render the device completely unresponsive. A manual restart of the device is required. The vendor did not respond in any way. Only version 1.1.0.18 was tested, other versions might be vulnerable as well.	N/A	More Details
CVE-2025-40028	In the Linux kernel, the following vulnerability has been resolved: binder: fix double-free in dbitmap A process might fail to allocate a new bitmap when trying to expand its proc->dmap. In that case, dbitmap_grow() fails and frees the old bitmap via dbitmap_free(). However, the driver calls dbitmap_free() again when the same process terminates, leading to a double-free error: == BUG: KASAN: double-free in binder_proc_dec_tmpref+0x2e0/0x55c Free of addr ffff00000b7c1420 by task kworker/9:1/209 CPU: 9 UID: 0 PID: 209 Comm: kworker/9:1 Not tainted 6.17.0-rc6-dirty #5 PREEMPT Hardware name: linux,dummy-virt (DT) Workqueue: events binder_deferred_func Call trace: kfree+0x164/0x31c binder_proc_dec_tmpref+0x2e0/0x55c binder_deferred_func+0xc24/0x1120 process_one_work+0x520/0xba4 [...] Allocated by task 448: __kmalloc_noprof+0x178/0x3c0 bitmap_zalloc+0x24/0x30 binder_open+0x14c/0xc10 [...] Freed by task 449: kfree+0x184/0x31c binder_inc_ref_for_node+0xb44/0xe44 binder_transaction+0x29b4/0x7fbc binder_thread_write+0x1708/0x442c binder_ioctl+0x1b50/0x2900 [...] == Fix this issue by marking proc->map NULL in dbitmap_free().	N/A	More Details
CVE-2025-1679	Cross-site Scripting has been identified in Moxa’s Ethernet switches, which allows an authenticated administrative attacker to inject malicious scripts to an affected device’s web service that could impact authenticated users interacting with the device’s web interface. This vulnerability is classified as stored cross-site scripting (XSS); attackers inject malicious scripts into the system, and the scripts persist across sessions. There is no impact to the confidentiality, integrity, and availability of the affected device; no loss of availability within any subsequent systems but has some loss of confidentiality and integrity within the subsequent system.	N/A	More Details
CVE-2025-8536	A SQL injection vulnerability has been identified in DobryCMS. Improper neutralization of input provided by user into language functionality allows for SQL Injection attacks. This issue affects older branches of this software.	N/A	More Details

CVE-2025-40039	In the Linux kernel, the following vulnerability has been resolved: ksmbd: Fix race condition in RPC handle list access The 'sess->rpc_handle_list' XArray manages RPC handles within a ksmbd session. Access to this list is intended to be protected by 'sess->rpc_lock' (an rw_semaphore). However, the locking implementation was flawed, leading to potential race conditions. In ksmbd_session_rpc_open(), the code incorrectly acquired only a read lock before calling xa_store() and xa_erase(). Since these operations modify the XArray structure, a write lock is required to ensure exclusive access and prevent data corruption from concurrent modifications. Furthermore, ksmbd_session_rpc_method() accessed the list using xa_load() without holding any lock at all. This could lead to reading inconsistent data or a potential use-after-free if an entry is concurrently removed and the pointer is dereferenced. Fix these issues by: 1. Using down_write() and up_write() in ksmbd_session_rpc_open() to ensure exclusive access during XArray modification, and ensuring the lock is correctly released on error paths. 2. Adding down_read() and up_read() in ksmbd_session_rpc_method() to safely protect the lookup.	N/A	More Details
CVE-2025-34310	IPFire versions prior to 2.29 (Core Update 198) contain a stored cross-site scripting (XSS) vulnerability that allows an authenticated attacker to inject arbitrary JavaScript code through the INC_SPD, OUT_SPD, DEFCLASS_INC, and DEFCLASS_OUT parameters when updating Quality of Service (QoS) settings. When a user updates speeds or classes, the application issues an HTTP POST request to /cgi-bin/qos.cgi and the values for incoming/outgoing speeds and default classes are provided in the INC_SPD, OUT_SPD, DEFCLASS_INC, and DEFCLASS_OUT parameters. The values of these parameters are stored and later rendered in the web interface without proper sanitation or encoding, allowing injected scripts to execute in the context of other users who view the affected QoS entries.	N/A	More Details
CVE-2025-62713	Kottster is a self hosted Node.js admin panel. From versions 3.2.0 to before 3.3.2, Kottster contains a pre-authentication remote code execution (RCE) vulnerability when running in development mode. This affects development mode only, production deployments were never affected. This issue has been fixed in version 3.3.2.	N/A	More Details
CVE-2025-34318	IPFire versions prior to 2.29 (Core Update 198) contain a stored cross-site scripting (XSS) vulnerability that allows an authenticated attacker to inject arbitrary JavaScript code through the TLS_HOSTNAME, UPSTREAM_USER, UPSTREAM_PASSWORD, ADMIN_MAIL_ADDRESS, and ADMIN_PASSWORD parameters when adding a new DNS entry. When a user adds a DNS entry, the application issues an HTTP POST request to /cgi-bin/dns.cgi and these values are provided in the corresponding parameters. The values are stored and later rendered in the web interface without proper sanitation or encoding, allowing injected scripts to execute in the context of other users who view the affected DNS configuration.	N/A	More Details
CVE-2025-34317	IPFire versions prior to 2.29 (Core Update 198) contain a stored cross-site scripting (XSS) vulnerability that allows an authenticated attacker to inject arbitrary JavaScript code through the TLS_HOSTNAME parameter when adding a new DNS entry. When a user adds a DNS entry, the application issues an HTTP POST request to /cgi-bin/dns.cgi and the TLS hostname is provided in the TLS_HOSTNAME parameter. The value of this parameter is stored and later rendered in the web interface without proper sanitation or encoding, allowing injected scripts to execute in the context of other users who view the affected DNS configuration.	N/A	More Details
CVE-2025-34316	IPFire versions prior to 2.29 (Core Update 198) contain a stored cross-site scripting (XSS) vulnerability that allows an authenticated attacker to inject arbitrary JavaScript code through the txt_mailuser and txt_mailpass parameters when updating the mail server settings. When a user updates the mail server, the application issues an HTTP POST request to /cgi-bin/mail.cgi and the username and password are provided in the txt_mailuser and txt_mailpass parameters. The values of these parameters are stored and later rendered in the web interface without proper sanitation or encoding, allowing injected scripts to execute in the context of other users who view the affected mail configuration.	N/A	More Details
CVE-2025-34315	IPFire versions prior to 2.29 (Core Update 198) contain a stored cross-site scripting (XSS) vulnerability that allows an authenticated attacker to inject arbitrary JavaScript code through the REMOTELOG_ADDR parameter when updating the remote syslog server address. When a user updates the Remote logging Syslog server, the application issues an HTTP POST request to /cgi-bin/logs.cgi/config.dat and the server address is provided in the REMOTELOG_ADDR parameter. The value of this parameter is stored and later rendered in the web interface without proper sanitation or encoding, allowing injected scripts to execute in the context of other users who view the affected configuration page.	N/A	More Details
CVE-2025-34314	IPFire versions prior to 2.29 (Core Update 198) contain a stored cross-site scripting (XSS) vulnerability that allows an authenticated attacker to inject arbitrary JavaScript code through the SRC, DST, and COMMENT parameters when creating a time constraint rule. When a user adds a time constraint rule the application issues an HTTP POST request to /cgi-bin/urlfilter.cgi with the MODE parameter set to TIMECONSTRAINT and the source hostnames/IPs, destination, and remark provided in the SRC, DST, and COMMENT parameters respectively. The values of these parameters are stored and later rendered in the web interface without proper sanitation or encoding, allowing injected scripts to execute in the context of other users who view the affected time constraint entry.	N/A	More Details
CVE-2025-34313	IPFire versions prior to 2.29 (Core Update 198) contain a stored cross-site scripting (XSS) vulnerability that allows an authenticated attacker to inject arbitrary JavaScript code through the QUOTA_USERS parameter when creating a user quota rule. When a user adds a new user quota rule the application issues an HTTP POST request to /cgi-bin/urlfilter.cgi with the MODE parameter set to USERQUOTA and the assigned user(s) provided in the QUOTA_USERS parameter. The value of this parameter is stored and later rendered in the web interface without proper sanitation or encoding, allowing injected scripts to execute in the context of other users who view the affected quota entry.	N/A	More Details
CVE-2025-34312	IPFire versions prior to 2.29 (Core Update 198) contain a command injection vulnerability that allows an authenticated attacker to execute arbitrary commands as the 'nobody' user via the BE_NAME parameter when installing a blacklist. When a blacklist is installed the application issues an HTTP POST to /cgi-bin/urlfilter.cgi and interpolates the value of BE_NAME directly into a shell invocation without appropriate sanitation. Crafted input can inject shell metacharacters, leading to arbitrary command execution in the context of the 'nobody' user.	N/A	More Details
CVE-2025-34311	IPFire versions prior to 2.29 (Core Update 198) contain a command injection vulnerability that allows an authenticated attacker to execute arbitrary commands as the user 'nobody' via multiple parameters when creating a Proxy report. When a user creates a Proxy report the application issues an HTTP POST to /cgi-bin/logs.cgi/calamaris.dat and reads the values of DAY_BEGIN, MONTH_BEGIN, YEAR_BEGIN, DAY_END, MONTH_END, YEAR_END, NUM_DOMAINS, PERF_INTERVAL, NUM_CONTENT, HIST_LEVEL, NUM_HOSTS, NUM_URLS, and BYTE_UNIT, which are interpolated directly into the shell invocation of the mkreport helper. Because these parameters are never sanitized for improper characters or constructs, a crafted POST can inject shell metacharacters into one or more fields, causing arbitrary commands to run with the privileges of the 'nobody' user.	N/A	More Details
	IPFire versions prior to 2.29 (Core Update 198) contain a stored cross-site scripting (XSS) vulnerability that allows an		

CVE-2025-34309	authenticated attacker to inject arbitrary JavaScript code through the SERVICE, LOGIN, and PASSWORD parameters when creating or editing a Dynamic DNS host. When a new Dynamic DNS host is added, the application issues an HTTP POST request to /cgi-bin/ddns.cgi and saves the values of the LOGIN, PASSWORD, and SERVICE parameters. The SERVICE value is displayed after the host entry is created, and the LOGIN and PASSWORD values are displayed when that host entry is edited. The values of these parameters are stored and later rendered in the web interface without proper sanitation or encoding, allowing injected scripts to execute in the context of other users who view or edit the affected Dynamic DNS entries.	N/A	More Details
CVE-2025-62782	InventoryGui is a library for creating chest GUIs for Bukkit/Spigot plugins. Versions 1.6.3-SNAPSHOT and earlier contain a vulnerability where GUIs using GuiStorageElement can allow item duplication when the experimental Bundle item feature is enabled on the server. The vulnerability is resolved in version 1.6.4-SNAPSHOT.	N/A	More Details
CVE-2025-34308	IPFire versions prior to 2.29 (Core Update 198) contain a stored cross-site scripting (XSS) vulnerability that allows an authenticated attacker to inject arbitrary JavaScript code through the UPDATE_VALUE parameter when updating the default time synchronization settings. When the default values displayed on the Time Server page are updated, the application issues an HTTP POST request to /cgi-bin/time.cgi, and the synchronization value is provided in the UPDATE_VALUE parameter. The value of this parameter is stored and later rendered in the web interface without proper sanitation or encoding, allowing injected scripts to execute in the context of other users who view the affected Time Server configuration page.	N/A	More Details
CVE-2025-34307	IPFire versions prior to 2.29 (Core Update 198) contain a stored cross-site scripting (XSS) vulnerability that allows an authenticated attacker to inject arbitrary JavaScript code through the pienumber parameter when updating the firewall country search defaults. When a user updates the default values for the firewall country search, the application issues an HTTP POST request to /cgi-bin/logs.cgi/firewalllogcountry.dat and the default number of countries to display is provided in the pienumber parameter. The value of this parameter is stored and later rendered in the web interface without proper sanitation or encoding, allowing injected scripts to execute in the context of other users who view the affected firewall country search settings.	N/A	More Details
CVE-2025-34306	IPFire versions prior to 2.29 (Core Update 198) contain a stored cross-site scripting (XSS) vulnerability that allows an authenticated attacker to inject arbitrary JavaScript code through the pienumber parameter when updating the default firewall IP search values. When a user updates these defaults, the application issues an HTTP POST request to /cgi-bin/logs.cgi/firewalllogip.dat with the default number of IPs in the pienumber parameter. The value of this parameter is stored and later rendered in the web interface without proper sanitation or encoding, allowing injected scripts to execute in the context of other users who view the affected page.	N/A	More Details
CVE-2025-34305	IPFire versions prior to 2.29 (Core Update 198) contain multiple stored cross-site scripting (XSS) vulnerabilities caused by a bug in the cleanhtml() function (/var/ipfire/header.pl) that fails to apply HTML-entity encoding to user input. When an authenticated user submits data to affected endpoints - for example, POST /cgi-bin/wakeonlan.cgi (CLIENT_COMMENT), /cgi-bin/dhcp.cgi (ADVOPT_DATA, FIX_REMARK, FIX_FILENAME, FIX_ROOTPATH), /cgi-bin/connscheduler.cgi (ACTION_COMMENT), /cgi-bin/dnsforward.cgi (REMARK), /cgi-bin/vpnmain.cgi (REMARK), or /cgi-bin/dns.cgi (REMARK) - the application calls escape() and HTML::Entities::encode_entities() but never assigns the sanitized result back to the output variable. The original unsanitized value is therefore stored and later rendered in the web interface without proper sanitation or encoding, allowing injected scripts to execute in the context of other users who view the affected entries.	N/A	More Details
CVE-2025-34304	IPFire versions prior to 2.29 (Core Update 198) contain a SQL injection vulnerability that allows an authenticated attacker to manipulate the SQL query used when viewing OpenVPN connection logs via the CONNECTION_NAME parameter. When viewing a range of OpenVPN connection logs, the application issues an HTTP POST request to the Request-URI /cgi-bin/logs.cgi/ovpnclients.dat and inserts the value of the CONNECTION_NAME parameter directly into the WHERE clause without proper sanitization or parameterization. The unsanitized value can alter the executed query and be used to disclose sensitive information from the database.	N/A	More Details
CVE-2025-34303	IPFire versions prior to 2.29 (Core Update 198) contain a stored cross-site scripting (XSS) vulnerability that allows an authenticated attacker to inject arbitrary JavaScript code through the IGNORE_ENTRY_REMARK parameter when adding a whitelisted host. When a whitelisted host is added, an HTTP POST request is sent to the Request-URI /cgi-bin/ids.cgi and the remark for the entry is provided in the IGNORE_ENTRY_REMARK parameter. The value of this parameter is stored and later rendered in the web interface without proper sanitization or encoding, allowing injected scripts to execute in the context of other users who view the affected whitelist entry.	N/A	More Details
CVE-2025-34302	IPFire versions prior to 2.29 (Core Update 198) contain a stored cross-site scripting (XSS) vulnerability that allows an authenticated attacker to inject arbitrary JavaScript code through the PROT parameter when creating a new service. When a user adds a service, the application issues an HTTP POST request with the ACTION parameter set to saveservice, and the protocol type is specified in the PROT parameter. The value of this parameter is stored and later rendered in the web interface without proper sanitization or encoding, allowing injected scripts to execute in the context of other users viewing the affected service entry.	N/A	More Details
CVE-2025-34301	IPFire versions prior to 2.29 (Core Update 198) contain a stored cross-site scripting (XSS) vulnerability that allows an authenticated attacker to inject arbitrary JavaScript code into the COUNTRY_CODE parameter when creating a location group. When a user adds a new location group, the application issues an HTTP POST request with the ACTION parameter set to savelocationgrp, and the value of the COUNTRY_CODE parameter determines the flag displayed for that group. The value of this parameter is stored and later rendered in the web interface without proper sanitization or encoding, allowing malicious scripts to be executed in the context of other users viewing the affected page.	N/A	More Details
CVE-2025-34156	Tibbo AggreGate Network Manager < 6.40.05 exposes sensitive system information through an unauthenticated endpoint at /cwmp/happyaxis.jsp. The page discloses Java system properties, server path details, and version information to unauthorized users, resulting in information disclosure that could aid further compromise.	N/A	More Details
CVE-2025-61043	An out-of-bounds read vulnerability has been discovered in Monkey's Audio 11.31, specifically in the CAPECharacterHelper::GetUTF16FromUTF8 function. The issue arises from improper handling of the length of the input UTF-8 string, causing the function to read past the memory boundary. This vulnerability may result in a crash or expose sensitive data.	N/A	More Details
CVE-2025-62255	Self Cross-site scripting (XSS) vulnerability on the edit Knowledge Base article page in Liferay Portal 7.4.0 through 7.4.3.101, and older unsupported versions, and Liferay DXP 2023.Q3.1 through 2023.Q3.5, 7.4 GA through update 92, and older unsupported versions allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into an	N/A	More Details

	attachment's filename.		
CVE-2025-61128	Stack-based buffer overflow vulnerability in WAVLINK QUANTUM D3G/WL-WN530HG3 firmware M30HG3_V240730, and possibly other wavlink models allows attackers to execute arbitrary code via crafted referrer value POST to login.cgi.	N/A	More Details
CVE-2025-34294	Wazuh's File Integrity Monitoring (FIM), when configured with automatic threat removal, contains a time-of-check/time-of-use (TOCTOU) race condition that can allow a local, low-privileged attacker to cause the Wazuh service (running as NT AUTHORITY\SYSTEM) to delete attacker-controlled files or paths. The root cause is insufficient synchronization and lack of robust final-path validation in the threat-removal workflow: the agent records an active-response action and proceeds to perform deletion without guaranteeing the deletion target is the originally intended file. This can result in SYSTEM-level arbitrary file or folder deletion and consequent local privilege escalation. Wazuh made an attempted fix via pull request 8697 on 2025-07-10, but that change was incomplete.	N/A	More Details
CVE-2025-62801	FastMCP is the standard framework for building MCP applications. Versions prior to 2.13.0, a command-injection vulnerability lets any attacker who can influence the server_name field of an MCP execute arbitrary OS commands on Windows hosts that run fastmcp install cursor. This vulnerability is fixed in 2.13.0.	N/A	More Details
CVE-2025-62800	FastMCP is the standard framework for building MCP applications. Versions prior to 2.13.0 have a reflected cross-site scripting vulnerability in the OAuth client callback page (oauth_callback.py) where unescaped user-controlled values are inserted into the generated HTML, allowing arbitrary JavaScript execution in the callback server origin. The issue is fixed in version 2.13.0.	N/A	More Details
CVE-2025-61598	Discourse is an open source discussion platform. Version before 3.6.2 and 3.6.0.beta2, default Cache-Control response header with value no-store, no-cache was missing from error responses. This may caused unintended caching of those responses by proxies potentially leading to cache poisoning attacks. This vulnerability is fixed in 3.6.2 and 3.6.0.beta2.	N/A	More Details
CVE-2025-43017	HP ThinPro 8.1 System management application failed to verify user's true id. HP has released HP ThinPro 8.1 SP8, which includes updates to mitigate potential vulnerabilities.	N/A	More Details
CVE-2025-61235	An issue was discovered in Dataphone A920 v2025.07.161103. A custom packet based on public documentation can be crafted, where some fields can contain arbitrary or trivial data. Normally, such data should cause the device to reject the packet. However, due to a lack of validation, the device accepts it with no authetication and triggers the functionality instead.	N/A	More Details
CVE-2025-12425	Local Privilege Escalation.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5 .	N/A	More Details
CVE-2025-12424	Privilege Escalation through SUID-bit Binary.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5 .	N/A	More Details
CVE-2025-12423	Protocol manipulation might lead to denial of service.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5 .	N/A	More Details
CVE-2025-60805	An issue was discovered in BESSystem BES Application Server thru 9.5.x allowing unauthorized attackers to gain sensitive information via the "pre-resource" option in bes-web.xml.	N/A	More Details
CVE-2025-60800	Incorrect access control in the /jshERP-boot/user/info interface of jshERP up to commit 90c411a allows attackers to access sensitive information via a crafted GET request.	N/A	More Details
CVE-2025-60355	zhangyd-c OneBlog before 2.3.9 was vulnerable to SSTI (Server-Side Template Injection) via FreeMarker templates.	N/A	More Details
CVE-2025-60354	Unauthorized modification of arbitrary articles vulnerability exists in blog-vue-springboot.	N/A	More Details
CVE-2025-12422	Vulnerable Upgrade Feature (Arbitrary File Write) may lead to obtaining super user permissions on board.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-54605	Bitcoin Core through 29.0 allows Uncontrolled Resource Consumption (issue 2 of 2).	N/A	More Details
CVE-2025-54604	Bitcoin Core through 29.0 allows Uncontrolled Resource Consumption (issue 1 of 2).	N/A	More Details
CVE-2025-61155	Hotta Studio GameDriverX64.sys 7.23.4.7, a signed kernel-mode anti-cheat driver, allows local attackers to cause a denial of service by crashing arbitrary processes via sending crafted IOCTL requests.	N/A	More Details
CVE-2025-60858	Reolink Video Doorbell Wi-Fi DB_566128M5MP_W stores and transmits DDNS credentials in plaintext within its configuration and update scripts, allowing attackers to intercept or extract sensitive information.	N/A	More Details

CVE-2025-60349	An issue was discovered in Prevx v3.0.5.220 allowing attackers to cause a denial of service via sending IOCTL code 0x22E044 to the pxscan.sys driver. Any processes listed under registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\pxscan\Files will be terminated.	N/A	More Details
CVE-2025-56399	alexusmai laravel-file-manager 3.3.1 and before allows an authenticated attacker to achieve Remote Code Execution (RCE) through a crafted file upload. A file with a '.png` extension containing PHP code can be uploaded via the file manager interface. Although the upload appears to fail client-side validation, the file is still saved on the server. The attacker can then use the rename API to change the file extension to `.php`, and upon accessing it via a public URL, the server executes the embedded code.	N/A	More Details
CVE-2025-12380	Starting with Firefox 142, it was possible for a compromised child process to trigger a use-after-free in the GPU or browser process using WebGPU-related IPC calls. This may have been usable to escape the child process sandbox. This vulnerability affects Firefox < 144.0.2.	N/A	More Details
CVE-2025-1037	By making minor configuration changes to the TropOS 4th Gen device, an authenticated user with the ability to run user level shell commands can enable access via secure shell (SSH) to an unrestricted root shell. This is possible through abuse of a particular set of scripts and executables that allow for certain commands to be run as root from an unprivileged context.	N/A	More Details
CVE-2025-40040	In the Linux kernel, the following vulnerability has been resolved: mm/ksm: fix flag-dropping behavior in ksm_madvise syzkaller discovered the following crash: (kernel BUG) [44.607039] ------------[cut here]------------ [44.607422] kernel BUG at mm/userfaultfd.c:2067! [44.608148] Oops: invalid opcode: 0000 [#1] SMP DEBUG_PAGEALLOC KASAN NOPTI [44.608814] CPU: 1 UID: 0 PID: 2475 Comm: reproducer Not tainted 6.16.0-rc6 #1 PREEMPT(none) [44.609635] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [44.610695] RIP: 0010:userfaultfd_release_all+0x3a8/0x460 <snip other registers, drop unreliable trace> [44.617726] Call Trace: [44.617926] <TASK> [44.619284] userfaultfd_release+0xef/0x1b0 [44.620976] __fput+0x3f9/0xb60 [44.621240] fput_close_sync+0x110/0x210 [44.622222] __x64_sys_close+0x8f/0x120 [44.622530] do_syscall_64+0x5b/0x2f0 [44.622840] entry_SYSCALL_64_after_hwframe+0x76/0x7e [44.623244] RIP: 0033:0x7f365bb3f227 Kernel panics because it detects UFFD inconsistency during userfaultfd_release_all(). Specifically, a VMA which has a valid pointer to vma->vm_userfaultfd_ctx, but no UFFD flags in vma->vm_flags. The inconsistency is caused in ksm_madvise(): when user calls madvise() with MADV_UNMEARGEABLE on a VMA that is registered for UFFD in MINOR mode, it accidentally clears all flags stored in the upper 32 bits of vma->vm_flags. Assuming x86_64 kernel build, unsigned long is 64-bit and unsigned int and int are 32-bit wide. This setup causes the following mishap during the &= ~VM_MERGEABLE assignment. VM_MERGEABLE is a 32-bit constant of type unsigned int, 0x8000'0000. After ~ is applied, it becomes 0x7fff'ffff unsigned int, which is then promoted to unsigned long before the & operation. This promotion fills upper 32 bits with leading 0s, as we're doing unsigned conversion (and even for a signed conversion, this wouldn't help as the leading bit is 0). & operation thus ends up AND-ing vm_flags with 0x0000'0000'7fff'ffff instead of intended 0xffff'ffff'7fff'ffff and hence accidentally clears the upper 32-bits of its value. Fix it by changing `VM_MERGEABLE` constant to unsigned long, using the BIT() macro. Note: other VM_* flags are not affected: This only happens to the VM_MERGEABLE flag, as the other VM_* flags are all constants of type int and after ~ operation, they end up with leading 1 and are thus converted to unsigned long with leading 1s. Note 2: After commit 31defc3b01d9 ("userfaultfd: remove (VM_)BUG_ON()s"), this is no longer a kernel BUG, but a WARNING at the same place: [45.595973] WARNING: CPU: 1 PID: 2474 at mm/userfaultfd.c:2067 but the root-cause (flag-drop) remains the same. [akpm@linux-foundation.org: rust bindgen wasn't able to handle BIT(), from Miguel]	N/A	More Details
CVE-2025-40051	In the Linux kernel, the following vulnerability has been resolved: vhost: vringh: Modify the return value check The return value of copy_from_iter and copy_to_iter can't be negative, check whether the copied lengths are equal.	N/A	More Details
CVE-2025-40060	In the Linux kernel, the following vulnerability has been resolved: coresight: trbe: Return NULL pointer for allocation failures When the TRBE driver fails to allocate a buffer, it currently returns the error code "-ENOMEM". However, the caller etm_setup_aux() only checks for a NULL pointer, so it misses the error. As a result, the driver continues and eventually causes a kernel panic. Fix this by returning a NULL pointer from arm_trbe_alloc_buffer() on allocation failures. This allows that the callers can properly handle the failure.	N/A	More Details
CVE-2025-40059	In the Linux kernel, the following vulnerability has been resolved: coresight: Fix incorrect handling for return value of devm_kzalloc The return value of devm_kzalloc could be an null pointer, use "!desc.pdata" to fix incorrect handling return value of devm_kzalloc.	N/A	More Details
CVE-2025-40058	In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Disallow dirty tracking if incoherent page walk Dirty page tracking relies on the IOMMU atomically updating the dirty bit in the paging-structure entry. For this operation to succeed, the paging- structure memory must be coherent between the IOMMU and the CPU. In another word, if the iommu page walk is incoherent, dirty page tracking doesn't work. The Intel VT-d specification, Section 3.10 "Snoop Behavior" states: "Remapping hardware encountering the need to atomically update A/EA/D bits in a paging-structure entry that is not snooped will result in a non- recoverable fault." To prevent an IOMMU from being incorrectly configured for dirty page tracking when it is operating in an incoherent mode, mark SSADS as supported only when both ecap_slads and ecap_smpwc are supported.	N/A	More Details
CVE-2025-40057	In the Linux kernel, the following vulnerability has been resolved: ptp: Add a upper bound on max_vclocks syzbot reported WARNING in max_vclocks_store. This occurs when the argument max is too large for kcalloc to handle. Extend the guard to guard against values that are too large for kcalloc	N/A	More Details
CVE-2025-40056	In the Linux kernel, the following vulnerability has been resolved: vhost: vringh: Fix copy_to_iter return value check The return value of copy_to_iter can't be negative, check whether the copied length is equal to the requested length instead of checking for negative values.	N/A	More Details
CVE-2025-40055	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix double free in user_cluster_connect() user_cluster_disconnect() frees "conn->cc_private" which is "lc" but then the error handling frees "lc" a second time. Set "lc" to NULL on this path to avoid a double free.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix UAF issue in f2fs_merge_page_bio() As JY reported in bugzilla [1], Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 pc : [0xffffffe51d249484] f2fs_is_cp_guaranteed+0x70/0x98 lr : [0xffffffe51d24adbc] f2fs_merge_page_bio+0x520/0x6d4 CPU: 3 UID: 0 PID: 6790 Comm: kworker/u16:3 Tainted: P B W OE 6.12.30-android16-5-maybe-dirty-4k #1 5f7701c9cbf727d1eebe77c89bbbeb3371e895e5		

CVE-2025-40054	Tainted: [P]=PROPRIETARY_MODULE, [B]=BAD_PAGE, [W]=WARN, [O]=OOT_MODULE, [E]=UNSIGNED_MODULE Workqueue: writeback wb_workfn (flush-254:49) Call trace: f2fs_is_cp_guaranteed+0x70/0x98 f2fs_inplace_write_data+0x174/0x2f4 f2fs_do_write_data_page+0x214/0x81c f2fs_write_single_data_page+0x28c/0x764 f2fs_write_data_pages+0x78c/0xce4 do_writepages+0xe8/0x2fc __writeback_single_inode+0x4c/0x4b4 writeback_sb_inodes+0x314/0x540 __writeback_inodes_wb+0xa4/0xf4 wb_writeback+0x160/0x448 wb_workfn+0x2f0/0x5dc process_scheduled_works+0x1c8/0x458 worker_thread+0x334/0x3f0 kthread+0x118/0x1ac ret_from_fork+0x10/0x20 [1] https://bugzilla.kernel.org/show_bug.cgi?id=220575 The panic was caused by UAF issue w/ below race condition: kworker - writepages - f2fs_write_cache_pages - f2fs_write_single_data_page - f2fs_do_write_data_page - f2fs_inplace_write_data - f2fs_merge_page_bio - add_inu_page : cache page #1 into bio & cache bio in io->bio_list - f2fs_write_single_data_page - f2fs_do_write_data_page - f2fs_inplace_write_data - f2fs_merge_page_bio - add_inu_page : cache page #2 into bio which is linked in io->bio_list write - f2fs_write_begin : write page #1 - f2fs_folio_wait_writeback - f2fs_submit_merged_ipu_write - f2fs_submit_write_bio : submit bio which inclues page #1 and #2 software IRQ - f2fs_write_end_io - fscrypt_free_bounce_page : freed bounced page which belongs to page #2 - inc_page_count(, WB_DATA_TYPE(data_folio), false) : data_folio points to fio->encrypted_page the bounced page can be freed before accessing it in f2fs_is_cp_guarantee() It can reproduce w/ below testcase: Run below script in shell #1: for ((i=1;i>0;i++)) do xfs_io -f /mnt/f2fs/enc/file \ -c "pwrite 0 32k" -c "fdatasync" Run below script in shell #2: for ((i=1;i>0;i++)) do xfs_io -f /mnt/f2fs/enc/file \ -c "pwrite 0 32k" -c "fdatasync" So, in f2fs_merge_page_bio(), let's avoid using fio->encrypted_page after commit page into internal ipu cache.	N/A	More Details
CVE-2025-40053	In the Linux kernel, the following vulnerability has been resolved: net: dlink: handle copy_thresh allocation failure The driver did not handle failure of `netdev_alloc_skb_ip_align()`. If the allocation failed, dereferencing `skb->protocol` could lead to a NULL pointer dereference. This patch tries to allocate `skb`. If the allocation fails, it falls back to the normal path. Tested-on: D-Link DGE-550T Rev-A3	N/A	More Details
CVE-2025-40052	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix crypto buffers in non-linear memory The crypto API, through the scatterlist API, expects input buffers to be in linear memory. We handle this with the cifs_sg_set_buf() helper that converts vmalloc'd memory to their corresponding pages. However, when we allocate our aead_request buffer (@creq in smb2ops.c::crypt_message()), we do so with kvzalloc(), which possibly puts aead_request->__ctx in vmalloc area. AEAD algorithm then uses ->__ctx for its private/internal data and operations, and uses sg_set_buf() for such data on a few places. This works fine as long as @creq falls into kmalloc zone (small requests) or vmalloc'd memory is still within linear range. Tasks' stacks are vmalloc'd by default (CONFIG_VMAP_STACK=y), so too many tasks will increment the base stacks' addresses to a point where virt_addr_valid(buf) will fail (BUG() in sg_set_buf()) when that happens. In practice: too many parallel reads and writes on an encrypted mount will trigger this bug. To fix this, always alloc @creq with kmalloc() instead. Also drop the @sensitive_size variable/arguments since kfree_sensitive() doesn't need it. Backtrace: [945.272081] ------------[cut here]------------ [945.272774] kernel BUG at include/linux/scatterlist.h:209! [945.273520] Oops: invalid opcode: 0000 [#1] SMP DEBUG_PAGEALLOC NOPTI [945.274412] CPU: 7 UID: 0 PID: 56 Comm: kworker/u33:0 Kdump: loaded Not tainted 6.15.0-lku-11779-g8e9d6efccdd7-dirty #1 PREEMPT(voluntary) [945.275736] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.16.3-2-gc13ff2cd-prebuilt.qemu.org 04/01/2014 [945.276877] Workqueue: writeback wb_workfn (flush-cifs-2) [945.277457] RIP: 0010:crypto_gcm_init_common+0x1f9/0x220 [945.278018] Code: b0 00 00 00 48 83 c4 08 5b 5d 41 5c 41 5d 41 5e 41 5f c3 cc cc cc cc 48 c7 c0 00 00 00 80 48 2b 05 5c 58 e5 00 e9 58 ff ff ff <0f> 0b 0f 0b 0f 0b 0f 0b 0f 0b 48 c7 04 24 01 00 00 00 48 8b [945.279992] RSP: 0018:ffffc90000a27360 EFLAGS: 00010246 [945.280578] RAX: 0000000000000000 RBX: ffffc90001d85060 RCX: 0000000000000030 [945.281376] RDX: 0000000000080000 RSI: 0000000000000000 RDI: ffffc90081d85070 [945.282145] RBP: ffffc90001d85010 R08: ffffc90001d85000 R09: 0000000000000000 [945.282898] R10: ffffc90001d85090 R11: 0000000000001000 R12: ffffc90001d85070 [945.283656] R13: ffff888113522948 R14: ffffc90001d85060 R15: ffffc90001d85010 [945.284407] FS: 0000000000000000(0000) GS:ffff8882e66cf000(0000) knlGS:0000000000000000 [945.285262] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [945.285884] CR2: 00007fa7ffdd31f4 CR3: 000000010540d000 CR4: 0000000000350ef0 [945.286683] Call Trace: [945.286952] <TASK> [945.287184] ? crypt_message+0x33f/0xad0 [cifs] [945.287719] crypto_gcm_encrypt+0x36/0xe0 [945.288152] crypt_message+0x54a/0xad0 [cifs] [945.288724] smb3_init_transform_rq+0x277/0x300 [cifs] [945.289300] smb_send_rqst+0xa3/0x160 [cifs] [945.289944] cifs_call_async+0x178/0x340 [cifs] [945.290514] ? __pfx_smb2_writev_callback+0x10/0x10 [cifs] [945.291177] smb2_async_writev+0x3e3/0x670 [cifs] [945.291759] ? find_held_lock+0x32/0x90 [945.292212] ? netfs_advance_write+0xf2/0x310 [945.292723] netfs_advance_write+0xf2/0x310 [945.293210] netfs_write_folio+0x346/0xcc0 [945.293689] ? __pfx__raw_spin_unlock_irq+0x10/0x10 [945.294250] netfs_writepages+0x117/0x460 [945.294724] do_writepages+0xbe/0x170 [945.295152] ? find_held_lock+0x32/0x90 [945.295600] ? kvm_sched_clock_read+0x11/0x20 [945.296103] __writeback_single_inode+0x56/0x4b0 [945.296643] writeback_sb_inodes+0x229/0x550 [945.297140] __writeback_inodes_wb+0x4c/0xe0 [945.297642] wb_writeback+0x2f1/0x3f0 [945.298069] wb_workfn+0x300/0x490 [945.298472] process_one_work+0x1fe/0x590 [945.298949] worker_thread+0x1ce/0x3c0 [945.299397] ? __pfx_worker_thread+0x10/0x10 [945.299900] kthr ---truncated---	N/A	More Details
CVE-2025-40050	In the Linux kernel, the following vulnerability has been resolved: bpf: Skip scalar adjustment for BPF_NEG if dst is a pointer In check_alu_op(), the verifier currently calls check_reg_arg() and adjust_scalar_min_max_vals() unconditionally for BPF_NEG operations. However, if the destination register holds a pointer, these scalar adjustments are unnecessary and potentially incorrect. This patch adds a check to skip the adjustment logic when the destination register contains a pointer.	N/A	More Details
CVE-2025-1036	Command injection vulnerability exists in the “Logging” page of the web-based configuration utility. An authenticated user with low privileged network access for the configuration utility can execute arbitrary commands on the underlying OS to obtain root SSH access to the TropOS 4th Gen device.	N/A	More Details
CVE-2025-40049	In the Linux kernel, the following vulnerability has been resolved: Squashfs: fix uninit-value in squashfs_get_parent Syzkaller reports a "KMSAN: uninit-value in squashfs_get_parent" bug. This is caused by open_by_handle_at() being called with a file handle containing an invalid parent inode number. In particular the inode number is that of a symbolic link, rather than a directory. Squashfs_get_parent() gets called with that symbolic link inode, and accesses the parent member field. unsigned int parent_ino = squashfs_i(inode)->parent; Because non-directory inodes in Squashfs do not have a parent value, this is uninitialised, and this causes an uninitialised value access. The fix is to initialise parent with the invalid inode 0, which will cause an EINVAL error to be returned. Regular inodes used to share the parent field with the block_list_start field. This is removed in this commit to enable the parent field to contain the invalid inode number 0.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: uio_hv_generic: Let userspace take care of interrupt mask Remove the logic to set interrupt mask by default in uio_hv_generic driver as the interrupt mask value is supposed to be controlled completely by the user space. If the mask bit gets changed by the driver, concurrently with user mode operating on		

CVE-2025-40048	the ring, the mask bit may be set when it is supposed to be clear, and the user-mode driver will miss an interrupt which will cause a hang. For eg- when the driver sets inbound ring buffer interrupt mask to 1, the host does not interrupt the guest on the UIO VMBus channel. However, setting the mask does not prevent the host from putting a message in the inbound ring buffer. So let’s assume that happens, the host puts a message into the ring buffer but does not interrupt. Subsequently, the user space code in the guest sets the inbound ring buffer interrupt mask to 0, saying “Hey, I’m ready for interrupts”. User space code then calls pread() to wait for an interrupt. Then one of two things happens: * The host never sends another message. So the pread() waits forever. * The host does send another message. But because there’s already a message in the ring buffer, it doesn’t generate an interrupt. This is the correct behavior, because the host should only send an interrupt when the inbound ring buffer transitions from empty to not-empty. Adding an additional message to a ring buffer that is not empty is not supposed to generate an interrupt on the guest. Since the guest is waiting in pread() and not removing messages from the ring buffer, the pread() waits forever. This could be easily reproduced in hv_fcopy_uio_daemon if we delay setting interrupt mask to 0. Similarly if hv_uio_channel_cb() sets the interrupt_mask to 1, there’s a race condition. Once user space empties the inbound ring buffer, but before user space sets interrupt_mask to 0, the host could put another message in the ring buffer but it wouldn’t interrupt. Then the next pread() would hang. Fix these by removing all instances where interrupt_mask is changed, while keeping the one in set_event() unchanged to enable userspace control the interrupt mask by writing 0/1 to /dev/uioX.	N/A	More Details
CVE-2025-40047	In the Linux kernel, the following vulnerability has been resolved: io_uring/waitid: always prune wait queue entry in io_waitid_wait() For a successful return, always remove our entry from the wait queue entry list. Previously this was skipped if a cancelation was in progress, but this can race with another invocation of the wait queue entry callback.	N/A	More Details
CVE-2025-40046	In the Linux kernel, the following vulnerability has been resolved: io_uring/zcrx: fix overshooting recv limit It's reported that sometimes a zcrx request can receive more than was requested. It's caused by io_zcrx_recv_skb() adjusting desc->count for all received buffers including frag lists, but then doing recursive calls to process frag list skbs, which leads to desc->count double accounting and underflow.	N/A	More Details
CVE-2025-40045	In the Linux kernel, the following vulnerability has been resolved: ASoC: codecs: wcd937x: set the comp soundwire port correctly For some reason we endup with setting soundwire port for HPHL_COMP and HPHR_COMP as zero, this can potentially result in a memory corruption due to accessing and setting -1 th element of port_map array.	N/A	More Details
CVE-2025-40044	In the Linux kernel, the following vulnerability has been resolved: fs: udf: fix OOB read in lengthAllocDescs handling When parsing Allocation Extent Descriptor, lengthAllocDescs comes from on-disk data and must be validated against the block size. Crafted or corrupted images may set lengthAllocDescs so that the total descriptor length (sizeof(allocExtDesc) + lengthAllocDescs) exceeds the buffer, leading udf_update_tag() to call crc_itu_t() on out-of-bounds memory and trigger a KASAN use-after-free read. BUG: KASAN: use-after-free in crc_itu_t+0x1d5/0x2b0 lib/crc-itu-t.c:60 Read of size 1 at addr ffff888041e7d000 by task syz-executor317/5309 CPU: 0 UID: 0 PID: 5309 Comm: syz-executor317 Not tainted 6.12.0-rc4-syzkaller-00261-g850925a8133c #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2~bpo12+1 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 crc_itu_t+0x1d5/0x2b0 lib/crc-itu-t.c:60 udf_update_tag+0x70/0x6a0 fs/udf/misc.c:261 udf_write_aext+0x4d8/0x7b0 fs/udf/inode.c:2179 extent_trunc+0x2f7/0x4a0 fs/udf/truncate.c:46 udf_truncate_tail_extent+0x527/0x7e0 fs/udf/truncate.c:106 udf_release_file+0xc1/0x120 fs/udf/file.c:185 __fput+0x23f/0x880 fs/file_table.c:431 task_work_run+0x24f/0x310 kernel/task_work.c:239 exit_task_work include/linux/task_work.h:43 [inline] do_exit+0xa2f/0x28e0 kernel/exit.c:939 do_group_exit+0x207/0x2c0 kernel/exit.c:1088 __do_sys_exit_group kernel/exit.c:1099 [inline] __se_sys_exit_group kernel/exit.c:1097 [inline] __x64_sys_exit_group+0x3f/0x40 kernel/exit.c:1097 x64_sys_call+0x2634/0x2640 arch/x86/include/generated/asm/syscalls_64.h:232 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> Validate the computed total length against epos->bh->b_size. Found by Linux Verification Center (linuxtesting.org) with Syzkaller.	N/A	More Details
CVE-2025-40043	In the Linux kernel, the following vulnerability has been resolved: net: nfc: nci: Add parameter validation for packet data Syzbot reported an uninitialized value bug in nci_init_req, which was introduced by commit 5aca7966d2a7 ("Merge tag 'perf-tools-fixes-for-v6.17-2025-09-16' of git://git.kernel.org/pub/scm/linux/kernel/git/perf/perf-tools"). This bug arises due to very limited and poor input validation that was done at nic_valid_size(). This validation only validates the skb->len (directly reflects size provided at the userspace interface) with the length provided in the buffer itself (interpreted as NCI_HEADER). This leads to the processing of memory content at the address assuming the correct layout per what opcode requires there. This leads to the accesses to buffer of `skb_buff->data` which is not assigned anything yet. Following the same silent drop of packets of invalid sizes at `nic_valid_size()`, add validation of the data in the respective handlers and return error values in case of failure. Release the skb if error values are returned from handlers in `nci_nft_packet` and effectively do a silent drop Possible TODO: because we silently drop the packets, the call to `nci_request` will be waiting for completion of request and will face timeouts. These timeouts can get excessively logged in the dmesg. A proper handling of them may require to export `nci_request_cancel` (or propagate error handling from the nft packets handlers).	N/A	More Details
CVE-2025-40042	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix race condition in kprobe initialization causing NULL pointer dereference There is a critical race condition in kprobe initialization that can lead to NULL pointer dereference and kernel crash. [1135630.084782] Unable to handle kernel paging request at virtual address 0000710a04630000 ... [1135630.260314] pstate: 404003c9 (nZcv DAIF +PAN -UAO) [1135630.269239] pc : kprobe_perf_func+0x30/0x260 [1135630.277643] lr : kprobe_dispatcher+0x44/0x60 [1135630.286041] sp : ffffaeff4977fa40 [1135630.293441] x29: ffffaeff4977fa40 x28: ffffaf015340e400 [1135630.302837] x27: 0000000000000000 x26: 0000000000000000 [1135630.312257] x25: ffffaf029ed108a8 x24: ffffaf015340e528 [1135630.321705] x23: ffffaeff4977fc50 x22: ffffaeff4977fc50 [1135630.331154] x21: 0000000000000000 x20: ffffaeff4977fc50 [1135630.340586] x19: ffffaf015340e400 x18: 0000000000000000 [1135630.349985] x17: 0000000000000000 x16: 0000000000000000 [1135630.359285] x15: 0000000000000000 x14: 0000000000000000 [1135630.368445] x13: 0000000000000000 x12: 0000000000000000 [1135630.377473] x11: 0000000000000000 x10: 0000000000000000 [1135630.386411] x9 : 0000000000000000 x8 : 0000000000000000 [1135630.395252] x7 : 0000000000000000 x6 : 0000000000000000 [1135630.403963] x5 : 0000000000000000 x4 : 0000000000000000 [1135630.412545] x3 : 0000710a04630000 x2 : 0000000000000006 [1135630.421021] x1 : ffffaeff4977fc50 x0 : 0000710a04630000 [1135630.429410] Call trace: [1135630.434828] kprobe_perf_func+0x30/0x260 [1135630.441661] kprobe_dispatcher+0x44/0x60 [1135630.448396] aggr_pre_handler+0x70/0xc8 [1135630.454959] kprobe_breakpoint_handler+0x140/0x1e0 [1135630.462435] brk_handler+0xbc/0xd8 [1135630.468437] do_debug_exception+0x84/0x138 [1135630.475074] el1_dbg+0x18/0x8c [1135630.480582] security_file_permission+0x0/0xd0 [1135630.487426] vfs_write+0x70/0x1c0 [1135630.493059]	N/A	More Details

	ksys_write+0x5c/0xc8 [1135630.498638] __arm64_sys_write+0x24/0x30 [1135630.504821] el0_svc_common+0x78/0x130 [1135630.510838] el0_svc_handler+0x38/0x78 [1135630.516834] el0_svc+0x8/0x1b0 kernel/trace/trace_kprobe.c: 1308 0xffff3df8995039ec <kprobe_perf_func+0x2c>: ldr x21, [x24,#120] include/linux/compiler.h: 294 0xffff3df8995039f0 <kprobe_perf_func+0x30>: ldr x1, [x21,x0] kernel/trace/trace_kprobe.c 1308: head = this_cpu_ptr(call->perf_events); 1309: if (hlist_empty(head)) 1310: return 0; crash> struct trace_event_call -o struct trace_event_call { ... [120] struct hlist_head *perf_events; //(call->perf_event) ... } crash> struct trace_event_call ffffaf015340e528 struct trace_event_call { ... perf_events = 0xffff0ad5fa89f088, //this value is correct, but x21 = 0 ... } Race Condition Analysis: The race occurs between kprobe activation and perf_events initialization: CPU0 CPU1 ==== ==== perf_kprobe_init perf_trace_event_init tp_event->perf_events = list;(1) tp_event->class->reg (2)← KPROBE ACTIVE Debug exception triggers ... kprobe_dispatcher kprobe_perf_func (tk->tp.flags & TP_FLAG_PROFILE) head = this_cpu_ptr(call->perf_events)(3) (perf_events is still NULL) Problem: 1. CPU0 executes (1) assigning tp_event->perf_events = list 2. CPU0 executes (2) enabling kprobe functionality via class->reg() 3. CPU1 triggers and reaches kprobe_dispatcher 4. CPU1 checks TP_FLAG_PROFILE - condition passes (step 2 completed) 5. CPU1 calls kprobe_perf_func() and crashes at (3) because call->perf_events is still NULL CPU1 sees that kprobe functionality is enabled but does not see that perf_events has been assigned. Add pairing read an ---truncated---		
CVE-2025-40041	In the Linux kernel, the following vulnerability has been resolved: LoongArch: BPF: Sign-extend struct ops return values properly The ns_bpf_qdisc selftest triggers a kernel panic: Oops[#1]: CPU 0 Unable to handle kernel paging request at virtual address 0000000000741d58, era == 90000000851b5ac0, ra == 90000000851b5aa4 CPU: 0 UID: 0 PID: 449 Comm: test_progs Tainted: G OE 6.16.0+ #3 PREEMPT(full) Tainted: [O]=OOT_MODULE, [E]=UNSIGNED_MODULE Hardware name: QEMU QEMU Virtual Machine, BIOS unknown 2/2/2022 pc 90000000851b5ac0 ra 90000000851b5aa4 tp 90000001076b8000 sp 90000001076bb600 a0 0000000000741ce8 a1 0000000000000001 a2 90000001076bb5c0 a3 0000000000000008 a4 90000001004c4620 a5 9000000100741ce8 a6 0000000000000000 a7 0100000000000000 t0 0000000000000010 t1 0000000000000000 t2 9000000104d24d30 t3 0000000000000001 t4 4f2317da8a7e08c4 t5 ffffffefffc002f00 t6 90000001004c4620 t7 ffffffffc61c5b3d t8 0000000000000000 u0 0000000000000001 s9 0000000000000050 s0 90000001075bc800 s1 0000000000000040 s2 900000010597c400 s3 0000000000000008 s4 90000001075bc880 s5 90000001075bc8f0 s6 0000000000000000 s7 0000000000741ce8 s8 0000000000000000 ra: 90000000851b5aa4 __qdisc_run+0xac/0x8d8 ERA: 90000000851b5ac0 __qdisc_run+0xc8/0x8d8 CRMD: 000000b0 (PLV0 -IE -DA +PG DACF=CC DACM=CC -WE) PRMD: 00000004 (PPLV0 +PIE -PWE) EUEN: 00000007 (+FPE +SXE +ASXE -BTE) ECFG: 00071c1d (LIE=0,2-4,10-12 VS=7) ESTAT: 00010000 [PIL] (IS= ECode=1 EsubCode=0) BADV: 0000000000741d58 PRID: 0014c010 (Loongson-64bit, Loongson-3A5000) Modules linked in: bpf_testmod(OE) [last unloaded: bpf_testmod(OE)] Process test_progs (pid: 449, threadinfo=000000009af02b3a, task=00000000e9ba4956) Stack : 0000000000000000 90000001075bc8ac 90000000869524a8 9000000100741ce8 90000001075bc800 9000000100415300 90000001075bc8ac 0000000000000000 900000010597c400 900000008694a000 0000000000000000 9000000105b59000 90000001075bc800 9000000100741ce8 0000000000000050 9000000008513000c 9000000086936000 0000000100094d4c ffffffff400676208 0000000000000000 9000000105b59000 900000008694a000 9000000086bf0dc0 9000000105b59000 9000000086bf0d68 9000000085147010 90000001075be788 0000000000000000 9000000086bf0f98 0000000000000001 0000000000000010 9000000006015840 0000000000000000 9000000086be6c40 0000000000000000 0000000000000000 0000000000000000 4f2317da8a7e08c4 0000000000000101 4f2317da8a7e08c4 ... Call Trace: [<90000000851b5ac0>] __qdisc_run+0xc8/0x8d8 [<9000000085130008>] __dev_queue_xmit+0x578/0x10f0 [<90000000853701c0>] ip6_finish_output2+0x2f0/0x950 [<9000000085374bc8>] ip6_finish_output+0x2b8/0x448 [<900000085370b24>] ip6_xmit+0x304/0x858 [<90000000853c4438>] inet6_csk_xmit+0x100/0x170 [<90000000852b32f0>] __tcp_transmit_skb+0x490/0xdd0 [<90000000852b47fc>] tcp_connect+0xbcc/0x1168 [<90000000853b9088>] tcp_v6_connect+0x580/0x8a0 [<90000000852e7738>] __inet_stream_connect+0x170/0x480 [<90000000852e7a98>] inet_stream_connect+0x50/0x88 [<90000000850f2814>] __sys_connect+0xe4/0x110 [<90000000850f2858>] sys_connect+0x18/0x28 [<9000000085520c94>] do_syscall+0x94/0x1a0 [<9000000083df1fb8>] handle_syscall+0xb8/0x158 Code: 4001ad80 2400873f 2400832d <240073cc> 001137ff 001133ff 6407b41f 001503cc 0280041d ---[end trace 0000000000000000]--- The bpf_fifo_dequeue prog returns a skb which is a pointer. The pointer is treated as a 32bit value and sign extend to 64bit in epilogue. This behavior is right for most bpf prog types but wrong for struct ops which requires LoongArch ABI. So let's sign extend struct ops return values according to the LoongArch ABI ([1]) and return value spec in function model. [1]: https://loongson.github.io/LoongArch-Documentation/LoongArch-ELF-ABI-EN.html	N/A	More Details
CVE-2025-40061	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Fix race in do_task() when draining When do_task() exhausts its iteration budget (!ret), it sets the state to TASK_STATE_IDLE to reschedule, without a secondary check on the current task->state. This can overwrite the TASK_STATE_DRAINING state set by a concurrent call to rxe_cleanup_task() or rxe_disable_task(). While state changes are protected by a spinlock, both rxe_cleanup_task() and rxe_disable_task() release the lock while waiting for the task to finish draining in the while(!is_done(task)) loop. The race occurs if do_task() hits its iteration limit and acquires the lock in this window. The cleanup logic may then proceed while the task incorrectly reschedules itself, leading to a potential use-after-free. This bug was introduced during the migration from tasklets to workqueues, where the special handling for the draining case was lost. Fix this by restoring the original pre-migration behavior. If the state is TASK_STATE_DRAINING when iterations are exhausted, set cont to 1 to force a new loop iteration. This allows the task to finish its work, so that a subsequent iteration can reach the switch statement and correctly transition the state to TASK_STATE_DRAINED, stopping the task as intended.	N/A	More Details
CVE-2025-40062	In the Linux kernel, the following vulnerability has been resolved: crypto: hisilicon/qm - set NULL to qm->debug.qm_diff_regs When the initialization of qm->debug.acc_diff_reg fails, the probe process does not exit. However, after qm->debug.qm_diff_regs is freed, it is not set to NULL. This can lead to a double free when the remove process attempts to free it again. Therefore, qm->debug.qm_diff_regs should be set to NULL after it is freed.	N/A	More Details
CVE-2025-40063	In the Linux kernel, the following vulnerability has been resolved: crypto: comp - Use same definition of context alloc and free ops In commit 42d9f6c77479 ("crypto: acomp - Move scomp stream allocation code into acomp"), the crypto_acomp_streams struct was made to rely on having the alloc_ctx and free_ctx operations defined in the same order as the scomp_alg struct. But in that same commit, the alloc_ctx and free_ctx members of scomp_alg may be randomized by structure layout randomization, since they are contained in a pure ops structure (containing only function pointers). If the pointers within scomp_alg are randomized, but those in crypto_acomp_streams are not, then the order may no longer match. This fixes the problem by removing the union from scomp_alg so that both crypto_acomp_streams and scomp_alg will share the same definition of alloc_ctx and free_ctx, ensuring they will always have the same layout.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: smc: Fix use-after-free in __pnet_find_base_ndev(). syzbot reported use-after-free of net_device in __pnet_find_base_ndev(), which was called during connect(). [0] smc_pnet_find_ism_resource() fetches sk_dst_get(sk)->dev and passes down to pnet_find_base_ndev(), where RTNL is held. Then, UAF happened at __pnet_find_base_ndev() when the dev is first used. This means dev had already been freed before		

CVE-2025-40064	acquiring RTNL in pnet_find_base_ndev(). While dev is going away, dst->dev could be swapped with blackhole_netdev, and the dev's refcnt by dst will be released. We must hold dev's refcnt before calling smc_pnet_find_ism_resource(). Also, smc_pnet_find_roce_resource() has the same problem. Let's use __sk_dst_get() and dst_dev_rcu() in the two functions. [0]: BUG: KASAN: use-after-free in __pnet_find_base_ndev+0x1b1/0x1c0 net/smc/smc_pnet.c:926 Read of size 1 at addr ffff888036bac33a by task syz.0.3632/18609 CPU: 1 UID: 0 PID: 18609 Comm: syz.0.3632 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/18/2025 Call Trace: <TASK> dump_stack_lvl+0x189/0x250 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xca/0x240 mm/kasan/report.c:482 kasan_report+0x118/0x150 mm/kasan/report.c:595 __pnet_find_base_ndev+0x1b1/0x1c0 net/smc/smc_pnet.c:926 pnet_find_base_ndev net/smc/smc_pnet.c:946 [inline] smc_pnet_find_ism_by_pnetid net/smc/smc_pnet.c:1103 [inline] smc_pnet_find_ism_resource+0xef/0x390 net/smc/smc_pnet.c:1154 smc_find_ism_device net/smc/af_smc.c:1030 [inline] smc_find_proposal_devices net/smc/af_smc.c:1115 [inline] __smc_connect+0x372/0x1890 net/smc/af_smc.c:1545 smc_connect+0x877/0xd90 net/smc/af_smc.c:1715 __sys_connect_file net/socket.c:2086 [inline] __sys_connect+0x313/0x440 net/socket.c:2105 __do_sys_connect net/socket.c:2111 [inline] __se_sys_connect net/socket.c:2108 [inline] __x64_sys_connect+0x7a/0x90 net/socket.c:2108 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0x3b0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f47cbf8eba9 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f47ccdb1038 EFLAGS: 00000246 ORIG_RAX: 000000000000002a RAX: ffffffffffffffda RBX: 00007f47cc1d5fa0 RCX: 00007f47cbf8eba9 RDX: 0000000000000010 RSI: 0000200000000280 RDI: 000000000000000b RBP: 00007f47cc011e19 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007f47cc1d6038 R14: 00007f47cc1d5fa0 R15: 00007ffc512f8aa8 </TASK> The buggy address belongs to the physical page: page: refcount:0 mapcount:0 mapping:0000000000000000 index:0xffff888036bacd00 pfn:0x36bac flags: 0xfff00000000000(node=0|zone=1|lastcpupid=0x7ff) raw: 00fff00000000000 ffffea0001243d08 ffff8880b863fdc0 0000000000000000 raw: ffff888036bacd00 0000000000000000 00000000ffffffff 0000000000000000 page dumped because: kasan: bad access detected page_owner tracks the page as freed page last allocated via order 2, migratetype Unmovable, gfp_mask 0x446dc0(GFP_KERNEL_ACCOUNT|__GFP_ZERO|__GFP_NOWARN|__GFP_RETRY_MAYFAIL|__GFP_COMP), pid 16741, tgid 16741 (syz-executor), ts 343313197788, free_ts 380670750466 set_page_owner include/linux/page_owner.h:32 [inline] post_alloc_hook+0x240/0x2a0 mm/page_alloc.c:1851 prep_new_page mm/page_alloc.c:1859 [inline] get_page_from_freelist+0x21e4/0x22c0 mm/page_alloc.c:3858 __alloc_frozen_pages_noprof+0x181/0x370 mm/page_alloc.c:5148 alloc_pages_mpol+0x232/0x4a0 mm/mempolicy.c:2416 ___kmalloc_large_node+0x5f/0x1b0 mm/slub.c:4317 __kmalloc_large_node_noprof+0x18/0x90 mm/slub.c:4348 __do_kmalloc_node mm/slub.c:4364 [inline] __kvmalloc_node ---truncated---	N/A	More Details
CVE-2025-9313	An unauthenticated user can connect to a publicly accessible database using arbitrary credentials. The system grants full access to the database by leveraging a previously authenticated connection through a "mmBackup" application. This flaw allows attackers to bypass authentication mechanisms and gain unauthorized access to database with sensitive data. This issue affects Asseco mMedica in versions before 11.9.5.	N/A	More Details
CVE-2025-40082	In the Linux kernel, the following vulnerability has been resolved: hfsplus: fix slab-out-of-bounds read in hfsplus_uni2asc() BUG: KASAN: slab-out-of-bounds in hfsplus_uni2asc+0xa71/0xb90 fs/hfsplus/unicode.c:186 Read of size 2 at addr ffff8880289ef218 by task syz.6.248/14290 CPU: 0 UID: 0 PID: 14290 Comm: syz.6.248 Not tainted 6.16.4 #1 PREEMPT(full) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x116/0x1b0 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xca/0x5f0 mm/kasan/report.c:482 kasan_report+0xca/0x100 mm/kasan/report.c:595 hfsplus_uni2asc+0xa71/0xb90 fs/hfsplus/unicode.c:186 hfsplus_listxattr+0x5b6/0xbd0 fs/hfsplus/xattr.c:738 vfs_listxattr+0xbe/0x140 fs/xattr.c:493 listxattr+0xee/0x190 fs/xattr.c:924 filename_listxattr fs/xattr.c:958 [inline] path_listxattrat+0x143/0x360 fs/xattr.c:988 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xcb/0x4c0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7fe0e9fae16d Code: 02 b8 ff ff ff ff c3 66 0f 1f 44 00 00 f3 0f 1e fa 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007fe0eae67f98 EFLAGS: 00000246 ORIG_RAX: 00000000000000c3 RAX: ffffffffffffffda RBX: 00007fe0ea205fa0 RCX: 00007fe0e9fae16d RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000200000000000 RBP: 00007fe0ea0480f0 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007fe0ea206038 R14: 00007fe0ea205fa0 R15: 00007fe0eae48000 </TASK> Allocated by task 14290: kasan_save_stack+0x24/0x50 mm/kasan/common.c:47 kasan_save_track+0x14/0x30 mm/kasan/common.c:68 poison_kmalloc_redzone mm/kasan/common.c:377 [inline] __kasan_kmalloc+0xaa/0xb0 mm/kasan/common.c:394 kasan_kmalloc include/linux/kasan.h:260 [inline] __do_kmalloc_node mm/slub.c:4333 [inline] __kmalloc_noprof+0x219/0x540 mm/slub.c:4345 kmalloc_noprof include/linux/slab.h:909 [inline] hfsplus_find_init+0x95/0x1f0 fs/hfsplus/bfind.c:21 hfsplus_listxattr+0x331/0xbd0 fs/hfsplus/xattr.c:697 vfs_listxattr+0xbe/0x140 fs/xattr.c:493 listxattr+0xee/0x190 fs/xattr.c:924 filename_listxattr fs/xattr.c:958 [inline] path_listxattrat+0x143/0x360 fs/xattr.c:988 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xcb/0x4c0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f When hfsplus_uni2asc is called from hfsplus_listxattr, it actually passes in a struct hfsplus_attr_unistr*. The size of the corresponding structure is different from that of hfsplus_unistr, so the previous fix (94458781aee6) is insufficient. The pointer on the unicode buffer is still going beyond the allocated memory. This patch introduces two warpper functions hfsplus_uni2asc_xattr_str and hfsplus_uni2asc_str to process two unicode buffers, struct hfsplus_attr_unistr* and struct hfsplus_unistr* respectively. When ustrlen value is bigger than the allocated memory size, the ustrlen value is limited to an safe size.	N/A	More Details
CVE-2025-40081	In the Linux kernel, the following vulnerability has been resolved: perf: arm_spe: Prevent overflow in PERF_IDX2OFF() Cast nr_pages to unsigned long to avoid overflow when handling large AUX buffer sizes (>= 2 GiB).	N/A	More Details
CVE-2025-40080	In the Linux kernel, the following vulnerability has been resolved: nbd: restrict sockets to TCP and UDP Recently, syzbot started to abuse NBD with all kinds of sockets. Commit cf1b2326b734 ("nbd: verify socket is supported during setup") made sure the socket supported a shutdown() method. Explicitely accept TCP and UNIX stream sockets.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: riscv, bpf: Sign extend struct ops return values properly The ns_bpf_qdisc selftest triggers a kernel panic: Unable to handle kernel paging request at virtual address ffffffffa38dbf58 Current test_progs pgtable: 4K pagesize, 57-bit VAs, pgdp=0x00000001109cc000 [ffffffffa38dbf58] pgd=000000011fffd801,		

CVE-2025-40079	p4d=000000011fffd401, pud=000000011fffd001, pmd=0000000000000000 Oops [#1] Modules linked in: bpf_testmod(OE) xt_conntrack nls_iso8859_1 [...] [last unloaded: bpf_testmod(OE)] CPU: 1 UID: 0 PID: 23584 Comm: test_progs Tainted: G W OE 6.17.0-rc1-g2465bb83e0b4 #1 NONE Tainted: [W]=WARN, [O]=OOT_MODULE, [E]=UNSIGNED_MODULE Hardware name: Unknown Unknown Product/Unknown Product, BIOS 2024.01+dfsg-1ubuntu5.1 01/01/2024 epc : __qdisc_run+0x82/0x6f0 ra : __qdisc_run+0x6e/0x6f0 epc : ffffffff80bd5c7a ra : ffffffff80bd5c66 sp : ff2000000eecb550 gp : ffffffff82472098 tp : ff60000096895940 t0 : ffffffff8001f180 t1 : ffffffff801e1664 t2 : 0000000000000000 s0 : ff2000000eecb5d0 s1 : ff60000093a6a600 a0 : ffffffffa38dbee8 a1 : 0000000000000001 a2 : ff2000000eecb510 a3 : 0000000000000001 a4 : 0000000000000000 a5 : 0000000000000010 a6 : 0000000000000000 a7 : 0000000000735049 s2 : ffffffffa38dbee8 s3 : 0000000000000040 s4 : ff6000008bcda000 s5 : 0000000000000008 s6 : ff60000093a6a680 s7 : ff60000093a6a6f0 s8 : ff60000093a6a6ac s9 : ff60000093140000 s10: 0000000000000000 s11: ff2000000eecb9d0 t3 : 0000000000000000 t4 : 0000000000ff0000 t5 : 0000000000000000 t6 : ff60000093a6a8b6 status: 0000000200000120 badaddr: ffffffffa38dbf58 cause: 000000000000000d [<ffffffff80bd5c7a>] __qdisc_run+0x82/0x6f0 [<ffffffff80b6fe58>] __dev_queue_xmit+0x4c0/0x1128 [<ffffffff80b80ae0>] neigh_resolve_output+0xd0/0x170 [<ffffffff80d2daf6>] ip6_finish_output2+0x226/0x6c8 [<ffffffff80d31254>] ip6_finish_output+0x10c/0x2a0 [<ffffffff80d31446>] ip6_output+0x5e/0x178 [<ffffffff80d2e232>] ip6_xmit+0x29a/0x608 [<ffffffff80d6f4c6>] inet6_csk_xmit+0xe6/0x140 [<ffffffff80c985e4>] __tcp_transmit_skb+0x45c/0xaa8 [<ffffffff80c995fe>] tcp_connect+0x9ce/0xd10 [<ffffffff80d66524>] tcp_v6_connect+0x4ac/0x5e8 [<ffffffff80cc19b8>] __inet_stream_connect+0xd8/0x318 [<ffffffff80cc1c36>] inet_stream_connect+0x3e/0x68 [<ffffffff80b42b20>] __sys_connect_file+0x50/0x88 [<ffffffff80b42bee>] __sys_connect+0x96/0xc8 [<ffffffff80b42c40>] __riscv_sys_connect+0x20/0x30 [<ffffffff80e5bcae>] do_trap_ecall_u+0x256/0x378 [<ffffffff80e69af2>] handle_exception+0x14a/0x156 Code: 892a 0363 1205 489c 8bc1 c7e5 2d03 084a 2703 080a (2783) 0709 ---[end trace 0000000000000000]--- The bpf_fifo_dequeue prog returns a skb which is a pointer. The pointer is treated as a 32bit value and sign extend to 64bit in epilogue. This behavior is right for most bpf prog types but wrong for struct ops which requires RISC-V ABI. So let's sign extend struct ops return values according to the function model and RISC-V ABI([0]). [0]: https://riscv.org/wp-content/uploads/2024/12/riscv-calling.pdf	N/A	More Details
CVE-2025-40078	In the Linux kernel, the following vulnerability has been resolved: bpf: Explicitly check accesses to bpf_sock_addr Syzkaller found a kernel warning on the following sock_addr program: 0: r0 = 0 1: r2 = *(u32 *)(r1 +60) 2: exit which triggers: verifier bug: error during ctx access conversion (0) This is happening because offset 60 in bpf_sock_addr corresponds to an implicit padding of 4 bytes, right after msg_src_ip4. Access to this padding isn't rejected in sock_addr_is_valid_access and it thus later fails to convert the access. This patch fixes it by explicitly checking the various fields of bpf_sock_addr in sock_addr_is_valid_access. I checked the other ctx structures and is_valid_access functions and didn't find any other similar cases. Other cases of (properly handled) padding are covered in new tests in a subsequent patch.	N/A	More Details
CVE-2025-40077	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid overflow while left shift operation Should cast type of folio->index from pgoff_t to loff_t to avoid overflow while left shift operation.	N/A	More Details
CVE-2025-40076	In the Linux kernel, the following vulnerability has been resolved: PCI: rcar-host: Pass proper IRQ domain to generic_handle_domain_irq() Starting with commit dd26c1a23fd5 ("PCI: rcar-host: Switch to msi_create_parent_irq_domain()"), the MSI parent IRQ domain is NULL because the object of type struct irq_domain_info passed to: msi_create_parent_irq_domain() -> irq_domain_instantiate()() -> __irq_domain_instantiate() has no reference to the parent IRQ domain. Using msi->domain->parent as an argument for generic_handle_domain_irq() leads to below error: "Unable to handle kernel NULL pointer dereference at virtual address" This error was identified while switching the upcoming RZ/G3S PCIe host controller driver to msi_create_parent_irq_domain() (which was using a similar pattern to handle MSIs (see link section)), but it was not tested on hardware using the pcie-rcar-host controller driver due to lack of hardware. [mani: reworded subject and description]	N/A	More Details
CVE-2025-40075	In the Linux kernel, the following vulnerability has been resolved: tcp_metrics: use dst_dev_net_rcu() Replace three dst_dev() with a lockdep enabled helper.	N/A	More Details
CVE-2025-40074	In the Linux kernel, the following vulnerability has been resolved: ipv4: start using dst_dev_rcu() Change icmpv4_xrlim_allow(), ip_defrag() to prevent possible UAF. Change ipmr_prepare_xmit(), ipmr_queue_fwd_xmit(), ip_mr_output(), ipv4_neigh_lookup() to use lockdep enabled dst_dev_rcu().	N/A	More Details
CVE-2025-40073	In the Linux kernel, the following vulnerability has been resolved: drm/msm: Do not validate SSPP when it is not ready Current code will validate current plane and previous plane to confirm they can share a SSPP with multi-rect mode. The SSPP is already allocated for previous plane, while current plane is not associated with any SSPP yet. Null pointer is referenced when validating the SSPP of current plane. Skip SSPP validation for current plane. Unable to handle kernel NULL pointer dereference at virtual address 0000000000000020 Mem abort info: ESR = 0x0000000096000004 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 user pgtable: 4k pages, 48-bit VAs, pgdp=0000000888ac3000 [0000000000000020] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000096000004 [#1] SMP Modules linked in: CPU: 4 UID: 0 PID: 1891 Comm: modetest Tainted: G S 6.15.0-rc2-g3ee3f6e1202e #335 PREEMPT Tainted: [S]=CPU_OUT_OF_SPEC Hardware name: SM8650 EV1 rev1 4slam 2et (DT) pstate: 63400009 (nZCv daif +PAN -UAO +TCO +DIT -SSBS BTYPE=--) pc : dpu_plane_is_multirect_capable+0x68/0x90 lr : dpu_assign_plane_resources+0x288/0x410 sp : ffff800093dcb770 x29: ffff800093dcb770 x28: 0000000000002000 x27: ffff000817c6c000 x26: ffff000806b46368 x25: ffff0008013f6080 x24: ffff00080cbf4800 x23: ffff000810842680 x22: ffff0008013f1080 x21: ffff00080cc86080 x20: ffff000806b463b0 x19: ffff00080cbf5a00 x18: 00000000ffffffff x17: 707a5f657a696c61 x16: 0000000000000003 x15: 0000000000002200 x14: 00000000ffffffff x13: 00aaaaaa00aaaaaa x12: 0000000000000000 x11: ffff000817c6e2b8 x10: 0000000000000000 x9 : ffff80008106a950 x8 : ffff00080cbf48f4 x7 : 0000000000000000 x6 : 0000000000000000 x5 : 0000000000000000 x4 : 0000000000000438 x3 : 0000000000000438 x2 : ffff800082e245e0 x1 : 0000000000000008 x0 : 0000000000000000 Call trace: dpu_plane_is_multirect_capable+0x68/0x90 (P) dpu_crtc_atomic_check+0x5bc/0x650 drm_atomic_helper_check_planes+0x13c/0x220 drm_atomic_helper_check+0x58/0xb8 msm_atomic_check+0xd8/0xf0 drm_atomic_check_only+0x4a8/0x968 drm_atomic_commit+0x50/0xd8 drm_atomic_helper_update_plane+0x140/0x188 __setplane_atomic+0xfc/0x148 drm_mode_setplane+0x164/0x378 drm_ioctl_kernel+0xc0/0x140 drm_ioctl+0x20c/0x500 __arm64_sys_ioctl+0xbc/0xf8 invoke_syscall+0x50/0x120 el0_svc_common.constprop.0+0x48/0xf8 do_el0_svc+0x28/0x40 el0_svc+0x30/0xd0 el0t_64_sync_handler+0x144/0x168 el0t_64_sync+0x198/0x1a0 Code: b9402021 370fffc1 f9401441 3707ff81 (f94010a1) ---[end trace 0000000000000000]--- Patchwork: https://patchwork.freedesktop.org/patch/669224/	N/A	More Details

CVE-2025-40072	In the Linux kernel, the following vulnerability has been resolved: fanotify: Validate the return value of mnt_ns_from_dentry() before dereferencing The function do_fanotify_mark() does not validate if mnt_ns_from_dentry() returns NULL before dereferencing mntns->user_ns. This causes a NULL pointer dereference in do_fanotify_mark() if the path is not a mount namespace object. Fix this by checking mnt_ns_from_dentry()'s return value before dereferencing it. Before the patch $ gcc fanotify_nullptr.c -o fanotify_nullptr $ mkdir A $ ./fanotify_nullptr Fanotify fd: 3 fanotify_mark: Operation not permitted $ unshare -Urm Fanotify fd: 3 Killed int main(void){ int ffd; ffd = fanotify_init(FAN_CLASS_NOTIF | FAN_REPORT_MNT, 0); if(ffd < 0) { perror("fanotify_init"); exit(EXIT_FAILURE); } printf("Fanotify fd: %d\n",ffd); if(fanotify_mark(ffd, FAN_MARK_ADD | FAN_MARK_MNTNS, FAN_MNT_ATTACH, AT_FDCWD, "A") < 0){ perror("fanotify_mark"); exit(EXIT_FAILURE); } return 0; } After the patch $ gcc fanotify_nullptr.c -o fanotify_nullptr $ mkdir A $ ./fanotify_nullptr Fanotify fd: 3 fanotify_mark: Operation not permitted $ unshare -Urm Fanotify fd: 3 fanotify_mark: Invalid argument [25.694973] BUG: kernel NULL pointer dereference, address: 0000000000000038 [25.695006] #PF: supervisor read access in kernel mode [25.695012] #PF: error_code(0x0000) - not-present page [25.695017] PGD 109a30067 P4D 109a30067 PUD 142b46067 PMD 0 [25.695025] Oops: Oops: 0000 [#1] SMP NOPTI [25.695032] CPU: 4 UID: 1000 PID: 1478 Comm: fanotify_nullpt Not tainted 6.17.0-rc4 #1 PREEMPT(lazy) [25.695040] Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 11/12/2020 [25.695049] RIP: 0010:do_fanotify_mark+0x817/0x950 [25.695066] Code: 04 00 00 e9 45 fd ff ff 48 8b 7c 24 48 4c 89 54 24 18 4c 89 5c 24 10 4c 89 0c 24 e8 b3 11 fc ff 4c 8b 54 24 18 4c 8b 5c 24 10 <48> 8b 78 38 4c 8b 0c 24 49 89 c4 e9 13 fd ff ff 8b 4c 24 28 85 c9 [25.695081] RSP: 0018:ffffd31c469e3c08 EFLAGS: 00010203 [25.695104] RAX: 0000000000000000 RBX: 0000000001000000 RCX: ffff8eb48aebd220 [25.695110] RDX: 0000000000000000 RSI: 0000000000000000 RDI: ffff8eb4835e8180 [25.695115] RBP: 0000000000000111 R08: 0000000000000000 R09: 0000000000000000 [25.695142] R10: ffff8eb48a7d56c0 R11: ffff8eb482bede00 R12: 00000000004012a7 [25.695148] R13: 0000000000000110 R14: 0000000000000001 R15: ffff8eb48a7d56c0 [25.695154] FS: 00007f8733bda740(0000) GS:ffff8eb61ce5f000(0000) knlGS:0000000000000000 [25.695162] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [25.695170] CR2: 0000000000000038 CR3: 0000000136994006 CR4: 00000000003706f0 [25.695201] Call Trace: [25.695209] <TASK> [25.695215] __x64_sys_fanotify_mark+0x1f/0x30 [25.695222] do_syscall_64+0x82/0x2c0 ...	N/A	More Details
CVE-2025-40071	In the Linux kernel, the following vulnerability has been resolved: tty: n_gsm: Don't block input queue by waiting MSC Currently gsm_queue() processes incoming frames and when opening a DLC channel it calls gsm_dlci_open() which calls gsm_modem_update(). If basic mode is used it calls gsm_modem_upd_via_msc() and it cannot block the input queue by waiting the response to come into the same input queue. Instead allow sending Modem Status Command without waiting for remote end to respond. Define a new function gsm_modem_send_initial_msc() for this purpose. As MSC is only valid for basic encoding, it does not do anything for advanced or when convergence layer type 2 is used.	N/A	More Details
CVE-2025-40070	In the Linux kernel, the following vulnerability has been resolved: pps: fix warning in pps_register_cdev when register device fail Similar to previous commit 2a934fdb01db ("media: v4l2-dev: fix error handling in __video_register_device()"), the release hook should be set before device_register(). Otherwise, when device_register() return error and put_device() try to callback the release function, the below warning may happen. ------------[cut here]------------ WARNING: CPU: 1 PID: 4760 at drivers/base/core.c:2567 device_release+0x1bd/0x240 drivers/base/core.c:2567 Modules linked in: CPU: 1 UID: 0 PID: 4760 Comm: syz.4.914 Not tainted 6.17.0-rc3+ #1 NONE RIP: 0010:device_release+0x1bd/0x240 drivers/base/core.c:2567 Call Trace: <TASK> kobject_cleanup+0x136/0x410 lib/kobject.c:689 kobject_release lib/kobject.c:720 [inline] kref_put include/linux/kref.h:65 [inline] kobject_put+0xe9/0x130 lib/kobject.c:737 put_device+0x24/0x30 drivers/base/core.c:3797 pps_register_cdev+0x2da/0x370 drivers/pps/pps.c:402 pps_register_source+0x2f6/0x480 drivers/pps/kapi.c:108 pps_tty_open+0x190/0x310 drivers/pps/clients/pps-ldisc.c:57 tty_ldisc_open+0xa7/0x120 drivers/tty/tty_ldisc.c:432 tty_set_ldisc+0x333/0x780 drivers/tty/tty_ldisc.c:563 tiocsetd drivers/tty/tty_io.c:2429 [inline] tty_ioctl+0x5d1/0x1700 drivers/tty/tty_io.c:2728 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:598 [inline] __se_sys_ioctl fs/ioctl.c:584 [inline] __x64_sys_ioctl+0x194/0x210 fs/ioctl.c:584 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0x5f/0x2a0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x76/0x7e </TASK> Before commit c79a39dc8d06 ("pps: Fix a use-after-free"), pps_register_cdev() call device_create() to create pps->dev, which will init dev->release to device_create_release(). Now the comment is outdated, just remove it. Thanks for the reminder from Calvin Owens, 'kfree_pps' should be removed in pps_register_source() to avoid a double free in the failure case.	N/A	More Details
CVE-2025-40069	In the Linux kernel, the following vulnerability has been resolved: drm/msm: Fix obj leak in VM_BIND error path If we fail a handle-lookup part way thru, we need to drop the already obtained obj references. Patchwork: https://patchwork.freedesktop.org/patch/669784/	N/A	More Details
CVE-2025-40068	In the Linux kernel, the following vulnerability has been resolved: fs: ntfs3: Fix integer overflow in run_unpack() The MFT record relative to the file being opened contains its runlist, an array containing information about the file's location on the physical disk. Analysis of all Call Stack paths showed that the values of the runlist array, from which LCNs are calculated, are not validated before run_unpack function. The run_unpack function decodes the compressed runlist data format from MFT attributes (for example, $DATA), converting them into a runs_tree structure, which describes the mapping of virtual clusters (VCN) to logical clusters (LCN). The NTFS3 subsystem also has a shortcut for deleting files from MFT records - in this case, the RUN_DEALLOCATE command is sent to the run_unpack input, and the function logic provides that all data transferred to the runlist about file or directory is deleted without creating a runs_tree structure. Substituting the runlist in the $DATA attribute of the MFT record for an arbitrary file can lead either to access to arbitrary data on the disk bypassing access checks to them (since the inode access check occurs above) or to destruction of arbitrary data on the disk. Add overflow check for addition operation. Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2025-40067	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: reject index allocation if $BITMAP is empty but blocks exist Index allocation requires at least one bit in the $BITMAP attribute to track usage of index entries. If the bitmap is empty while index blocks are already present, this reflects on-disk corruption. syzbot triggered this condition using a malformed NTFS image. During a rename() operation involving a long filename (which spans multiple index entries), the empty bitmap allowed the name to be added without valid tracking. Subsequent deletion of the original entry failed with -ENOENT, due to unexpected index state. Reject such cases by verifying that the bitmap is not empty when index blocks exist.	N/A	More Details
CVE-2025-40066	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7996: Check phy before init msta_link in mt7996_mac_sta_add_links() In order to avoid a possible NULL pointer dereference in mt7996_mac_sta_init_link routine, move the phy pointer check before running mt7996_mac_sta_init_link() in mt7996_mac_sta_add_links routine.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: RISC-V: KVM: Write hgatp register with valid mode bits According to the RISC-V Privileged Architecture Spec, when MODE=Bare is selected,software must write zero to the remaining		More

2025-40065	fields of hgatp. We have detected the valid mode supported by the HW before, So using a valid mode to detect how many vmid bits are supported.	N/A	Details
CVE-2025-1038	The “Diagnostics Tools” page of the web-based configuration utility does not properly validate user-controlled input, allowing an authenticated user with high privileges to inject commands into the command shell of the TropOS 4th Gen device. The injected commands can be exploited to execute several set-uid (SUID) applications to ultimately gain root access to the TropOS device.	N/A	More Details
CVE-2022-50580	In the Linux kernel, the following vulnerability has been resolved: blk-throttle: prevent overflow while calculating wait time There is a problem found by code review in tg_with_in_bps_limit() that 'bps_limit * jiffy_elapsed_rnd' might overflow. Fix the problem by calling mul_u64_u64_div_u64() instead.	N/A	More Details
CVE-2025-62725	Docker Compose trusts the path information embedded in remote OCI compose artifacts. When a layer includes the annotations com.docker.compose.extends or com.docker.compose.envfile, Compose joins the attacker-supplied value from com.docker.compose.file/com.docker.compose.envfile with its local cache directory and writes the file there. This affects any platform or workflow that resolves remote OCI compose artifacts, Docker Desktop, standalone Compose binaries on Linux, CI/CD runners, cloud dev environments is affected. An attacker can escape the cache directory and overwrite arbitrary files on the machine running docker compose, even if the user only runs read-only commands such as docker compose config or docker compose ps. This issue is fixed in v2.40.2.	N/A	More Details
CVE-2025-40643	Stored Cross-Site Scripting (XSS) vulnerability in Energy CRM v2025 by Status Tracker Ltd, consisting of a stored XSS due to lack of proper validation of user input by sending a POST request to “/crm/create_job_submit.php”, using the “JobCreatedBy” parameter. This vulnerability could allow a remote user to send a specially crafted query to an authenticated user and steal their cookie session details.	N/A	More Details
CVE-2023-53732	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Fix NULL dereference in ni_write_inode Syzbot reports a NULL dereference in ni_write_inode. When creating a new inode, if allocation fails in mi_init function (called in mi_format_new function), mi->mrec is set to NULL. In the error path of this inode creation, mi->mrec is later dereferenced in ni_write_inode. Add a NULL check to prevent NULL dereference.	N/A	More Details
CVE-2025-11750	In langgenius/dify-web version 1.6.0, the authentication mechanism reveals the existence of user accounts by returning different error messages for non-existent and existing accounts. Specifically, when a login or registration attempt is made with a non-existent username or email, the system responds with a message such as "account not found." Conversely, when the username or email exists but the password is incorrect, a different error message is returned. This discrepancy allows an attacker to enumerate valid user accounts by analyzing the error responses, potentially facilitating targeted social engineering, brute force, or credential stuffing attacks.	N/A	More Details
CVE-2025-11844	Hugging Face Smolagents version 1.20.0 contains an XPath injection vulnerability in the search_item_ctrl_f function located in src/smolagents/vision_web_browser.py. The function constructs an XPath query by directly concatenating user-supplied input into the XPath expression without proper sanitization or escaping. This allows an attacker to inject malicious XPath syntax that can alter the intended query logic. The vulnerability enables attackers to bypass search filters, access unintended DOM elements, and disrupt web automation workflows. This can lead to information disclosure, manipulation of AI agent interactions, and compromise the reliability of automated web tasks. The issue is fixed in version 1.22.0.	N/A	More Details
CVE-2025-8848	A vulnerability in danny-avila/librechat version 0.7.9 allows for HTML injection via the Accept-Language header. When a logged-in user sends an HTTP GET request with a crafted Accept-Language header, arbitrary HTML can be injected into the <html lang=""> tag of the response. This can lead to potential security risks such as cross-site scripting (XSS) attacks.	N/A	More Details
CVE-2016-15048	AMTT Hotel Broadband Operation System (HiBOS) contains an unauthenticated command injection vulnerability in the /manager/radius/server_ping.php endpoint. The application constructs a shell command that includes the user-supplied ip parameter and executes it without proper validation or escaping. An attacker can insert shell metacharacters into the ip parameter to inject and execute arbitrary system commands as the web server user. The initial third-party disclosure in 2016 recommended contacting the vendor for remediation guidance. Additionally, this product may have been rebranded under a different name. VulnCheck has observed this vulnerability being exploited in the wild as of 2025-10-14 at 04:45:53.510819 UTC.	N/A	More Details
CVE-2025-11965	In Eclipse Vert.x versions [4.0.0, 4.5.21] and [5.0.0, 5.0.4], a StaticHandler configuration for restricting access to hidden files fails to restrict access to hidden directories, allowing unauthorized users to retrieve files within them (e.g. '.git/config').	N/A	More Details
CVE-2025-11966	In Eclipse Vert.x versions [4.0.0, 4.5.21] and [5.0.0, 5.0.4], when "directory listing" is enabled, file and directory names are inserted into generated HTML without proper escaping in the href, title, and link attributes. An attacker who can create or rename files or directories within a served path can craft filenames containing malicious script or HTML content, leading to stored cross-site scripting (XSS) that executes in the context of users viewing the affected directory listing.	N/A	More Details
CVE-2023-53733	In the Linux kernel, the following vulnerability has been resolved: net: sched: cls_u32: Undo tcf_bind_filter if u32_replace_hw_knode When u32_replace_hw_knode fails, we need to undo the tcf_bind_filter operation done at u32_set_parms.	N/A	More Details
CVE-2025-40018	In the Linux kernel, the following vulnerability has been resolved: ipvs: Defer ip_vs_ftp unregister during netns cleanup On the netns cleanup path, __ip_vs_ftp_exit() may unregister ip_vs_ftp before connections with valid cp->app pointers are flushed, leading to a use-after-free. Fix this by introducing a global `exiting_module` flag, set to true in ip_vs_ftp_exit() before unregistering the pernet subsystem. In __ip_vs_ftp_exit(), skip ip_vs_ftp unregister if called during netns cleanup (when exiting_module is false) and defer it to __ip_vs_cleanup_batch(), which unregisters all apps after all connections are flushed. If called during module exit, unregister ip_vs_ftp immediately.	N/A	More Details
CVE-2023-53711	In the Linux kernel, the following vulnerability has been resolved: NFS: Fix a potential data corruption We must ensure that the subrequests are joined back into the head before we can retransmit a request. If the head was not on the commit lists, because the server wrote it synchronously, we still need to add it back to the retransmission list. Add a call that mirrors the effect of nfs_cancel_remove_inode() for O_DIRECT.	N/A	More Details
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: crypto: essiv - Check ssize for decryption and in-place encryption Move the ssize check to the start in essiv_aead_crypt so that it's also checked for decryption and in-place	N/A	More Details

40019	encryption.		
CVE-2025-40020	In the Linux kernel, the following vulnerability has been resolved: can: peak_usb: fix shift-out-of-bounds issue Explicitly uses a 64-bit constant when the number of bits used for its shifting is 32 (which is the case for PC CAN FD interfaces supported by this driver). [mkl: update subject, apply manually]	N/A	More Details
CVE-2025-40021	In the Linux kernel, the following vulnerability has been resolved: tracing: dynevent: Add a missing lockdown check on dynevent Since dynamic_events interface on tracefs is compatible with kprobe_events and uprobe_events, it should also check the lockdown status and reject if it is set.	N/A	More Details
CVE-2025-40022	In the Linux kernel, the following vulnerability has been resolved: crypto: af_alg - Fix incorrect boolean values in af_alg_ctx Commit 1b34cbbf4f01 ("crypto: af_alg - Disallow concurrent writes in af_alg_sendmsg") changed some fields from bool to 1-bit bitfields of type u32. However, some assignments to these fields, specifically 'more' and 'merge', assign values greater than 1. These relied on C's implicit conversion to bool, such that zero becomes false and nonzero becomes true. With a 1-bit bitfields of type u32 instead, mod 2 of the value is taken instead, resulting in 0 being assigned in some cases when 1 was intended. Fix this by restoring the bool type.	N/A	More Details
CVE-2025-40023	In the Linux kernel, the following vulnerability has been resolved: drm/xe/vf: Don't expose sysfs attributes not applicable for VFs VFs can't read BMG_PCIE_CAP(0x138340) register nor access PCODE (already guarded by the info.skip_pcode flag) so we shouldn't expose attributes that require any of them to avoid errors like: [] xe 0000:03:00.1: [drm] Tile0: GT0: VF is trying to read an \ inaccessible register 0x138340+0x0 [] RIP: 0010:xe_gt_sriov_vf_read32+0x6c2/0x9a0 [xe] [] Call Trace: [] xe_mmio_read32+0x110/0x280 [xe] [] auto_link_downgrade_capable_show+0x2e/0x70 [xe] [] dev_attr_show+0x1a/0x70 [] sysfs_kf_seq_show+0xaa/0x120 [] kernfs_seq_show+0x41/0x60 (cherry picked from commit a2d6223d224f333f705ed8495bf8bebfbc585c35)	N/A	More Details
CVE-2025-40024	In the Linux kernel, the following vulnerability has been resolved: vhost: Take a reference on the task in struct vhost_task. vhost_task_create() creates a task and keeps a reference to its task_struct. That task may exit early via a signal and its task_struct will be released. A pending vhost_task_wake() will then attempt to wake the task and access a task_struct which is no longer there. Acquire a reference on the task_struct while creating the thread and release the reference while the struct vhost_task itself is removed. If the task exits early due to a signal, then the vhost_task_wake() will still access a valid task_struct. The wake is safe and will be skipped in this case.	N/A	More Details
CVE-2025-9981	QuickCMS is vulnerable to multiple Stored XSS in slider editor functionality (sliders-form). Malicious attacker with admin privileges can inject arbitrary HTML and JS into website, which will be rendered/executed on every page. By default admin user is not able to add JavaScript into the website. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.8 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-9980	QuickCMS is vulnerable to multiple Stored XSS in page editor functionality (pages-form). Malicious attacker with admin privileges can inject arbitrary HTML and JS into website, which will be rendered/executed when visiting edited page. By default admin user is not able to add JavaScript into the website. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.8 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2023-53731	In the Linux kernel, the following vulnerability has been resolved: netlink: fix potential deadlock in netlink_set_err() syzbot reported a possible deadlock in netlink_set_err() [1] A similar issue was fixed in commit 1d482e666b8e ("netlink: disable IRQs for netlink_lock_table()") in netlink_lock_table() This patch adds IRQ safety to netlink_set_err() and __netlink_diag_dump() which were not covered by cited commit. [1] WARNING: possible irq lock inversion dependency detected 6.4.0-rc6-syzkaller-00240-g4e9f0ec38852 #0 Not tainted syz-executor.2/23011 just changed the state of lock: ffffffff8e1a7a58 (nl_table_lock){.+.?}-{2:2}, at: netlink_set_err+0x2e/0x3a0 net/netlink/af_netlink.c:1612 but this lock was taken by another, SOFTIRQ-safe lock in the past: (&local->queue_stop_reason_lock){..-.}-{2:2} and interrupts could create inverse lock ordering between them. other info that might help us debug this: Possible interrupt unsafe locking scenario: CPU0 CPU1 ---- ---- lock(nl_table_lock); local_irq_disable(); lock(&local->queue_stop_reason_lock); lock(nl_table_lock); <Interrupt> lock(&local->queue_stop_reason_lock); *** DEADLOCK ***	N/A	More Details
CVE-2023-53730	In the Linux kernel, the following vulnerability has been resolved: blk-iocost: use spin_lock_irqsave in adjust_inuse_and_calc_cost adjust_inuse_and_calc_cost() use spin_lock_irq() and IRQ will be enabled when unlock. DEADLOCK might happen if we have held other locks and disabled IRQ before invoking it. Fix it by using spin_lock_irqsave() instead, which can keep IRQ state consistent with before when unlock. ================================ WARNING: inconsistent lock state 5.10.0-02758-g8e5f91fd772f #26 Not tainted -------------------------------- inconsistent {IN-HARDIRQ-W} -> {HARDIRQ-ON-W} usage. kworker/2:3/388 [HC0[0]:SC0[0]:HE0:SE1] takes: ffff888118c00c28 (&bfqd->lock){?.-.}-{2:2}, at: spin_lock_irq ffff888118c00c28 (&bfqd->lock){?.-.}-{2:2}, at: bfq_bio_merge+0x141/0x390 {IN-HARDIRQ-W} state was registered at: __lock_acquire+0x3d7/0x1070 lock_acquire+0x197/0x4a0 __raw_spin_lock_irqsave _raw_spin_lock_irqsave+0x3b/0x60 bfq_idle_slice_timer_body bfq_idle_slice_timer+0x53/0x1d0 __run_hrtimer+0x477/0xa70 __hrtimer_run_queues+0x1c6/0x2d0 hrtimer_interrupt+0x302/0x9e0 local_apic_timer_interrupt __sysvec_apic_timer_interrupt+0xfd/0x420 run_sysvec_on_irqstack_cond sysvec_apic_timer_interrupt+0x46/0xa0 asm_sysvec_apic_timer_interrupt+0x12/0x20 irq event stamp: 837522 hardirqs last enabled at (837521): [<ffffffff84b9419d>] __raw_spin_unlock_irqrestore hardirqs last enabled at (837521): [<ffffffff84b9419d>] _raw_spin_unlock_irqrestore+0x3d/0x40 hardirqs last disabled at (837522): [<ffffffff84b93fa3>] __raw_spin_lock_irq hardirqs last disabled at (837522): [<ffffffff84b93fa3>] _raw_spin_lock_irq+0x43/0x50 softirqs last enabled at (835852): [<ffffffff84e00558>] __do_softirq+0x558/0x8ec softirqs last disabled at (835845): [<ffffffff84c010ff>] asm_call_irq_on_stack+0xf/0x20 other info that might help us debug this: Possible unsafe locking scenario: CPU0 ---- lock(&bfqd->lock); <Interrupt> lock(&bfqd->lock); *** DEADLOCK *** 3 locks held by kworker/2:3/388: #0: ffff888107af0f38 ((wq_completion)kthrotld){+.+.}-{0:0}, at: process_one_work+0x742/0x13f0 #1: ffff8881176bfdd8 ((work_completion)(&td->dispatch_work)){+.+.}-{0:0}, at: process_one_work+0x777/0x13f0 #2: ffff888118c00c28 (&bfqd->lock){?.-.}-{2:2}, at: spin_lock_irq #2: ffff888118c00c28 (&bfqd->lock){?.-.}-{2:2}, at: bfq_bio_merge+0x141/0x390 stack backtrace: CPU: 2 PID: 388 Comm: kworker/2:3 Not tainted 5.10.0-02758-g8e5f91fd772f #26 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-prebuilt.qemu.org 04/01/2014 Workqueue: kthrotld blk_throtl_dispatch_work_fn Call Trace: __dump_stack lib/dump_stack.c:77 [inline] dump_stack+0x107/0x167 print_usage_bug valid_state mark_lock_irq.cold+0x32/0x3a mark_lock+0x693/0xbc0 mark_held_locks+0x9e/0xe0 __trace_hardirqs_on_caller lockdep_hardirqs_on_prepare.part.0+0x151/0x360 trace_hardirqs_on+0x5b/0x180 __raw_spin_unlock_irq	N/A	More Details

	_raw_spin_unlock_irq+0x24/0x40 spin_unlock_irq adjust_inuse_and_calc_cost+0x4fb/0x970 ioc_rqos_merge+0x277/0x740 __rq_qos_merge+0x62/0xb0 rq_qos_merge bio_attempt_back_merge+0x12c/0x4a0 blk_mq_sched_try_merge+0x1b6/0x4d0 bfq_bio_merge+0x24a/0x390 __blk_mq_sched_bio_merge+0xa6/0x460 blk_mq_sched_bio_merge blk_mq_submit_bio+0x2e7/0x1ee0 __submit_bio_noacct_mq+0x175/0x3b0 submit_bio_noacct+0x1fb/0x270 blk_throtl_dispatch_work_fn+0x1ef/0x2b0 process_one_work+0x83e/0x13f0 process_scheduled_works worker_thread+0x7e3/0xd80 kthread+0x353/0x470 ret_from_fork+0x1f/0x30		
CVE-2023-53729	In the Linux kernel, the following vulnerability has been resolved: soc: qcom: qmi_encdec: Restrict string length in decode The QMI TLV value for strings in a lot of qmi element info structures account for null terminated strings with MAX_LEN + 1. If a string is actually MAX_LEN + 1 length, this will cause an out of bounds access when the NULL character is appended in decoding.	N/A	More Details
CVE-2023-53728	In the Linux kernel, the following vulnerability has been resolved: posix-timers: Ensure timer ID search-loop limit is valid posix_timer_add() tries to allocate a posix timer ID by starting from the cached ID which was stored by the last successful allocation. This is done in a loop searching the ID space for a free slot one by one. The loop has to terminate when the search wrapped around to the starting point. But that's racy vs. establishing the starting point. That is read out lockless, which leads to the following problem: CPU0 CPU1 posix_timer_add() start = sig->posix_timer_id; lock(hash_lock); ... posix_timer_add() if (++sig->posix_timer_id < 0) start = sig->posix_timer_id; sig->posix_timer_id = 0; So CPU1 can observe a negative start value, i.e. -1, and the loop break never happens because the condition can never be true: if (sig->posix_timer_id == start) break; While this is unlikely to ever turn into an endless loop as the ID space is huge (INT_MAX), the racy read of the start value caught the attention of KCSAN and Dmitry unearthed that incorrectness. Rewrite it so that all id operations are under the hash lock.	N/A	More Details
CVE-2023-53713	In the Linux kernel, the following vulnerability has been resolved: arm64: sme: Use STR P to clear FFR context field in streaming SVE mode The FFR is a predicate register which can vary between 16 and 256 bits in size depending upon the configured vector length. When saving the SVE state in streaming SVE mode, the FFR register is inaccessible and so commit 9f5848665788 ("arm64/sve: Make access to FFR optional") simply clears the FFR field of the in-memory context structure. Unfortunately, it achieves this using an unconditional 8-byte store and so if the SME vector length is anything other than 64 bytes in size we will either fail to clear the entire field or, worse, we will corrupt memory immediately following the structure. This has led to intermittent kfence splats in CI [1] and can trigger kmalloc Redzone corruption messages when running the 'fp-stress' kselftest: | ========== | BUG kmalloc-1k (Not tainted): kmalloc Redzone overwritten | ---------- | | 0xffff000809bf1e22-0xffff000809bf1e27 @offset=7714. First byte 0x0 instead of 0xcc | Allocated in do_sme_acc+0x9c/0x220 age=2613 cpu=1 pid=531 | __kmalloc+0x8c/0xcc | do_sme_acc+0x9c/0x220 | ... Replace the 8-byte store with a store of a predicate register which has been zero-initialised with PFALSE, ensuring that the entire field is cleared in memory. [1] https://lore.kernel.org/r/CA+G9fYtU7HsV0R0dp4XEH5xXHSJFw8KyDf5VQrLLfMxWfxQkag@mail.gmail.com	N/A	More Details
CVE-2023-53714	In the Linux kernel, the following vulnerability has been resolved: drm/stm: ltdc: fix late dereference check In ltdc_crtc_set_crc_source(), struct drm_crtc was dereferenced in a container_of() before the pointer check. This could cause a kernel panic. Fix this smatch warning: drivers/gpu/drm/stm/ltdc.c:1124 ltdc_crtc_set_crc_source() warn: variable dereferenced before check 'crtc' (see line 1119)	N/A	More Details
CVE-2023-53715	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: cfg80211: Pass the PMK in binary instead of hex Apparently the hex passphrase mechanism does not work on newer chips/firmware (e.g. BCM4387). It seems there was a simple way of passing it in binary all along, so use that and avoid the hexification. OpenBSD has been doing it like this from the beginning, so this should work on all chips. Also clear the structure before setting the PMK. This was leaking uninitialized stack contents to the device.	N/A	More Details
CVE-2023-53716	In the Linux kernel, the following vulnerability has been resolved: net: fix skb leak in __skb_tstamp_tx() Commit 50749f2dd685 ("tcp/udp: Fix memleaks of sk and zerocopy skbs with TX timestamp.") added a call to skb_orphan_frags_rx() to fix leaks with zerocopy skbs. But it ended up adding a leak of its own. When skb_orphan_frags_rx() fails, the function just returns, leaking the skb it just cloned. Free it before returning. This bug was discovered and resolved using Coverity Static Analysis Security Testing (SAST) by Synopsys, Inc.	N/A	More Details
CVE-2024-14011	Rejected reason: This is a duplicate.	N/A	More Details
CVE-2023-53717	In the Linux kernel, the following vulnerability has been resolved: wifi: ath9k: Fix potential stack-out-of-bounds write in ath9k_wmi_rsp_callback() Fix a stack-out-of-bounds write that occurs in a WMI response callback function that is called after a timeout occurs in ath9k_wmi_cmd(). The callback writes to wmi->cmd_rsp_buf, a stack-allocated buffer that could no longer be valid when a timeout occurs. Set wmi->last_seq_id to 0 when a timeout occurred. Found by a modified version of syzkaller. BUG: KASAN: stack-out-of-bounds in ath9k_wmi_ctrl_rx Write of size 4 Call Trace: memcpy ath9k_wmi_ctrl_rx ath9k_htc_rx_msg ath9k_hif_usb_reg_in_cb __usb_hcd_giveback_urb usb_hcd_giveback_urb dummy_timer call_timer_fn run_timer_softirq __do_softirq irq_exit_rcu sysvec_apic_timer_interrupt	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: ring-buffer: Do not swap cpu_buffer during resize process When ring_buffer_swap_cpu was called during resize process, the cpu buffer was swapped in the middle, resulting in incorrect state. Continuing to run in the wrong state will result in oops. This issue can be easily reproduced using the following two scripts: /tmp # cat test1.sh //#! /bin/sh for i in `seq 0 100000` do echo 2000 > /sys/kernel/debug/tracing/buffer_size_kb sleep 0.5 echo 5000 > /sys/kernel/debug/tracing/buffer_size_kb sleep 0.5 done /tmp # cat test2.sh //#! /bin/sh for i in `seq 0 100000` do echo irqsoff > /sys/kernel/debug/tracing/current_tracer sleep 1 echo nop > /sys/kernel/debug/tracing/current_tracer sleep 1 done /tmp # ./test1.sh & /tmp # ./test2.sh & A typical oops log is as follows, sometimes with other different oops logs. [231.711293] WARNING: CPU: 0 PID: 9 at kernel/trace/ring_buffer.c:2026 rb_update_pages+0x378/0x3f8 [231.713375] Modules linked in: [231.714735] CPU: 0 PID: 9 Comm: kworker/0:1 Tainted: G W 6.5.0-rc1-00276-g20edcec23f92 #15 [231.716750] Hardware name: linux,dummy-virt (DT) [231.718152] Workqueue: events update_pages_handler [231.719714] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [231.721171] pc : rb_update_pages+0x378/0x3f8 [231.722212] lr : rb_update_pages+0x25c/0x3f8 [231.723248] sp : ffff800082b9bd50 [231.724169] x29: ffff800082b9bd50 x28: ffff8000825f7000 x27: 0000000000000000 [231.726102] x26: 0000000000000001 x25: fffffffffffff010 x24: 0000000000000ff0 [231.728122] x23: ffff0000c3a0b600 x22: ffff0000c3a0b5c0 x21: fffffffffffffe0a [231.730203] x20: ffff0000c3a0b600 x19: ffff0000c0102400 x18: 0000000000000000 [231.732329] x17: 0000000000000000 x16: 0000000000000000 x15:		

CVE-2023-53718	0000ffffe7aa8510 [231.734212] x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000002 [231.736291] x11: ffff8000826998a8 x10: ffff800082b9baf0 x9 : ffff800081137558 [231.738195] x8 : fffffc00030e82c8 x7 : 0000000000000000 x6 : 0000000000000001 [231.740192] x5 : ffff0000ffbafe00 x4 : 0000000000000000 x3 : 0000000000000000 [231.742118] x2 : 00000000000006aa x1 : 0000000000000001 x0 : ffff0000c0007208 [231.744196] Call trace: [231.744892] rb_update_pages+0x378/0x3f8 [231.745893] update_pages_handler+0x1c/0x38 [231.746893] process_one_work+0x1f0/0x468 [231.747852] worker_thread+0x54/0x410 [231.748737] kthread+0x124/0x138 [231.749549] ret_from_fork+0x10/0x20 [231.750434] ---[end trace 0000000000000000]--- [233.720486] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 [233.721696] Mem abort info: [233.721935] ESR = 0x0000000096000004 [233.722283] EC = 0x25: DABT (current EL), IL = 32 bits [233.722596] SET = 0, FnV = 0 [233.722805] EA = 0, S1PTW = 0 [233.723026] FSC = 0x04: level 0 translation fault [233.723458] Data abort info: [233.723734] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [233.724176] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [233.724589] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [233.725075] user pgtable: 4k pages, 48-bit VAs, pgdp=0000000104943000 [233.725592] [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 [233.726231] Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP [233.726720] Modules linked in: [233.727007] CPU: 0 PID: 9 Comm: kworker/0:1 Tainted: G W 6.5.0-rc1-00276-g20edcec23f92 #15 [233.727777] Hardware name: linux,dummy-virt (DT) [233.728225] Workqueue: events update_pages_handler [233.728655] pstate: 200000c5 (nzCv daIF -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [233.729054] pc : rb_update_pages+0x1a8/0x3f8 [233.729334] lr : rb_update_pages+0x154/0x3f8 [233.729592] sp : ffff800082b9bd50 [233.729792] x29: ffff800082b9bd50 x28: ffff8000825f7000 x27: 00000000 ---truncated---	N/A	More Details
CVE-2023-53719	In the Linux kernel, the following vulnerability has been resolved: serial: arc_uart: fix of_iomap leak in `arc_serial_probe` Smatch reports: drivers/tty/serial/arc_uart.c:631 arc_serial_probe() warn: 'port->membase' from of_iomap() not released on lines: 631. In arc_serial_probe(), if uart_add_one_port() fails, port->membase is not released, which would cause a resource leak. To fix this, I replace of_iomap with devm_platform_ioremap_resource.	N/A	More Details
CVE-2023-53720	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Release the label when replacing existing ct entry Cited commit doesn't release the label mapping when replacing existing ct entry which leads to following memleak report: unreferenced object 0xffff8881854cf280 (size 96): comm "kworker/u48:74", pid 23093, jiffies 4296664564 (age 175.944s) hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace: [<000000002722d368>] __kmalloc+0x4b/0x1c0 [<00000000cc44e18f>] mapping_add+0x6e8/0xc90 [mlx5_core] [<000000003ad942a7>] mlx5_get_label_mapping+0x66/0xe0 [mlx5_core] [<00000000266308ac>] mlx5_tc_ct_entry_create_mod_hdr+0x1c4/0xf50 [mlx5_core] [<000000009a768b4f>] mlx5_tc_ct_entry_add_rule+0x16f/0xaf0 [mlx5_core] [<00000000a178f3e5>] mlx5_tc_ct_block_flow_offload_add+0x10cb/0x1f90 [mlx5_core] [<000000007b46c496>] mlx5_tc_ct_block_flow_offload+0x14a/0x630 [mlx5_core] [<00000000a9a18ac5>] nf_flow_offload_tuple+0x1a3/0x390 [nf_flow_table] [<00000000d0881951>] flow_offload_work_handler+0x257/0xd30 [nf_flow_table] [<000000009e4935a4>] process_one_work+0x7c2/0x13e0 [<00000000f5cd36a7>] worker_thread+0x59d/0xec0 [<00000000baed1daf>] kthread+0x28f/0x330 [<0000000063d282a4>] ret_from_fork+0x1f/0x30 Fix the issue by correctly releasing the label mapping.	N/A	More Details
CVE-2023-53721	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: Fix a NULL pointer dereference in ath12k_mac_op_hw_scan() In ath12k_mac_op_hw_scan(), the return value of kzalloc() is directly used in memcpy(), which may lead to a NULL pointer dereference on failure of kzalloc(). Fix this bug by adding a check of arg.extraie.ptr. Tested-on: WCN7850 hw2.0 PCI WLAN.HMT.1.0-03427-QCAHMTSWPL_V1.0_V2.0_SILICONZ-1.15378.4	N/A	More Details
CVE-2023-53722	In the Linux kernel, the following vulnerability has been resolved: md: raid1: fix potential OOB in raid1_remove_disk() If rddev->raid_disk is greater than mddev->raid_disks, there will be an out-of-bounds in raid1_remove_disk(). We have already found similar reports as follows: 1) commit d17f744e883b ("md-raid10: fix KASAN warning") 2) commit 1ebc2cec0b7d ("dm raid: fix KASAN warning in raid5_remove_disk") Fix this bug by checking whether the "number" variable is valid.	N/A	More Details
CVE-2023-53723	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: disable sdma ecc irq only when sdma RAS is enabled in suspend sdma_v4_0_ip is shared on a few asics, but in sdma_v4_0_hw_fini, driver unconditionally disables ecc_irq which is only enabled on those asics enabling sdma ecc. This will introduce a warning in suspend cycle on those chips with sdma ip v4.0, while without sdma ecc. So this patch correct this. [7283.166354] RIP: 0010:amdgpu_irq_put+0x45/0x70 [amdgpu] [7283.167001] RSP: 0018:ffff9a5fc3967d08 EFLAGS: 00010246 [7283.167019] RAX: ffff98d88afd3770 RBX: 0000000000000001 RCX: 0000000000000000 [7283.167023] RDX: 0000000000000000 RSI: ffff98d89da30390 RDI: ffff98d89da20000 [7283.167025] RBP: ffff98d89da20000 R08: 0000000000036838 R09: 0000000000000006 [7283.167028] R10: ffffd5764243c008 R11: 0000000000000000 R12: ffff98d89da30390 [7283.167030] R13: ffff98d89da38978 R14: ffffffff999ae15a R15: ffff98d880130105 [7283.167032] FS: 0000000000000000(0000) GS:ffff98d996f00000(0000) knlGS:0000000000000000 [7283.167036] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [7283.167039] CR2: 00000000f7a9d178 CR3: 00000001c42ea000 CR4: 00000000003506e0 [7283.167041] Call Trace: [7283.167046] <TASK> [7283.167048] sdma_v4_0_hw_fini+0x38/0xa0 [amdgpu] [7283.167704] amdgpu_device_ip_suspend_phase2+0x101/0x1a0 [amdgpu] [7283.168296] amdgpu_device_suspend+0x103/0x180 [amdgpu] [7283.168875] amdgpu_pmops_freeze+0x21/0x60 [amdgpu] [7283.169464] pci_pm_freeze+0x54/0xc0	N/A	More Details
CVE-2023-53724	In the Linux kernel, the following vulnerability has been resolved: mfd: pcf50633-adc: Fix potential memleak in pcf50633_adc_async_read() `req` is allocated in pcf50633_adc_async_read(), but adc_enqueue_request() could fail to insert the `req` into queue. We need to check the return value and free it in the case of failure.	N/A	More Details
CVE-2023-53725	In the Linux kernel, the following vulnerability has been resolved: clocksource/drivers/cadence-ttc: Fix memory leak in ttc_timer_probe Smatch reports: drivers/clocksource/timer-cadence-ttc.c:529 ttc_timer_probe() warn: 'timer_baseaddr' from of_iomap() not released on lines: 498,508,516. timer_baseaddr may have the problem of not being released after use, I replaced it with the devm_of_iomap() function and added the clk_put() function to cleanup the "clk_ce" and "clk_cs".	N/A	More Details
CVE-2025-41073	Path Traversal vulnerability in version 4.4.2236.1 of TESI Gandia Integra Total. This issue allows an authenticated attacker to download a ZIP file containing files from the server, including those located in parent directories (e.g., ..\..\..), by exploiting the “direstudio” parameter in “/encuestas/integraweb[_v4]/integra/html/view/comprimir.php”.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: arm64: csum: Fix OoB access in IP checksum code for negative lengths Although commit c2c24edb1d9c ("arm64: csum: Fix pathological zero-length calls") added an early return for zero-length input, syzkaller has popped up with an example of a _negative_ length which causes an undefined shift and an out-of-bounds read: | BUG: KASAN: slab-out-of-bounds in do_csum+0x44/0x254 arch/arm64/lib/csum.c:39 | Read of size		

CVE-2023-53726	4294966928 at addr ffff0000d7ac0170 by task syz-executor412/5975 | | CPU: 0 PID: 5975 Comm: syz-executor412 Not tainted 6.4.0-rc4-syzkaller-g908f31f2a05b #0 | Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/25/2023 | Call trace: | dump_backtrace+0x1b8/0x1e4 arch/arm64/kernel/stacktrace.c:233 | show_stack+0x2c/0x44 arch/arm64/kernel/stacktrace.c:240 | __dump_stack lib/dump_stack.c:88 [inline] | dump_stack_lvl+0xd0/0x124 lib/dump_stack.c:106 | print_address_description mm/kasan/report.c:351 [inline] | print_report+0x174/0x514 mm/kasan/report.c:462 | kasan_report+0xd4/0x130 mm/kasan/report.c:572 | kasan_check_range+0x264/0x2a4 mm/kasan/generic.c:187 | __kasan_check_read+0x20/0x30 mm/kasan/shadow.c:31 | do_csum+0x44/0x254 arch/arm64/lib/csum.c:39 | csum_partial+0x30/0x58 lib/checksum.c:128 | gso_make_checksum include/linux/skbuff.h:4928 [inline] | __udp_gso_segment+0xaf4/0x1bc4 net/ipv4/udp_offload.c:332 | udp6_ufo_fragment+0x540/0xca0 net/ipv6/udp_offload.c:47 | ipv6_gso_segment+0x5cc/0x1760 net/ipv6/ip6_offload.c:119 | skb_mac_gso_segment+0x2b4/0x5b0 net/core/gro.c:141 | __skb_gso_segment+0x250/0x3d0 net/core/dev.c:3401 | skb_gso_segment include/linux/netdevice.h:4859 [inline] | validate_xmit_skb+0x364/0xdbc net/core/dev.c:3659 | validate_xmit_skb_list+0x94/0x130 net/core/dev.c:3709 | sch_direct_xmit+0xe8/0x548 net/sched/sch_generic.c:327 | __dev_xmit_skb net/core/dev.c:3805 [inline] | __dev_queue_xmit+0x147c/0x3318 net/core/dev.c:4210 | dev_queue_xmit include/linux/netdevice.h:3085 [inline] | packet_xmit+0x6c/0x318 net/packet/af_packet.c:276 | packet_snd net/packet/af_packet.c:3081 [inline] | packet_sendmsg+0x376c/0x4c98 net/packet/af_packet.c:3113 | sock_sendmsg_nosec net/socket.c:724 [inline] | sock_sendmsg net/socket.c:747 [inline] | __sys_sendto+0x3b4/0x538 net/socket.c:2144 Extend the early return to reject negative lengths as well, aligning our implementation with the generic code in lib/checksum.c	N/A	More Details
CVE-2023-53727	In the Linux kernel, the following vulnerability has been resolved: net/sched: fq_pie: avoid stalls in fq_pie_timer() When setting a high number of flows (limit being 65536), fq_pie_timer() is currently using too much time as syzbot reported. Add logic to yield the cpu every 2048 flows (less than 150 usec on debug kernels). It should also help by not blocking qdisc fast paths for too long. Worst case (65536 flows) would need 31 jiffies for a complete scan. Relevant extract from syzbot report: rcu: INFO: rcu_preempt detected expedited stalls on CPUs/tasks: { 0-.... } 2663 jiffies s: 873 root: 0x1/. rcu: blocking rcu_node structures (internal RCU debug): Sending NMI from CPU 1 to CPUs 0: NMI backtrace for cpu 0 CPU: 0 PID: 5177 Comm: syz-executor273 Not tainted 6.5.0-syzkaller-00453-g727dbda16b83 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 07/26/2023 RIP: 0010:check_kcov_mode kernel/kcov.c:173 [inline] RIP: 0010:write_comp_data+0x21/0x90 kernel/kcov.c:236 Code: 2e 0f 1f 84 00 00 00 00 00 65 8b 05 01 b2 7d 7e 49 89 f1 89 c6 49 89 d2 81 e6 00 01 00 00 49 89 f8 65 48 8b 14 25 80 b9 03 00 <a9> 00 01 ff 00 74 0e 85 f6 74 59 8b 82 04 16 00 00 85 c0 74 4f 8b RSP: 0018:ffffc90000007bb8 EFLAGS: 00000206 RAX: 0000000000000101 RBX: ffffc9000dc0d140 RCX: ffffffff885893b0 RDX: ffff88807c075940 RSI: 0000000000000100 RDI: 0000000000000001 RBP: 0000000000000000 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffc9000dc0d178 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 0000555555d54380(0000) GS:ffff8880b9800000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f6b442f6130 CR3: 000000006fe1c000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <NMI> </NMI> <IRQ> pie_calculate_probability+0x480/0x850 net/sched/sch_pie.c:415 fq_pie_timer+0x1da/0x4f0 net/sched/sch_fq_pie.c:387 call_timer_fn+0x1a0/0x580 kernel/time/timer.c:1700	N/A	More Details
CVE-2025-62499	Movable Type contains a stored cross-site scripting vulnerability in Edit CategorySet of ContentType page. If crafted input is stored by an attacker with "ContentType Management" privilege, an arbitrary script may be executed on the web browser of the user who accesses Edit CategorySet of ContentType page.	N/A	More Details
CVE-2025-61865	NarSuS App registers a Windows service with an unquoted file path. A user with the write permission on the root directory of the system drive may execute arbitrary code with SYSTEM privilege.	N/A	More Details
CVE-2025-54856	Movable Type contains a stored cross-site scripting vulnerability in Edit ContentData page. If crafted input is stored by an attacker with "ContentType Management" privilege, an arbitrary script may be executed on the web browser of the user who accesses Edit ContentData page.	N/A	More Details
CVE-2025-4106	An authenticated admin user with access to both the management WebUI and command line interface on a Firebox can enable a diagnostic debug shell by uploading a platform and version-specific diagnostic package and executing a leftover diagnostic command. This issue affects Fireware OS: from 12.0 before 12.11.2.	N/A	More Details
CVE-2025-62248	A reflected cross-site scripting (XSS) vulnerability, resulting from a regression, has been identified in Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.9, 2025.Q1.0 through 2025.Q1.16, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.1 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.19 allows a remote, authenticated attacker to inject and execute JavaScript code via the _com_liferay_dynamic_data_mapping_web_portlet_DDMPortlet_definition parameter. The malicious payload is executed within the victim's browser when they access a URL that includes the crafted parameter.	N/A	More Details
CVE-2025-62714	Karmada Dashboard is a general-purpose, web-based control panel for Karmada which is a multi-cluster management project. Prior to version 0.2.0, there is an authentication bypass vulnerability in the Karmada Dashboard API. The backend API endpoints (e.g., /api/v1/secret, /api/v1/service) did not enforce authentication, allowing unauthenticated users to access sensitive cluster information such as Secrets and Services directly. Although the web UI required a valid JWT for access, the API itself remained exposed to direct requests without any authentication checks. Any user or entity with network access to the Karmada Dashboard service could exploit this vulnerability to retrieve sensitive data.	N/A	More Details
CVE-2025-62247	Missing Authorization in Collection Provider component in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.9, 2025.Q1.0 through 2025.Q1.16, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.19 allows instance users to read and select unauthorized Blueprints through the Collection Providers across instances.	N/A	More Details
CVE-2025-62611	aiomysql is a library for accessing a MySQL database from the asyncio. Prior to version 0.3.0, the client-side settings are not checked before sending local files to MySQL server, which allows obtaining arbitrary files from the client using a rogue server. It is possible to create a rogue MySQL server that emulates authorization, ignores client flags and requests arbitrary files from the client by sending a LOAD_LOCAL instruction packet. This issue has been patched in version 0.3.0.	N/A	More Details
CVE-2025-	FastGPT is an AI Agent building platform. Prior to version 4.11.1, in the workflow file reading node, the network link is not security-verified, posing a risk of SSRF attacks. This issue has been patched in version 4.11.1.	N/A	More Details

62612			
CVE-2025-62613	VDO.Ninja is a tool that brings remote video feeds into OBS or other studio software via WebRTC. From versions 28.0 to before 28.4, a reflected Cross-Site Scripting (XSS) vulnerability exists on examples/control.html through the room parameter, which is improperly sanitized before being rendered in the DOM. The application fails to validate and encode user input, allowing malicious scripts to be injected and executed. This issue has been patched in version 28.4.	N/A	More Details
CVE-2025-62614	BookLore is a self-hosted web app for organizing and managing personal book collections. In versions 1.8.1 and prior, an authentication bypass vulnerability in the BookMediaController allows any unauthenticated user to access and download book covers, thumbnails, and complete PDF/CBX page content without authorization. The vulnerability exists because multiple media endpoints lack proper access control annotations, and the CoverJwtFilter continues request processing even when no authentication token is provided. This enables attackers to enumerate and exfiltrate all book content from the system, bypassing the intended download permissions (canDownload) entirely. This issue has been patched via commit b226c43.	N/A	More Details
CVE-2025-62804	Rejected reason: Not used	N/A	More Details
CVE-2025-62805	Rejected reason: Not used	N/A	More Details
CVE-2025-62806	Rejected reason: Not used	N/A	More Details
CVE-2025-62807	Rejected reason: Not used	N/A	More Details
CVE-2025-62808	Rejected reason: Not used	N/A	More Details
CVE-2025-62809	Rejected reason: Not used	N/A	More Details
CVE-2025-62810	Rejected reason: Not used	N/A	More Details
CVE-2025-62811	Rejected reason: Not used	N/A	More Details
CVE-2025-62812	Rejected reason: Not used	N/A	More Details
CVE-2025-12104	Outdated and Vulnerable UI Dependencies might potentially lead to exploitation.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-34293	GN4 Publishing System versions prior to 2.6 contain an insecure direct object reference (IDOR) vulnerability via the API. Authenticated requests to the API's object endpoints allow an authenticated user to request arbitrary user IDs and receive sensitive account data for those users, including the stored password and the account's security question and answer. The exposed recovery data and encrypted password may be used to reset or take over the target account.	N/A	More Details
CVE-2025-62711	Wasmtime is a runtime for WebAssembly. In versions from 38.0.0 to before 38.0.3, the implementation of component-model related host-to-wasm trampolines in Wasmtime contained a bug where it's possible to carefully craft a component, which when called in a specific way, would crash the host with a segfault or assert failure. Wasmtime 38.0.3 has been released and is patched to fix this issue. There are no workarounds.	N/A	More Details
CVE-2025-54806	GROWI v4.2.7 and earlier contains a cross-site scripting vulnerability in the page alert function. If a user accesses a crafted URL while logged in to the affected product, an arbitrary script may be executed on the user's web browser.	N/A	More Details
CVE-2025-12194	Uncontrolled Resource Consumption vulnerability in Legion of the Bouncy Castle Inc. Bouncy Castle for Java FIPS bc-fips on All (API modules), Legion of the Bouncy Castle Inc. Bouncy Castle for Java LTS bcprov-lts8on on All (API modules) allows Excessive Allocation. This vulnerability is associated with program files core/src/main/jdk1.9/org/bouncycastle/crypto/fips/AESNativeCFB.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/fips/AESNativeGCM.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/fips/SHA256NativeDigest.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/fips/AESNativeEngine.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/fips/AESNativeCBC.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/fips/AESNativeCTR.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/engines/AESNativeCFB.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/engines/AESNativeGCM.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/engines/AESNativeEngine.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/engines/AESNativeCBC.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/engines/AESNativeGCMSIV.Java,	N/A	More Details

	core/src/main/jdk1.9/org/bouncycastle/crypto/engines/AESNativeCCM.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/engines/AESNativeCTR.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/digests/SHA256NativeDigest.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/digests/SHA224NativeDigest.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/digests/SHA3NativeDigest.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/digests/SHAKENativeDigest.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/digests/SHA512NativeDigest.Java, core/src/main/jdk1.9/org/bouncycastle/crypto/digests/SHA384NativeDigest.Java. This issue affects Bouncy Castle for Java FIPS: from 2.1.0 through 2.1.1; Bouncy Castle for Java LTS: from 2.73.0 through 2.73.7.		
CVE-2025-60228	Deserialization of Untrusted Data vulnerability in designthemes Knowledge Base kbase allows Object Injection.This issue affects Knowledge Base: from n/a through <= 2.9.	N/A	More Details
CVE-2025-12285	Missing Initial Password Change.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-12284	Lack of Input Validation in the web UI might lead to potential exploitation.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-12278	Logout Functionality not Working.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-12275	Mail Configuration File Manipulation + Command Execution.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-8709	A SQL injection vulnerability exists in the langchain-ai/langchain repository, specifically in the LangGraph's SQLite store implementation. The affected version is langgraph-checkpoint-sqlite 2.0.10. The vulnerability arises from improper handling of filter operators ($eq, $ne, $gt, $lt, $gte, $lte) where direct string concatenation is used without proper parameterization. This allows attackers to inject arbitrary SQL, leading to unauthorized access to all documents, data exfiltration of sensitive fields such as passwords and API keys, and a complete bypass of application-level security filters.	N/A	More Details
CVE-2025-12221	Busybox 1.31.1 - Multiple Known Vulnerabilities.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-12220	Busybox 1.31.1 - Multiple Known Vulnerabilities.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-12219	Vulnerable Components in Azure Access OS.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-12218	Weak Default Credentials.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-12217	SNMP Default Community String (public).This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-12216	Malicious / Malformed App can be Installed but not Uninstalled/may lead to unavailability.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-62813	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2025-62659	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation MediaWiki CookieConsent extension allows Cross-Site Scripting (XSS).This issue affects MediaWiki CookieConsent extension: from v0.1.0 before v2.0.0.	N/A	More Details
CVE-2025-34503	Deck Mate 1 executes firmware directly from an external EEPROM without verifying authenticity or integrity. An attacker with physical access can replace or reflash the EEPROM to run arbitrary code that persists across reboots. Because this design predates modern secure-boot or signed-update mechanisms, affected systems should be physically protected or retired from service. The vendor has not indicated that firmware updates are available for this legacy model.	N/A	More Details
CVE-2025-34502	Deck Mate 2 lacks a verified secure-boot chain and runtime integrity validation for its controller and display modules. Without cryptographic boot verification, an attacker with physical access can modify or replace the bootloader, kernel, or filesystem and gain persistent code execution on reboot. This weakness allows long-term firmware tampering that survives power cycles. The vendor indicates that more recent firmware updates strengthen update-chain integrity and disable physical update ports to mitigate related attack avenues.	N/A	More Details
CVE-	Deck Mate 2's firmware update mechanism accepts packages without cryptographic signature verification, encrypts them with a single hard-coded AES key shared across devices, and uses a truncated HMAC for integrity validation. Attackers with access to the update interface - typically via the unit's USB update port - can craft or modify firmware packages to execute arbitrary		More

2025-34500	code as root, allowing persistent compromise of the device's integrity and deck randomization process. Physical or on-premises access remains the most likely attack path, though network-exposed or telemetry-enabled deployments could theoretically allow remote exploitation if misconfigured. The vendor confirmed that firmware updates have been issued to correct these update-chain weaknesses and that USB update access has been disabled on affected units.	N/A	Details
CVE-2023-53712	In the Linux kernel, the following vulnerability has been resolved: ARM: 9317/1: kexec: Make smp stop calls asynchronous If a panic is triggered by a hrtimer interrupt all online cpus will be notified and set offline. But as highlighted by commit 19dbdcb8039c ("smp: Warn on function calls from softirq context") this call should not be made synchronous with disabled interrupts: softdog: Initiating panic Kernel panic - not syncing: Software Watchdog Timer expired WARNING: CPU: 1 PID: 0 at kernel/smp.c:753 smp_call_function_many_cond unwind_backtrace: show_stack dump_stack_lvl __warn warn_slowpath_fmt smp_call_function_many_cond smp_call_function crash_smp_send_stop.part.0 machine_crash_shutdown __crash_kexec panic softdog_fire __hrtimer_run_queues hrtimer_interrupt Make the smp call for machine_crash_nonpanic_core() asynchronous.	N/A	More Details
CVE-2023-53710	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7921: fix error code of return in mt7921_acpi_read Kernel NULL pointer dereference when ACPI SAR table isn't implemented well. Fix the error code of return to mark the ACPI SAR table as invalid. [5.077128] mt7921e 0000:06:00.0: sar cnt = 0 [5.077381] BUG: kernel NULL pointer dereference, address: 0000000000000004 [5.077630] #PF: supervisor read access in kernel mode [5.077883] #PF: error_code(0x0000) - not-present page [5.078138] PGD 0 P4D 0 [5.078398] Oops: 0000 [#1] PREEMPT SMP NOPTI [5.079202] RIP: 0010:mt7921_init_acpi_sar+0x106/0x220 [mt7921_common] ... [5.080786] Call Trace: [5.080786] <TASK> [5.080786] mt7921_register_device+0x37d/0x490 [mt7921_common] [5.080786] mt7921_pci_probe.part.0+0x2ee/0x310 [mt7921e] [5.080786] mt7921_pci_probe+0x52/0x70 [mt7921e] [5.080786] local_pci_probe+0x47/0x90 [5.080786] pci_call_probe+0x55/0x190 [5.080786] pci_device_probe+0x84/0x120	N/A	More Details
CVE-2025-62262	Information exposure through log file vulnerability in LDAP import feature in Liferay Portal 7.4.0 through 7.4.3.97, and older unsupported versions, and Liferay DXP 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions allows local users to view user email address in the log files.	N/A	More Details
CVE-2025-9158	The Request Tracker software is vulnerable to a Stored XSS vulnerability in calendar invitation parsing feature, which displays invitation data without HTML sanitization. XSS vulnerability allows an attacker to send a specifically crafted e-mail enabling JavaScript code execution by displaying the ticket in the context of the logged-in user. This vulnerability affects versions from 5.0.4 through 5.0.8 and from 6.0.0 through 6.0.1.	N/A	More Details
CVE-2022-50556	In the Linux kernel, the following vulnerability has been resolved: drm: Fix potential null-ptr-deref due to drmm_mode_config_init() drmm_mode_config_init() will call drm_mode_create_standard_properties() and won't check the ret value. When drm_mode_create_standard_properties() failed due to alloc, property will be a NULL pointer and may causes the null-ptr-deref. Fix the null-ptr-deref by adding the ret value check. Found null-ptr-deref while testing insert module bochs: general protection fault, probably for non-canonical address 0xdfffffc000000000c: 0000 [#1] SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000060-0x0000000000000067] CPU: 3 PID: 249 Comm: modprobe Not tainted 6.1.0-rc1+ #364 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.15.0-0-g2dd4b9b3f840-prebuilt.qemu.org 04/01/2014 RIP: 0010:drm_object_attach_property+0x73/0x3c0 [drm] Call Trace: <TASK> __drm_connector_init+0xb6c/0x1100 [drm] bochs_pci_probe.cold.11+0x4cb/0x7fe [bochs] pci_device_probe+0x17d/0x340 really_probe+0x1db/0x5d0 __driver_probe_device+0x1e7/0x250 driver_probe_device+0x4a/0x120 __driver_attach+0xcd/0x2c0 bus_for_each_dev+0x11a/0x1b0 bus_add_driver+0x3d7/0x500 driver_register+0x18e/0x320 do_one_initcall+0xc4/0x3e0 do_init_module+0x1b4/0x630 load_module+0x5dca/0x7230 __do_sys_finit_module+0x100/0x170 do_syscall_64+0x3f/0x90 entry_SYSCALL_64_after_hwframe+0x63/0xcd RIP: 0033:0x7ff65af9f839	N/A	More Details
CVE-2025-58070	Pleasanter contains a stored cross-site scripting vulnerability in Preview for Attachments, which allows an attacker to execute an arbitrary script in a logged-in user's web browser.	N/A	More Details
CVE-2022-50557	In the Linux kernel, the following vulnerability has been resolved: pinctrl: thunderbay: fix possible memory leak in thunderbay_build_functions() The thunderbay_add_functions() will free memory of thunderbay_funcs when everything is ok, but thunderbay_funcs will not be freed when thunderbay_add_functions() fails, then there will be a memory leak, so we need to add kfree() when thunderbay_add_functions() fails to fix it. In addition, doing some cleaner works, moving kfree(funcs) from thunderbay_add_functions() to thunderbay_build_functions().	N/A	More Details
CVE-2025-61931	Pleasanter contains a stored cross-site scripting vulnerability in Body, Description and Comments, which allows an attacker to execute an arbitrary script in a logged-in user's web browser.	N/A	More Details
CVE-2025-12364	Weak Password Policy.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-12363	Email Password Disclosure.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2022-50558	In the Linux kernel, the following vulnerability has been resolved: regmap-irq: Use the new num_config_regs property in regmap_add_irq_chip_fwnode Commit faa87ce9196d ("regmap-irq: Introduce config registers for irq types") added the num_config_regs, then commit 9edd4f5aee84 ("regmap-irq: Deprecate type registers and virtual registers") suggested to replace num_type_reg with it. However, regmap_add_irq_chip_fwnode wasn't modified to use the new property. Later on, commit 255a03bb1bb3 ("ASoC: wcd9335: Convert irq chip to config regs") removed the old num_type_reg property from the WCD9335 driver's struct regmap_irq_chip, causing a null pointer dereference in regmap_irq_set_type when it tried to index d->type_buf as it was never allocated in regmap_add_irq_chip_fwnode: [39.199374] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 [39.200006] Call trace: [39.200014] regmap_irq_set_type+0x84/0x1c0 [39.200026] __irq_set_trigger+0x60/0x1c0 [39.200040] __setup_irq+0x2f4/0x78c [39.200051] request_threaded_irq+0xe8/0x1a0 Use num_config_regs in regmap_add_irq_chip_fwnode instead of num_type_reg, and fall back to it if num_config_regs isn't defined to maintain backward compatibility.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: clk: imx: scu: fix memleak on platform_device_add() fails No		

2022-50559	error handling is performed when platform_device_add() fails. Add error processing before return, and modified the return value.	N/A	More Details
CVE-2022-50560	In the Linux kernel, the following vulnerability has been resolved: drm/meson: explicitly remove aggregate driver at module unload time Because component_master_del wasn't being called when unloading the meson_drm module, the aggregate device would linger forever in the global aggregate_devices list. That means when unloading and reloading the meson_dw_hdmi module, component_add would call into try_to_bring_up_aggregate_device and find the unbound meson_drm aggregate device. This would in turn dereference some of the aggregate_device's struct entries which point to memory automatically freed by the devres API when unbinding the aggregate device from meson_drv_unbind, and trigger an use-after-free bug: [+0.000014] ========== [+0.000007] BUG: KASAN: use-after-free in find_components+0x468/0x500 [+0.000017] Read of size 8 at addr ffff000006731688 by task modprobe/2536 [+0.000018] CPU: 4 PID: 2536 Comm: modprobe Tainted: G C O 5.19.0-rc6-lrmbkasan+ #1 [+0.000010] Hardware name: Hardkernel ODROID-N2Plus (DT) [+0.000008] Call trace: [+0.000005] dump_backtrace+0x1ec/0x280 [+0.000011] show_stack+0x24/0x80 [+0.000007] dump_stack_lvl+0x98/0xd4 [+0.000010] print_address_description.constprop.0+0x80/0x520 [+0.000011] print_report+0x128/0x260 [+0.000007] kasan_report+0xb8/0xfc [+0.000007] __asan_report_load8_noabort+0x3c/0x50 [+0.000009] find_components+0x468/0x500 [+0.000008] try_to_bring_up_aggregate_device+0x64/0x390 [+0.000009] __component_add+0x1dc/0x49c [+0.000009] component_add+0x20/0x30 [+0.000008] meson_dw_hdmi_probe+0x28/0x34 [meson_dw_hdmi] [+0.000013] platform_probe+0xd0/0x220 [+0.000008] really_probe+0x3ac/0xa80 [+0.000008] __driver_probe_device+0x1f8/0x400 [+0.000008] driver_probe_device+0x68/0x1b0 [+0.000008] __driver_attach+0x20c/0x480 [+0.000009] bus_for_each_dev+0x114/0x1b0 [+0.000007] driver_attach+0x48/0x64 [+0.000009] bus_add_driver+0x390/0x564 [+0.000007] driver_register+0x1a8/0x3e4 [+0.000009] __platform_driver_register+0x6c/0x94 [+0.000007] meson_dw_hdmi_platform_driver_init+0x30/0x1000 [meson_dw_hdmi] [+0.000014] do_one_initcall+0xc4/0x2b0 [+0.000008] do_init_module+0x154/0x570 [+0.000010] load_module+0x1a78/0x1ea4 [+0.000008] __do_sys_init_module+0x184/0x1cc [+0.000008] __arm64_sys_init_module+0x78/0xb0 [+0.000008] invoke_syscall+0x74/0x260 [+0.000008] el0_svc_common.constprop.0+0xcc/0x260 [+0.000009] do_el0_svc+0x50/0x70 [+0.000008] el0_svc+0x68/0x1a0 [+0.000009] el0t_64_sync_handler+0x11c/0x150 [+0.000009] el0t_64_sync+0x18c/0x190 [+0.000014] Allocated by task 902: [+0.000007] kasan_save_stack+0x2c/0x5c [+0.000009] __kasan_kmalloc+0x90/0xd0 [+0.000007] __kmalloc_node+0x240/0x580 [+0.000010] memcg_alloc_slab_cgroups+0xa4/0x1ac [+0.000010] memcg_slab_post_alloc_hook+0xbc/0x4c0 [+0.000008] kmem_cache_alloc_node+0x1d0/0x490 [+0.000009] __alloc_skb+0x1d4/0x310 [+0.000010] alloc_skb_with_frags+0x8c/0x620 [+0.000008] sock_alloc_send_pskb+0x5ac/0x6d0 [+0.000010] unix_dgram_sendmsg+0x2e0/0x12f0 [+0.000010] sock_sendmsg+0xcc/0x110 [+0.000007] sock_write_iter+0x1d0/0x304 [+0.000008] new_sync_write+0x364/0x460 [+0.000007] vfs_write+0x420/0x5ac [+0.000008] ksys_write+0x19c/0x1f0 [+0.000008] __arm64_sys_write+0x78/0xb0 [+0.000007] invoke_syscall+0x74/0x260 [+0.000008] el0_svc_common.constprop.0+0x1a8/0x260 [+0.000009] do_el0_svc+0x50/0x70 [+0.000007] el0_svc+0x68/0x1a0 [+0.000008] el0t_64_sync_handler+0x11c/0x150 [+0.000008] el0t_64_sync+0x18c/0x190 [+0.000013] Freed by task 2509: [+0.000008] kasan_save_stack+0x2c/0x5c [+0.000007] kasan_set_track+0x2c/0x40 [+0.000008] kasan_set_free_info+0x28/0x50 [+0.000008] ___kasan_slab_free+0x128/0x1d4 [+0.000008] __kasan_slab_free+0x18/0x24 [+0.000007] slab_free_freelist_hook+0x108/0x230 [+0.000010] ---truncated---	N/A	More Details
CVE-2023-53709	In the Linux kernel, the following vulnerability has been resolved: ring-buffer: Handle race between rb_move_tail and rb_check_pages It seems a data race between ring_buffer writing and integrity check. That is, RB_FLAG of head_page is been updating, while at same time RB_FLAG was cleared when doing integrity check rb_check_pages(): rb_check_pages() rb_handle_head_page(): -------- -------- rb_head_page_deactivate() rb_head_page_set_normal() rb_head_page_activate() We do intergrity test of the list to check if the list is corrupted and it is still worth doing it. So, let's refactor rb_check_pages() such that we no longer clear and set flag during the list sanity checking. [1] and [2] are the test to reproduce and the crash report respectively. 1: ``` read_trace.sh while true; do # the "trace" file is closed after read head -1 /sys/kernel/tracing/trace > /dev/null done ``` ``` repro.sh sysctl -w kernel.panic_on_warn=1 # function tracer will writing enough data into ring_buffer echo function > /sys/kernel/tracing/current_tracer ./read_trace.sh & ./read_trace.sh & ./read_trace.sh & ./read_trace.sh & ./read_trace.sh & ./read_trace.sh & ./read_trace.sh & ./read_trace.sh & ``` 2: ------------[cut here]------------ WARNING: CPU: 9 PID: 62 at kernel/trace/ring_buffer.c:2653 rb_move_tail+0x450/0x470 Modules linked in: CPU: 9 PID: 62 Comm: ksoftirqd/9 Tainted: G W 6.2.0-rc6+ Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.15.0-0-g2dd4b9b3f840-prebuilt.qemu.org 04/01/2014 RIP: 0010:rb_move_tail+0x450/0x470 Code: ff ff 4c 89 c8 f0 4d 0f b1 02 48 89 c2 48 83 e2 fc 49 39 d0 75 24 83 e0 03 83 f8 02 0f 84 e1 fb ff ff 48 8b 57 10 f0 ff 42 08 <0f> 0b 83 f8 02 0f 84 ce fb ff ff e9 db RSP: 0018:ffffb5564089bd00 EFLAGS: 00000203 RAX: 0000000000000000 RBX: ffff9db385a2bf81 RCX: ffffb5564089bd18 RDX: ffff9db281110100 RSI: 0000000000000fe4 RDI: ffff9db380145400 RBP: ffff9db385a2bf80 R08: ffff9db385a2bfc0 R09: ffff9db385a2bfc2 R10: ffff9db385a6c000 R11: ffff9db385a2bf80 R12: 0000000000000000 R13: 00000000000003e8 R14: ffff9db281110100 R15: ffffffffbb006108 FS: 0000000000000000(0000) GS:ffff9db3bdcc0000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00005602323024c8 CR3: 0000000022e0c000 CR4: 00000000000006e0 Call Trace: <TASK> ring_buffer_lock_reserve+0x136/0x360 ? __do_softirq+0x287/0x2df ? __pfx_rcu_softirq_qs+0x10/0x10 trace_function+0x21/0x110 ? __pfx_rcu_softirq_qs+0x10/0x10 ? __do_softirq+0x287/0x2df function_trace_call+0xf6/0x120 0xffffffffc038f097 ? rcu_softirq_qs+0x5/0x140 rcu_softirq_qs+0x5/0x140 __do_softirq+0x287/0x2df run_ksoftirqd+0x2a/0x30 smpboot_thread_fn+0x188/0x220 ? __pfx_smpboot_thread_fn+0x10/0x10 kthread+0xe7/0x110 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x2c/0x50 </TASK> ---[end trace 0000000000000000]--- [crash report and test reproducer credit goes to Zheng Yejian]	N/A	More Details
CVE-2022-50561	In the Linux kernel, the following vulnerability has been resolved: iio: fix memory leak in iio_device_register_eventset() When iio_device_register_sysfs_group() returns failed, iio_device_register_eventset() needs to free attrs array. Otherwise, kmemleak would scan & report memory leak as below: unreferenced object 0xffff88810a1cc3c0 (size 32): comm "100-i2c-vcnl302", pid 728, jiffies 4295052307 (age 156.027s) backtrace: __kmalloc+0x46/0x1b0 iio_device_register_eventset at drivers/iio/industrialio-event.c:541 __iio_device_register at drivers/iio/industrialio-core.c:1959 __devm_iio_device_register at drivers/iio/industrialio-core.c:2040	N/A	More Details
CVE-2022-50562	In the Linux kernel, the following vulnerability has been resolved: tpm: acpi: Call acpi_put_table() to fix memory leak The start and length of the event log area are obtained from TPM2 or TCPA table, so we call acpi_get_table() to get the ACPI information, but the acpi_get_table() should be coupled with acpi_put_table() to release the ACPI memory, add the acpi_put_table() properly to fix the memory leak. While we are at it, remove the redundant empty line at the end of the tpm_read_log_acpi().	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: dm thin: Fix UAF in run_timer_softirq() When dm_resume()		

CVE-2022-50563	and dm_destroy() are concurrent, it will lead to UAF, as follows: BUG: KASAN: use-after-free in __run_timers+0x173/0x710 Write of size 8 at addr ffff88816d9490f0 by task swapper/0/0 <snip> Call Trace: <IRQ> dump_stack_lvl+0x73/0x9f print_report.cold+0x132/0xaa2 _raw_spin_lock_irqsave+0xcd/0x160 __run_timers+0x173/0x710 kasan_report+0xad/0x110 __run_timers+0x173/0x710 __asan_store8+0x9c/0x140 __run_timers+0x173/0x710 call_timer_fn+0x310/0x310 pvclock_clocksource_read+0xfa/0x250 kvm_clock_read+0x2c/0x70 kvm_clock_get_cycles+0xd/0x20 ktime_get+0x5c/0x110 lapic_next_event+0x38/0x50 clockevents_program_event+0xf1/0x1e0 run_timer_softirq+0x49/0x90 __do_softirq+0x16e/0x62c __irq_exit_rcu+0x1fa/0x270 irq_exit_rcu+0x12/0x20 sysvec_apic_timer_interrupt+0x8e/0xc0 One of the concurrency UAF can be shown as below: use free do_resume | __find_device_hash_cell | dm_get | atomic_inc(&md->holders) | | dm_destroy | __dm_destroy | if (!dm_suspended_md(md)) | atomic_read(&md->holders) | msleep(1) dm_resume | __dm_resume | dm_table_resume_targets | pool_resume | do_waker #add delay work | dm_put | atomic_dec(&md->holders) | | dm_table_destroy | pool_dtr | __pool_dec | __pool_destroy | destroy_workqueue | kfree(pool) # free pool time out __do_softirq run_timer_softirq # pool has already been freed This can be easily reproduced using: 1. create thin-pool 2. dmsetup suspend pool 3. dmsetup resume pool 4. dmsetup remove_all # Concurrent with 3 The root cause of this UAF bug is that dm_resume() adds timer after dm_destroy() skips cancelling the timer because of suspend status. After timeout, it will call run_timer_softirq(), however pool has already been freed. The concurrency UAF bug will happen. Therefore, cancelling timer again in __pool_destroy().	N/A	More Details
CVE-2022-50564	In the Linux kernel, the following vulnerability has been resolved: s390/netiucv: Fix return type of netiucv_tx() With clang's kernel control flow integrity (kCFI, CONFIG_CFI_CLANG), indirect call targets are validated against the expected function pointer prototype to make sure the call target is valid to help mitigate ROP attacks. If they are not identical, there is a failure at run time, which manifests as either a kernel panic or thread getting killed. A proposed warning in clang aims to catch these at compile time, which reveals: drivers/s390/net/netiucv.c:1854:21: error: incompatible function pointer types initializing 'netdev_tx_t (*)(struct sk_buff *, struct net_device *)' (aka 'enum netdev_tx (*)(struct sk_buff *, struct net_device *)') with an expression of type 'int (struct sk_buff *, struct net_device *)' [-Werror,-Wincompatible-function-pointer-types-strict] .ndo_start_xmit = netiucv_tx, ^~~~~~~~~~ ->ndo_start_xmit() in 'struct net_device_ops' expects a return type of 'netdev_tx_t', not 'int'. Adjust the return type of netiucv_tx() to match the prototype's to resolve the warning and potential CFI failure, should s390 select ARCH_SUPPORTS_CFI_CLANG in the future. Additionally, while in the area, remove a comment block that is no longer relevant.	N/A	More Details
CVE-2022-50565	In the Linux kernel, the following vulnerability has been resolved: wifi: plfxlc: fix potential memory leak in __lf_x_usb_enable_rx() urbs does not be freed in exception paths in __lf_x_usb_enable_rx(). That will trigger memory leak. To fix it, add kfree() for urbs within "error" label. Compile tested only.	N/A	More Details
CVE-2022-50566	In the Linux kernel, the following vulnerability has been resolved: mtd: Fix device name leak when register device failed in add_mtd_device() There is a kmemleak when register device failed: unreferenced object 0xffff888101aab550 (size 8): comm "insmod", pid 3922, jiffies 4295277753 (age 925.408s) hex dump (first 8 bytes): 6d 74 64 30 00 88 ff ff mtd0.... backtrace: [<00000000bde26724>] __kmalloc_node_track_caller+0x4e/0x150 [<000000003c32b416>] kvasprintf+0xb0/0x130 [<000000001f7a8f15>] kobject_set_name_vargs+0x2f/0xb0 [<000000006e781163>] dev_set_name+0xab/0xe0 [<00000000e30d0c78>] add_mtd_device+0x4bb/0x700 [<00000000f3d34de7>] mtd_device_parse_register+0x2ac/0x3f0 [<00000000c0d88488>] 0xffffffffa0238457 [<00000000b40d0922>] 0xffffffffa02a008f [<0000000023d17b9d>] do_one_initcall+0x87/0x2a0 [<00000000770f6ca6>] do_init_module+0xdf/0x320 [<000000007b6768fe>] load_module+0x2f98/0x3330 [<00000000346bed5a>] __do_sys_finit_module+0x113/0x1b0 [<00000000674c2290>] do_syscall_64+0x35/0x80 [<000000004c6a8d97>] entry_SYSCALL_64_after_hwframe+0x46/0xb0 If register device failed, should call put_device() to give up the reference.	N/A	More Details
CVE-2022-50567	In the Linux kernel, the following vulnerability has been resolved: fs: jfs: fix shift-out-of-bounds in dbAllocAG Syzbot found a crash : UBSAN: shift-out-of-bounds in dbAllocAG. The underlying bug is the missing check of bmp->db_agl2size. The field can be greater than 64 and trigger the shift-out-of-bounds. Fix this bug by adding a check of bmp->db_agl2size in dbMount since this field is used in many following functions. The upper bound for this field is L2MAXL2SIZE - L2MAXAG, thanks for the help of Dave Kleikamp. Note that, for maintenance, I reorganized error handling code of dbMount.	N/A	More Details
CVE-2022-50568	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_hid: fix f_hidg lifetime vs cdev The embedded struct cdev does not have its lifetime correctly tied to the enclosing struct f_hidg, so there is a use-after-free if /dev/hidgN is held open while the gadget is deleted. This can readily be replicated with libusbgx's example programs (for conciseness - operating directly via configfs is equivalent): gadget-hid exec 3<> /dev/hidg0 gadget-vid-pid-remove exec 3<&- Pull the existing device up in to struct f_hidg and make use of the cdev_device_{add,del}() helpers. This changes the lifetime of the device object to match struct f_hidg, but note that it is still added and deleted at the same time.	N/A	More Details
CVE-2025-11411	NLnet Labs Unbound up to and including version 1.24.0 is vulnerable to possible domain hijack attacks. Promiscuous NS RRSets that complement positive DNS replies in the authority section can be used to trick resolvers to update their delegation information for the zone. Usually these RRSets are used to update the resolver's knowledge of the zone's name servers. A malicious actor can exploit the possible poisonous effect by injecting NS RRSets (and possibly their respective address records) in a reply. This could be done for example by trying to spoof a packet or fragmentation attacks. Unbound would then proceed to update the NS RRSet data it already has since the new data has enough trust for it, i.e., in-zone data for the delegation point. Unbound 1.24.1 includes a fix that scrubs unsolicited NS RRSets (and their respective address records) from replies mitigating the possible poison effect.	N/A	More Details
CVE-2025-11915	Connection desynchronization between an HTTP proxy and the model backend. The fixes were rolled out for all proxies in front of impacted models by 2025-09-28. Users do not need to take any action.	N/A	More Details
CVE-2025-12365	Error Messages Wrapped In HTTP Header.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-32785	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level advertisement and internet tracker blocking application. Pi-hole Admin Interface versions prior to 6.3 are vulnerable to cross-site scripting (XSS) via the Address field in the Subscribed Lists group management section. An authenticated user can inject malicious JavaScript by adding a payload to the Address field when creating or editing a list entry. The vulnerability is triggered when another user navigates to the Tools section and performs a gravity database update. The Address field does not properly sanitize input, allowing special characters and script tags to bypass validation. This has been patched in version 6.3.	N/A	More Details

CVE-2025-62827	Rejected reason: Not used	N/A	More Details
CVE-2025-62828	Rejected reason: Not used	N/A	More Details
CVE-2025-62829	Rejected reason: Not used	N/A	More Details
CVE-2025-62830	Rejected reason: Not used	N/A	More Details
CVE-2025-62831	Rejected reason: Not used	N/A	More Details
CVE-2025-62263	Multiple cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.3.7 through 7.4.3.103, and Liferay DXP 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 service pack 3 through update 36 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into an Account Role's "Title" text field to (1) view account role page, or (2) select account role page. Multiple cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.3.7 through 7.4.3.103, and Liferay DXP 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 service pack 3 through update 36 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into an Organization's "Name" text field to (1) view account page, (2) view account organization page, or (3) select account organization page.	N/A	More Details
CVE-2025-62832	Rejected reason: Not used	N/A	More Details
CVE-2025-62833	Rejected reason: Not used	N/A	More Details
CVE-2025-62834	Rejected reason: Not used	N/A	More Details
CVE-2025-62835	Rejected reason: Not used	N/A	More Details
CVE-2025-58356	Constellation is the first Confidential Kubernetes. The Constellation CVM image uses LUKS2-encrypted volumes for persistent storage. When opening an encrypted storage device, the CVM uses the libcryptsetup function crypt_activate_by_passhrase. If the VM is successful in opening the partition with the disk encryption key, it treats the volume as confidential. However, due to the unsafe handling of null keyslot algorithms in the cryptsetup 2.8.1, it is possible that the opened volume is not encrypted at all. Cryptsetup prior to version 2.8.1 does not report an error when processing LUKS2-formatted disks that use the cipher_null-ecb algorithm in the keyslot encryption field. This vulnerability is fixed in 2.24.0.	N/A	More Details
CVE-2025-62253	Open redirect vulnerability in page administration in Liferay Portal 7.4.0 through 7.4.3.97, and older unsupported versions, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions allows remote attackers to redirect users to arbitrary external URLs via the _com_liferay_layout_admin_web_portlet_GroupPagesPortlet_redirect parameter.	N/A	More Details
CVE-2025-11952	Stored Cross-site Scripting (XSS) in Oct8ne Chatbot v2.3. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by injecting a malicious payload through the creation of a transcript that is sent by email. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user, through /Records/SendSummaryMail.	N/A	More Details
CVE-2025-53533	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level advertisement and internet tracker blocking application. Pi-hole Admin Interface versions 6.2.1 and earlier are vulnerable to reflected cross-site scripting (XSS) via a malformed URL path. The 404 error page includes the requested path in the class attribute of the body tag without proper sanitization or escaping. An attacker can craft a URL containing an onload attribute that will execute arbitrary JavaScript code in the browser when a victim visits the malicious link. If an attacker sends a crafted pi-hole link to a victim and the victim visits it, attacker-controlled JavaScript code is executed in the browser of the victim. This has been patched in version 6.3.	N/A	More Details
CVE-2025-41108	The communication protocol implemented in Ghost Robotics Vision 60 v0.27.2 could allow an attacker to send commands to the robot from an external attack station, impersonating the control station (tablet) and gaining unauthorised full control of the robot. The absence of encryption and authentication mechanisms in the communication protocol allows an attacker to capture legitimate traffic between the robot and the controller, replicate it, and send any valid command to the robot from any attacking computer or device. The communication protocol used in this interface is based on MAVLink, a widely documented protocol, which increases the likelihood of attack. There are two methods for connecting to the robot remotely: Wi-Fi and 4G/LTE.	N/A	More Details
CVE-2025-41109	Ghost Robotics Vision 60 v0.27.2 includes, among its physical interfaces, three RJ45 connectors and a USB Type-C port. The vulnerability is due to the lack of authentication mechanisms when establishing connections through these ports. Specifically, with regard to network connectivity, the robot's internal router automatically assigns IP addresses to any device physically connected to it. An attacker could connect a WiFi access point under their control to gain access to the robot's network without needing the credentials for the deployed network. Once inside, the attacker can monitor all its data, as the robot runs on ROS 2	N/A	More Details

	without authentication by default.		
CVE-2025-41110	Encrypted WiFi and SSH credentials were found in the Ghost Robotics Vision 60 v0.27.2 APK. This vulnerability allows an attacker to connect to the robot's WiFi and view all its data, as it runs on ROS 2 without default authentication. In addition, the attacker can connect via SSH and gain full control of the robot, which could cause physical damage to the robot itself or its environment.	N/A	More Details
CVE-2025-34133	Wimi Teamwork versions prior to 7.38.17 contains a cross-site request forgery (CSRF) vulnerability in its API. The API accepts any authenticated request that contains a JSON field named 'csrf_token' without validating the field’s value; only the presence of the field is checked. An attacker can craft a cross-site request that causes a logged-in victim’s browser to submit a JSON POST containing an arbitrary or empty 'csrf_token', and the API will execute the request with the victim’s privileges. Successful exploitation can allow an attacker to perform privileged actions as the victim potentially resulting in account takeover, privilege escalation, or service disruption.	N/A	More Details
CVE-2022-50569	In the Linux kernel, the following vulnerability has been resolved: xfrm: Update ipcomp_scratches with NULL when freed Currently if ipcomp_alloc_scratches() fails to allocate memory ipcomp_scratches holds obsolete address. So when we try to free the percpu scratches using ipcomp_free_scratches() it tries to vfree non existent vm area. Described below: static void * __percpu *ipcomp_alloc_scratches(void) { ... scratches = alloc_percpu(void *); if (!scratches) return NULL; ipcomp_scratches does not know about this allocation failure. Therefore holding the old obsolete address. ... } So when we free, static void ipcomp_free_scratches(void) { ... scratches = ipcomp_scratches; Assigning obsolete address from ipcomp_scratches if (!scratches) return; for_each_possible_cpu(i) vfree(*per_cpu_ptr(scratches, i)); Trying to free non existent page, causing warning: trying to vfree existent vm area. ... } Fix this breakage by updating ipcomp_scrtches with NULL when scratches is freed	N/A	More Details
CVE-2022-50570	In the Linux kernel, the following vulnerability has been resolved: platform/chrome: fix memory corruption in ioctl If "s_mem.bytes" is larger than the buffer size it leads to memory corruption.	N/A	More Details
CVE-2023-53693	In the Linux kernel, the following vulnerability has been resolved: USB: gadget: Fix the memory leak in raw_gadget driver Currently, increasing raw_dev->count happens before invoke the raw_queue_event(), if the raw_queue_event() return error, invoke raw_release() will not trigger the dev_free() to be called. [268.905865][T5067] raw-gadget.0 gadget.0: failed to queue event [268.912053][T5067] udc dummy_udc.0: failed to start USB Raw Gadget: -12 [268.918885][T5067] raw-gadget.0: probe of gadget.0 failed with error -12 [268.925956][T5067] UDC core: USB Raw Gadget: couldn't find an available UDC or it's busy [268.934657][T5067] misc raw-gadget: fail, usb_gadget_register_driver returned -16 BUG: memory leak [<ffffffff8154bf94>] kmalloc_trace+0x24/0x90 mm/slab_common.c:1076 [<ffffffff8347eb55>] kmalloc include/linux/slab.h:582 [inline] [<ffffffff8347eb55>] kzalloc include/linux/slab.h:703 [inline] [<ffffffff8347eb55>] dev_new drivers/usb/gadget/legacy/raw_gadget.c:191 [inline] [<ffffffff8347eb55>] raw_open+0x45/0x110 drivers/usb/gadget/legacy/raw_gadget.c:385 [<ffffffff827d1d09>] misc_open+0x1a9/0x1f0 drivers/char/misc.c:165 [<ffffffff8154bf94>] kmalloc_trace+0x24/0x90 mm/slab_common.c:1076 [<ffffffff8347cd2f>] kmalloc include/linux/slab.h:582 [inline] [<ffffffff8347cd2f>] raw_ioctl_init+0xdf/0x410 drivers/usb/gadget/legacy/raw_gadget.c:460 [<ffffffff8347dfe9>] raw_ioctl+0x5f9/0x1120 drivers/usb/gadget/legacy/raw_gadget.c:1250 [<ffffffff81685173>] vfs_ioctl fs/ioctl.c:51 [inline] [<ffffffff8154bf94>] kmalloc_trace+0x24/0x90 mm/slab_common.c:1076 [<ffffffff833ecc6a>] kmalloc include/linux/slab.h:582 [inline] [<ffffffff833ecc6a>] kzalloc include/linux/slab.h:703 [inline] [<ffffffff833ecc6a>] dummy_alloc_request+0x5a/0xe0 drivers/usb/gadget/udc/dummy_hcd.c:665 [<ffffffff833e9132>] usb_ep_alloc_request+0x22/0xd0 drivers/usb/gadget/udc/core.c:196 [<ffffffff8347f13d>] gadget_bind+0x6d/0x370 drivers/usb/gadget/legacy/raw_gadget.c:292 This commit therefore invoke kref_get() under the condition that raw_queue_event() return success.	N/A	More Details
CVE-2023-53695	In the Linux kernel, the following vulnerability has been resolved: udf: Detect system inodes linked into directory hierarchy When UDF filesystem is corrupted, hidden system inodes can be linked into directory hierarchy which is an avenue for further serious corruption of the filesystem and kernel confusion as noticed by syzbot fuzzed images. Refuse to access system inodes linked into directory hierarchy and vice versa.	N/A	More Details
CVE-2023-53696	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Fix memory leak in qla2x00_probe_one() There is a memory leak reported by kmemleak: unreferenced object 0xffffc900003f0000 (size 12288): comm "modprobe", pid 19117, jiffies 4299751452 (age 42490.264s) hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace: [<00000000629261a8>] __vmalloc_node_range+0xe56/0x1110 [<0000000001906886>] __vmalloc_node+0xbd/0x150 [<000000005bb4dc34>] vmalloc+0x25/0x30 [<00000000a2dc1194>] qla2x00_create_host+0x7a0/0xe30 [qla2xxx] [<0000000062b14b47>] qla2x00_probe_one+0x2eb8/0xd160 [qla2xxx] [<00000000641ccc04>] local_pci_probe+0xeb/0x1a0 The root cause is traced to an error-handling path in qla2x00_probe_one() when the adapter "base_vha" initialize failed. The fab_scan_rp "scan.l" is used to record the port information and it is allocated in qla2x00_create_host(). However, it is not released in the error handling path "probe_failed". Fix this by freeing the memory of "scan.l" when an error occurs in the adapter initialization process.	N/A	More Details
CVE-2023-53697	In the Linux kernel, the following vulnerability has been resolved: nvdimm: Fix memleak of pmu attr_groups in unregister_nvdimm_pmu() Memory pointed by 'nd_pmu->pmu.attr_groups' is allocated in function 'register_nvdimm_pmu' and is lost after 'kfree(nd_pmu)' call in function 'unregister_nvdimm_pmu'.	N/A	More Details
CVE-2023-53698	In the Linux kernel, the following vulnerability has been resolved: xsk: fix refcount underflow in error path Fix a refcount underflow problem reported by syzbot that can happen when a system is running out of memory. If xp_alloc_tx_descs() fails, and it can only fail due to not having enough memory, then the error path is triggered. In this error path, the refcount of the pool is decremented as it has incremented before. However, the reference to the pool in the socket was not nulled. This means that when the socket is closed later, the socket teardown logic will think that there is a pool attached to the socket and try to decrease the refcount again, leading to a refcount underflow. I chose this fix as it involved adding just a single line. Another option would have been to move xp_get_pool() and the assignment of xs->pool to after the if-statement and using xs_umem->pool instead of xs->pool in the whole if-statement resulting in somewhat simpler code, but this would have led to much more churn in the code base perhaps making it harder to backport.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: riscv: move memblock_allow_resize() after linear mapping is ready The initial memblock metadata is accessed from kernel image mapping. The regions arrays need to "reallocated" from memblock and accessed through linear mapping to cover more memblock regions. So the resizing should not be allowed until		

CVE-2023-53699	linear mapping is ready. Note that there are memblock allocations when building linear mapping. This patch is similar to 24cc61d8cb5a ("arm64: memblock: don't permit memblock resizing until linear mapping is up"). In following log, many memblock regions are reserved before create_linear_mapping_page_table(). And then it triggered reallocation of memblock.reserved.regions and memcpy the old array in kernel image mapping to the new array in linear mapping which caused a page fault. [0.000000] memblock_reserve: [0x00000000bf01f000-0x00000000bf01ffff] early_init_fdt_scan_reserved_mem+0x28c/0x2c6 [0.000000] memblock_reserve: [0x00000000bf021000-0x00000000bf021fff] early_init_fdt_scan_reserved_mem+0x28c/0x2c6 [0.000000] memblock_reserve: [0x00000000bf023000-0x00000000bf023fff] early_init_fdt_scan_reserved_mem+0x28c/0x2c6 [0.000000] memblock_reserve: [0x00000000bf025000-0x00000000bf025fff] early_init_fdt_scan_reserved_mem+0x28c/0x2c6 [0.000000] memblock_reserve: [0x00000000bf027000-0x00000000bf027fff] early_init_fdt_scan_reserved_mem+0x28c/0x2c6 [0.000000] memblock_reserve: [0x00000000bf029000-0x00000000bf029fff] early_init_fdt_scan_reserved_mem+0x28c/0x2c6 [0.000000] memblock_reserve: [0x00000000bf02b000-0x00000000bf02bfff] early_init_fdt_scan_reserved_mem+0x28c/0x2c6 [0.000000] memblock_reserve: [0x00000000bf02d000-0x00000000bf02dfff] early_init_fdt_scan_reserved_mem+0x28c/0x2c6 [0.000000] memblock_reserve: [0x00000000bf02f000-0x00000000bf02ffff] early_init_fdt_scan_reserved_mem+0x28c/0x2c6 [0.000000] memblock_reserve: [0x00000000bf030000-0x00000000bf030fff] early_init_fdt_scan_reserved_mem+0x28c/0x2c6 [0.000000] OF: reserved mem: 0x0000000080000000..0x000000008007ffff (512 KiB) map non-reusable mmode_resv0@80000000 [0.000000] memblock_reserve: [0x00000000bf000000-0x00000000bf001fed] paging_init+0x19a/0x5ae [0.000000] memblock_phys_alloc_range: 4096 bytes align=0x1000 from=0x0000000000000000 max_addr=0x0000000000000000 alloc_pmd_fixmap+0x14/0x1c [0.000000] memblock_reserve: [0x000000017ffff000-0x000000017fffffff] memblock_alloc_range_nid+0xb8/0x128 [0.000000] memblock: reserved is doubled to 256 at [0x000000017fffd000-0x000000017fffe7ff] [0.000000] Unable to handle kernel paging request at virtual address ff600000ffffd000 [0.000000] Oops [#1] [0.000000] Modules linked in: [0.000000] CPU: 0 PID: 0 Comm: swapper Not tainted 6.4.0-rc1-00011-g99a670b2069c #66 [0.000000] Hardware name: riscv-virtio,qemu (DT) [0.000000] epc : __memcpy+0x60/0xf8 [0.000000] ra : memblock_double_array+0x192/0x248 [0.000000] epc : ffffffff8081d214 ra : ffffffff80a3dfc0 sp : ffffffff81403bd0 [0.000000] gp : ffffffff814fbb38 tp : ffffffff8140dac0 t0 : 0000000001600000 [0.000000] t1 : 0000000000000000 t2 : 000000008f001000 s0 : ffffffff81403c60 [0.000000] s1 : ffffffff80c0bc98 a0 : ff600000ffffd000 a1 : ffffffff80c0bcd8 [0.000000] a2 : 0000000000000c00 a3 : ffffffff80c0c8d8 a4 : 0000000080000000 [0.000000] a5 : 0000000000080000 a6 : 0000000000000000 a7 : 0000000080200000 [0.000000] s2 : ff600000ffffd000 s3 : 0000000000002000 s4 : 0000000000000c00 [0.000000] s5 : ffffffff80c0bc60 s6 : ffffffff80c0bcc8 s7 : 0000000000000000 [0.000000] s8 : ffffffff814fd0a8 s9 : 000000017fffe7ff s10: 0000000000000000 [0.000000] s11: 0000000000001000 t3 : 0000000000001000 t4 : 0000000000000000 [0.000000] t5 : 000000008f003000 t6 : ff600000ffffd000 [0.000000] status: 0000000200000100 badaddr: ff600000ffffd000 cause: 000000000000000f [0.000000] [<fff ---truncated---	N/A	More Details
CVE-2023-53700	In the Linux kernel, the following vulnerability has been resolved: media: max9286: Fix memleak in max9286_v4l2_register() There is a kmemleak when testing the media/i2c/max9286.c with bpf mock device: kmemleak: 5 new suspected memory leaks (see /sys/kernel/debug/kmemleak) unreferenced object 0xffff88810defc400 (size 256): comm "python3", pid 278, jiffies 4294737563 (age 31.978s) hex dump (first 32 bytes): 28 06 a7 0a 81 88 ff ff 00 fe 22 12 81 88 ff ff (.....".... 10 c4 ef 0d 81 88 ff ff 10 c4 ef 0d 81 88 ff ff ..... backtrace: [<00000000191de6a7>] __kmalloc_node+0x44/0x1b0 [<000000002f4912b7>] kvmalloc_node+0x34/0x180 [<0000000057dc4cae>] v4l2_ctrl_new+0x325/0x10f0 [videodev] [<0000000026030272>] v4l2_ctrl_new_std+0x16f/0x210 [videodev] [<00000000f0d9ea2f>] max9286_probe+0x76e/0xbff [max9286] [<00000000ea8f6455>] i2c_device_probe+0x28d/0x680 [<0000000087529af3>] really_probe+0x17c/0x3f0 [<00000000b08be526>] __driver_probe_device+0xe3/0x170 [<000000004382edea>] driver_probe_device+0x49/0x120 [<000000007bde528a>] __device_attach_driver+0xf7/0x150 [<000000009f9c6ab4>] bus_for_each_drv+0x114/0x180 [<00000000c8aaf588>] __device_attach+0x1e5/0x2d0 [<0000000041cc06b9>] bus_probe_device+0x126/0x140 [<000000002309860d>] device_add+0x810/0x1130 [<000000002827bf98>] i2c_new_client_device+0x359/0x4f0 [<00000000593bdc85>] of_i2c_register_device+0xf1/0x110 max9286_v4l2_register() calls v4l2_ctrl_new_std(), but won't free the created v412_ctrl when fwnode_graph_get_endpoint_by_id() failed, which causes the memleak. Call v4l2_ctrl_handler_free() to free the v412_ctrl.	N/A	More Details
CVE-2023-53701	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-53702	In the Linux kernel, the following vulnerability has been resolved: s390/crypto: use vector instructions only if available for ChaCha20 Commit 349d03ffd5f6 ("crypto: s390 - add crypto library interface for ChaCha20") added a library interface to the s390 specific ChaCha20 implementation. However no check was added to verify if the required facilities are installed before branching into the assembler code. If compiled into the kernel, this will lead to the following crash, if vector instructions are not available: data exception: 0007 ilc:3 [#1] SMP Modules linked in: CPU: 0 PID: 1 Comm: swapper/0 Not tainted 6.3.0-rc7+ #11 Hardware name: IBM 3931 A01 704 (KVM/Linux) Krnl PSW : 0704e00180000000 000000001857277a (chacha20_vx+0x32/0x818) R:0 T:1 IO:1 EX:1 Key:0 M:1 W:0 P:0 AS:3 CC:2 PM:0 RI:0 EA:3 Krnl GPRS: 0000037f0000000a ffffffffffffff60 000000008184b000 0000000019f5c8e6 0000000000000109 0000037fffb13c58 0000037fffb13c78 0000000019bb1780 0000037fffb13c58 0000000019f5c8e6 000000008184b000 0000000000000109 00000000802d8000 0000000000000109 0000000018571ebc 0000037fffb13718 Krnl Code: 000000001857276a: c07000b1f80b larl %r7,0000000019bb1780 0000000018572770: a708000a lhi %r0,10 #0000000018572774: e78950000c36 vlm %v24,%v25,0(%r5),0 >000000001857277a: e7a060000806 vl %v26,0(%r6),0 0000000018572780: e7bf70004c36 vlm %v27,%v31,0(%r7),4 0000000018572786: e70b00000456 vlr %v0,%v27 000000001857278c: e71800000456 vlr %v1,%v24 0000000018572792: e74b00000456 vlr %v4,%v27 Call Trace: [<000000001857277a>] chacha20_vx+0x32/0x818 Last Breaking-Event-Address: [<0000000018571eb6>] chacha20_crypt_s390.constprop.0+0x6e/0xd8 ---[end trace 0000000000000000]--- Kernel panic - not syncing: Attempted to kill init! exitcode=0x0000000b Fix this by adding a missing MACHINE_HAS_VX check. [agordeev@linux.ibm.com: remove duplicates in commit message]	N/A	More Details
CVE-2023-53703	In the Linux kernel, the following vulnerability has been resolved: HID: amd_sfh: Fix for shift-out-of-bounds Shift operation of 'exp' and 'shift' variables exceeds the maximum number of shift values in the u32 range leading to UBSAN shift-out-of-bounds. ... [6.120512] UBSAN: shift-out-of-bounds in drivers/hid/amd-sfh-hid/sfh1_1/amd_sfh_desc.c:149:50 [6.120598] shift exponent 104 is too large for 64-bit type 'long unsigned int' [6.120659] CPU: 4 PID: 96 Comm: kworker/4:1 Not tainted 6.4.0amd_1-next-20230519-dirty #10 [6.120665] Hardware name: AMD Birman-PHX/Birman-PHX, BIOS SFH_with_HPD_SEN.FD 04/05/2023 [6.120667] Workqueue: events amd_sfh_work_buffer [amd_sfh] [6.120687] Call Trace: [6.120690] <TASK> [6.120694] dump_stack_lvl+0x48/0x70 [6.120704] dump_stack+0x10/0x20 [6.120707] ubsan_epilogue+0x9/0x40 [6.120716] __ubsan_handle_shift_out_of_bounds+0x10f/0x170 [6.120720] ? psi_group_change+0x25f/0x4b0 [6.120729] float_to_int.cold+0x18/0xba [amd_sfh] [6.120739] get_input_rep+0x57/0x340 [amd_sfh] [6.120748] ?	N/A	More Details

	__schedule+0xba7/0x1b60 [6.120756] ? __pfx_get_input_rep+0x10/0x10 [amd_sfh] [6.120764] amd_sfh_work_buffer+0x91/0x180 [amd_sfh] [6.120772] process_one_work+0x229/0x430 [6.120780] worker_thread+0x4a/0x3c0 [6.120784] ? __pfx_worker_thread+0x10/0x10 [6.120788] kthread+0xf7/0x130 [6.120792] ? __pfx_kthread+0x10/0x10 [6.120795] ret_from_fork+0x29/0x50 [6.120804] </TASK> ... Fix this by adding the condition to validate shift ranges.		
CVE-2025-12080	On Wear OS devices, when Google Messages is configured as the default SMS/MMS/RCS application, the handling of ACTION_SENDTO intents utilizing the sms:, smsto:, mms:, and mmsto: Uniform Resource Identifier (URI) schemes is incorrectly implemented. Due to this misconfiguration, an attacker capable of invoking an Android intent can exploit this vulnerability to send messages on the user’s behalf to arbitrary receivers without requiring any further user interaction or specific permissions. This allows for the silent and unauthorized transmission of messages from a compromised Wear OS device.	N/A	More Details
CVE-2023-53704	In the Linux kernel, the following vulnerability has been resolved: clk: imx: clk-imx8mp: improve error handling in imx8mp_clocks_probe() Replace of_iomap() and kzalloc() with devm_of_iomap() and devm_kzalloc() which can automatically release the related memory when the device or driver is removed or unloaded to avoid potential memory leak. In this case, iounmap(anatop_base) in line 427,433 are removed as manual release is not required. Besides, referring to clk-imx8mq.c, check the return code of of_clk_add_hw_provider, if it returns negtive, print error info and unregister hws, which makes the program more robust.	N/A	More Details
CVE-2023-53705	In the Linux kernel, the following vulnerability has been resolved: ipv6: Fix out-of-bounds access in ipv6_find_tlv() optlen is fetched without checking whether there is more than one byte to parse. It can lead to out-of-bounds access. Found by InfoTeCS on behalf of Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2025-11682	Stored cross-site scripting (XSS) vulnerability in the LMT Dashboard of the Perx Customer Engagement & Loyalty Platform allows an authenticated attacker to execute arbitrary JavaScript code in a victim's browser. The vulnerability is due to improper sanitization of SVG file uploads. An attacker can upload a malicious SVG file containing a script payload to a campaign. When another user views this image on the public LMT microsite, the script executes, which can lead to session hijacking, data theft, or other unauthorized actions.This issue affects Customer Engagement & Loyalty Platform before 4.617.4.	N/A	More Details
CVE-2023-53706	In the Linux kernel, the following vulnerability has been resolved: mm/vmemmap/devdax: fix kernel crash when probing devdax devices commit 4917f55b4ef9 ("mm/sparse-vmemmap: improve memory savings for compound devmaps") added support for using optimized vmmemap for devdax devices. But how vmemmap mappings are created are architecture specific. For example, powerpc with hash translation doesn't have vmemmap mappings in init_mm page table instead they are bolted table entries in the hardware page table vmemmap_populate_compound_pages() used by vmemmap optimization code is not aware of these architecture-specific mapping. Hence allow architecture to opt for this feature. I selected architectures supporting HUGETLB_PAGE_OPTIMIZE_VMEMMAP option as also supporting this feature. This patch fixes the below crash on ppc64. BUG: Unable to handle kernel data access on write at 0xc00c000100400038 Faulting instruction address: 0xc000000001269d90 Oops: Kernel access of bad area, sig: 11 [#1] LE PAGE_SIZE=64K MMU=Hash SMP NR_CPUS=2048 NUMA pSeries Modules linked in: CPU: 7 PID: 1 Comm: swapper/0 Not tainted 6.3.0-rc5-150500.34-default+ #2 5c90a668b6bbd142599890245c2fb5de19d7d28a Hardware name: IBM,9009-42G POWER9 (raw) 0x4e0202 0xf000005 of:IBM,FW950.40 (VL950_099) hv:phyp pSeries NIP: c000000001269d90 LR: c0000000004c57d4 CTR: 0000000000000000 REGS: c000000003632c30 TRAP: 0300 Not tainted (6.3.0-rc5-150500.34-default+) MSR: 8000000000009033 <SF,EE,ME,IR,DR,RI,LE> CR: 24842228 XER: 00000000 CFAR: c0000000004c57d0 DAR: c00c000100400038 DSISR: 42000000 IRQMASK: 0 .... NIP [c000000001269d90] __init_single_page.isra.74+0x14/0x4c LR [c0000000004c57d4] __init_zone_device_page+0x44/0xd0 Call Trace: [c000000003632ed0] [c000000003632f60] 0xc000000003632f60 (unreliable) [c000000003632f10] [c0000000004c5ca0] memmap_init_zone_device+0x170/0x250 [c000000003632fe0] [c0000000005575f8] memremap_pages+0x2c8/0x7f0 [c0000000036330c0] [c000000000557b5c] devm_memremap_pages+0x3c/0xa0 [c000000003633100] [c000000000d458a8] dev_dax_probe+0x108/0x3e0 [c0000000036331a0] [c000000000d41430] dax_bus_probe+0xb0/0x140 [c0000000036331d0] [c000000000cef27c] really_probe+0x19c/0x520 [c000000003633260] [c000000000cef6b4] __driver_probe_device+0xb4/0x230 [c0000000036332e0] [c000000000cef888] driver_probe_device+0x58/0x120 [c000000003633320] [c000000000cefa6c] __device_attach_driver+0x11c/0x1e0 [c0000000036333a0] [c000000000cebc58] bus_for_each_drv+0xa8/0x130 [c000000003633400] [c000000000ceefcc] __device_attach+0x15c/0x250 [c0000000036334a0] [c000000000ced458] bus_probe_device+0x108/0x110 [c0000000036334f0] [c000000000ce92dc] device_add+0x7fc/0xa10 [c0000000036335b0] [c000000000d447c8] devm_create_dev_dax+0x1d8/0x530 [c000000003633640] [c000000000d46b60] __dax_pmem_probe+0x200/0x270 [c0000000036337b0] [c000000000d46bf0] dax_pmem_probe+0x20/0x70 [c0000000036337d0] [c000000000d2279c] nvdimm_bus_probe+0xac/0x2b0 [c000000003633860] [c000000000cef27c] really_probe+0x19c/0x520 [c0000000036338f0] [c000000000cef6b4] __driver_probe_device+0xb4/0x230 [c000000003633970] [c000000000cef888] driver_probe_device+0x58/0x120 [c0000000036339b0] [c000000000cefd08] __driver_attach+0x1d8/0x240 [c000000003633a30] [c000000000cebb04] bus_for_each_dev+0xb4/0x130 [c000000003633a90] [c000000000cee564] driver_attach+0x34/0x50 [c000000003633ab0] [c000000000ced878] bus_add_driver+0x218/0x300 [c000000003633b40] [c000000000cf1144] driver_register+0xa4/0x1b0 [c000000003633bb0] [c000000000d21a0c] __nd_driver_register+0x5c/0x100 [c000000003633c10] [c00000000206a2e8] dax_pmem_init+0x34/0x48 [c000000003633c30] [c0000000000132d0] do_one_initcall+0x60/0x320 [c000000003633d00] [c0000000020051b0] kernel_init_freeable+0x360/0x400 [c000000003633de0] [c0000000000013764] kernel_init+0x34/0x1d0 [c000000003633e50] [c00000000000de14] ret_from_kernel_thread+0x5c/0x64	N/A	More Details
CVE-2023-53707	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix integer overflow in amdgpu_cs_pass1 The type of size is unsigned int, if size is 0x40000000, there will be an integer overflow, size will be zero after size *= sizeof(uint32_t), will cause uninitialized memory to be referenced later.	N/A	More Details
CVE-2023-53708	In the Linux kernel, the following vulnerability has been resolved: ACPI: x86: s2idle: Catch multiple ACPI_TYPE_PACKAGE objects If a badly constructed firmware includes multiple `ACPI_TYPE_PACKAGE` objects while evaluating the AMD LPS0 _DSM, there will be a memory leak. Explicitly guard against this.	N/A	More Details
CVE-2025-10355	Open redirection vulnerability in MOLGENIS EMX2 v11.14.0. This vulnerability allows an attacker to create a malicious URL using a manipulated redirection parameter, potentially leading users to phishing sites or other malicious destinations via “/%2f%2f<MALICIOUS_DOMAIN>”.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: riscv: ftrace: Fixup panic by disabling preemption In RISCV, we must use an AUIPC + JALR pair to encode an immediate, forming a jump that jumps to an address over 4K. This may cause		

CVE-2023-53694	errors if we want to enable kernel preemption and remove dependency from patching code with stop_machine(). For example, if a task was switched out on auipc. And, if we changed the ftrace function before it was switched back, then it would jump to an address that has updated 11:0 bits mixing with previous XLEN:12 part. p: patched area performed by dynamic ftrace ftrace_prologue: p| REG_S ra, -SZREG(sp) p| auipc ra, 0x? ----------> preempted ... change ftrace function ... p| jalr -?(ra) <---------- switched back p| REG_L ra, -SZREG(sp) func: xxx ret	N/A	More Details
CVE-2025-11955	Incorrect validation of OCSP certificates vulnerability in TheGreenBow VPN, versions 7.5 and 7.6. During the IKEv2 authentication step, the OCSP-enabled VPN client establishes the tunnel even if it does not receive an OCSP response or if the OCSP response signature is invalid.	N/A	More Details
CVE-2022-50571	In the Linux kernel, the following vulnerability has been resolved: btrfs: call __btrfs_remove_free_space_cache_locked on cache load failure Now that lockdep is staying enabled through our entire CI runs I started seeing the following stack in generic/475 ----------[cut here]------------ WARNING: CPU: 1 PID: 2171864 at fs/btrfs/discard.c:604 btrfs_discard_update_discardable+0x98/0xb0 CPU: 1 PID: 2171864 Comm: kworker/u4:0 Not tainted 5.19.0-rc8+ #789 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.13.0-2.fc32 04/01/2014 Workqueue: btrfs-cache btrfs_work_helper RIP: 0010:btrfs_discard_update_discardable+0x98/0xb0 RSP: 0018:ffffb857c2f7bad0 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffff8c85c605c200 RCX: 0000000000000001 RDX: 0000000000000000 RSI: ffffffff86807c5b RDI: ffffffff868a831e RBP: ffff8c85c4c54000 R08: 0000000000000000 R09: 0000000000000000 R10: ffff8c85c66932f0 R11: 0000000000000001 R12: ffff8c85c3899010 R13: ffff8c85d5be4f40 R14: ffff8c85c4c54000 R15: ffff8c86114bfa80 FS: 0000000000000000(0000) GS:ffff8c863bd00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f2e7f168160 CR3: 000000010289a004 CR4: 0000000000370ee0 Call Trace: __btrfs_remove_free_space_cache+0x27/0x30 load_free_space_cache+0xad2/0xaf0 caching_thread+0x40b/0x650 ? lock_release+0x137/0x2d0 btrfs_work_helper+0xf2/0x3e0 ? lock_is_held_type+0xe2/0x140 process_one_work+0x271/0x590 ? process_one_work+0x590/0x590 worker_thread+0x52/0x3b0 ? process_one_work+0x590/0x590 kthread+0xf0/0x120 ? kthread_complete_and_exit+0x20/0x20 ret_from_fork+0x1f/0x30 This is the code ctl = block_group->free_space_ctl; discard_ctl = &block_group->fs_info->discard_ctl; lockdep_assert_held(&ctl->tree_lock); We have a temporary free space ctl for loading the free space cache in order to avoid having allocations happening while we're loading the cache. When we hit an error we free it all up, however this also calls btrfs_discard_update_discardable, which requires block_group->free_space_ctl->tree_lock to be held. However this is our temporary ctl so this lock isn't held. Fix this by calling __btrfs_remove_free_space_cache_locked instead so that we only clean up the entries and do not mess with the discardable stats.	N/A	More Details
CVE-2023-53692	In the Linux kernel, the following vulnerability has been resolved: ext4: fix use-after-free read in ext4_find_extent for bigalloc + inline Syzbot found the following issue: loop0: detected capacity change from 0 to 2048 EXT4-fs (loop0): mounted filesystem 00000000-0000-0000-0000-000000000000 without journal. Quota mode: none. == BUG: KASAN: use-after-free in ext4_ext_binsearch_idx fs/ext4/extents.c:768 [inline] BUG: KASAN: use-after-free in ext4_find_extent+0x76e/0xd90 fs/ext4/extents.c:931 Read of size 4 at addr ffff888073644750 by task syz-executor420/5067 CPU: 0 PID: 5067 Comm: syz-executor420 Not tainted 6.2.0-rc1-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/26/2022 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x1b1/0x290 lib/dump_stack.c:106 print_address_description+0x74/0x340 mm/kasan/report.c:306 print_report+0x107/0x1f0 mm/kasan/report.c:417 kasan_report+0xcd/0x100 mm/kasan/report.c:517 ext4_ext_binsearch_idx fs/ext4/extents.c:768 [inline] ext4_find_extent+0x76e/0xd90 fs/ext4/extents.c:931 ext4_clu_mapped+0x117/0x970 fs/ext4/extents.c:5809 ext4_insert_delayed_block fs/ext4/inode.c:1696 [inline] ext4_da_map_blocks fs/ext4/inode.c:1806 [inline] ext4_da_get_block_prep+0x9e8/0x13c0 fs/ext4/inode.c:1870 ext4_block_write_begin+0x6a8/0x2290 fs/ext4/inode.c:1098 ext4_da_write_begin+0x539/0x760 fs/ext4/inode.c:3082 generic_perform_write+0x2e4/0x5e0 mm/filemap.c:3772 ext4_buffered_write_iter+0x122/0x3a0 fs/ext4/file.c:285 ext4_file_write_iter+0x1d0/0x18f0 call_write_iter include/linux/fs.h:2186 [inline] new_sync_write fs/read_write.c:491 [inline] vfs_write+0x7dc/0xc50 fs/read_write.c:584 ksys_write+0x177/0x2a0 fs/read_write.c:637 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x3d/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd RIP: 0033:0x7f4b7a9737b9 RSP: 002b:00007ffc5cac3668 EFLAGS: 00000246 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007f4b7a9737b9 RDX: 00000000175d9003 RSI: 0000000020000200 RDI: 0000000000000004 RBP: 00007f4b7a933050 R08: 0000000000000000 R09: 0000000000000000 R10: 000000000000079f R11: 0000000000000246 R12: 00007f4b7a9330e0 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 </TASK> Above issue is happens when enable bigalloc and inline data feature. As commit 131294c35ed6 fixed delayed allocation bug in ext4_clu_mapped for bigalloc + inline. But it only resolved issue when has inline data, if inline data has been converted to extent(ext4_da_convert_inline_data_to_extent) before writepages, there is no EXT4_STATE_MAY_INLINE_DATA flag. However i_data is still store inline data in this scene. Then will trigger UAF when find extent. To resolve above issue, there is need to add judge "ext4_has_inline_data(inode)" in ext4_clu_mapped().	N/A	More Details
CVE-2022-50572	In the Linux kernel, the following vulnerability has been resolved: ASoC: audio-graph-card: fix refcount leak of cpu_ep in __graph_for_each_link() The of_get_next_child() returns a node with refcount incremented, and decrements the refcount of prev. So in the error path of the while loop, of_node_put() needs be called for cpu_ep.	N/A	More Details
CVE-2022-50573	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7915: fix mt7915_rate_txpower_get() resource leaks Coverity message: variable "buf" going out of scope leaks the storage. Addresses-Coverity-ID: 1527799 ("Resource leaks")	N/A	More Details
CVE-2025-52264	StarCharge Artemis AC Charger 7-22 kW v1.0.4 was discovered to contain a stack overflow via the cgiMain function at download.cgi.	N/A	More Details
CVE-2025-34292	Rox, the software running BeWelcome, contains a PHP object injection vulnerability resulting from deserialization of untrusted data. User-controlled input is passed to PHP's unserialize(): the POST parameter `formkit_memory_recovery` in \\RoxPostHandler::getCallbackAction and the 'memory cookie' read by \\RoxModelBase::getMemoryCookie (bwRemember). (1) If present, `formkit_memory_recovery` is processed and passed to unserialize(), and (2) restore-from-memory functionality calls unserialize() on the bwRemember cookie value. Gadget chains present in Rox and bundled libraries enable exploitation of object injection to write arbitrary files or achieve remote code execution. Successful exploitation can lead to full site compromise. This vulnerability was remediated with commit c60bf04 (2025-06-16).	N/A	More Details
CVE-	Unexpected authentication form rendering in HTML Form Adapter using only non-default redirectless mode in PingFederate		More

2025-26862	allows authentication attempts which may enable brute force login attacks.	N/A	Details
CVE-2022-50574	In the Linux kernel, the following vulnerability has been resolved: drm/omap: dss: Fix refcount leak bugs In dss_init_ports() and __dss_uninit_ports(), we should call of_node_put() for the reference returned by of_graph_get_port_by_id() in fail path or when it is not used anymore.	N/A	More Details
CVE-2025-9164	Docker Desktop Installer.exe is vulnerable to DLL hijacking due to insecure DLL search order. The installer searches for required DLLs in the user's Downloads folder before checking system directories, allowing local privilege escalation through malicious DLL placement.This issue affects Docker Desktop: through 4.48.0.	N/A	More Details
CVE-2022-50575	In the Linux kernel, the following vulnerability has been resolved: xen/privcmd: Fix a possible warning in privcmd_ioctl_mmap_resource() As 'kdata.num' is user-controlled data, if user tries to allocate memory larger than(>=) MAX_ORDER, then kcalloc() will fail, it creates a stack trace and messes up dmesg with a warning. Call trace: -> privcmd_ioctl --> privcmd_ioctl_mmap_resource Add __GFP_NOWARN in order to avoid too large allocation warning. This is detected by static analysis using smatch.	N/A	More Details
CVE-2025-50055	Cross-site scripting (XSS) vulnerability in the SAML Authentication module in OpenVPN Access Server version 2.14.0 through 2.14.3 allows configured remote SAML Assertion Consumer Service (ACS) endpoint servers to inject arbitrary web script or HTML via the RelayState parameter	N/A	More Details
CVE-2022-50576	In the Linux kernel, the following vulnerability has been resolved: serial: pch: Fix PCI device refcount leak in pch_request_dma() As comment of pci_get_slot() says, it returns a pci_device with its refcount increased. The caller must decrement the reference count by calling pci_dev_put(). Since 'dma_dev' is only used to filter the channel in filter(), we can call pci_dev_put() before exiting from pch_request_dma(). Add the missing pci_dev_put() for the normal and error path.	N/A	More Details
CVE-2022-50577	In the Linux kernel, the following vulnerability has been resolved: ima: Fix memory leak in __ima_inode_hash() Commit f3cc6b25dcc5 ("ima: always measure and audit files in policy") lets measurement or audit happen even if the file digest cannot be calculated. As a result, iint->ima_hash could have been allocated despite ima_collect_measurement() returning an error. Since ima_hash belongs to a temporary inode metadata structure, declared at the beginning of __ima_inode_hash(), just add a kfree() call if ima_collect_measurement() returns an error different from -ENOMEM (in that case, ima_hash should not have been allocated).	N/A	More Details
CVE-2022-50578	In the Linux kernel, the following vulnerability has been resolved: class: fix possible memory leak in __class_register() If class_add_groups() returns error, the 'cp->subsys' need be unregister, and the 'cp' need be freed. We can not call kset_unregister() here, because the 'cls' will be freed in callback function class_release() and it's also freed in caller's error path, it will cause double free. So fix this by calling kobject_del() and kfree_const(name) to cleanup kobject. Besides, call kfree() to free the 'cp'. Fault injection test can trigger this: unreferenced object 0xffff888102fa8190 (size 8): comm "modprobe", pid 502, jiffies 4294906074 (age 49.296s) hex dump (first 8 bytes): 70 6b 74 63 64 76 64 00 pktcdvd. backtrace: [<00000000e7c7703d>] __kmalloc_track_caller+0x1ae/0x320 [<000000005e4d70bc>] kstrdup+0x3a/0x70 [<00000000c2e5e85a>] kstrdup_const+0x68/0x80 [<0000000049a8c7>] kvasprintf_const+0x10b/0x190 [<0000000029123163>] kobject_set_name_vargs+0x56/0x150 [<00000000747219c9>] kobject_set_name+0xab/0xe0 [<0000000005f1ea4e>] __class_register+0x15c/0x49a unreferenced object 0xffff888037274000 (size 1024): comm "modprobe", pid 502, jiffies 4294906074 (age 49.296s) hex dump (first 32 bytes): 00 40 27 37 80 88 ff ff 00 40 27 37 80 88 ff ff .@'7.....@'7.... 00 00 00 00 ad 4e ad de ff ff ff ff 00 00 00 00 .....N..... backtrace: [<00000000151f9600>] kmem_cache_alloc_trace+0x17c/0x2f0 [<00000000ecf3dd95>] __class_register+0x86/0x49a	N/A	More Details
CVE-2022-50579	In the Linux kernel, the following vulnerability has been resolved: arm64: ftrace: fix module PLTs with mcount Li Huafei reports that mcount-based ftrace with module PLTs was broken by commit: a6253579977e4c6f ("arm64: ftrace: consistently handle PLTs.") When a module PLTs are used and a module is loaded sufficiently far away from the kernel, we'll create PLTs for any branches which are out-of-range. These are separate from the special ftrace trampoline PLTs, which the module PLT code doesn't directly manipulate. When mcount is in use this is a problem, as each mcount callsite in a module will be initialized to point to a module PLT, but since commit a6253579977e4c6f ftrace_make_nop() will assume that the callsite has been initialized to point to the special ftrace trampoline PLT, and ftrace_find_callable_addr() rejects other cases. This means that when ftrace tries to initialize a callsite via ftrace_make_nop(), the call to ftrace_find_callable_addr() will find that the `_mcount` stub is out-of-range and is not handled by the ftrace PLT, resulting in a splat: | ftrace_test: loading out-of-tree module taints kernel. | ftrace: no module PLT for _mcount | ------------[ftrace bug]------------ | ftrace failed to modify | [<ffff800029180014>] 0xffff800029180014 | actual: 44:00:00:94 | Initializing ftrace call sites | ftrace record flags: 2000000 | (0) | expected tramp: ffff80000802eb3c | ------------[cut here]------------ | WARNING: CPU: 3 PID: 157 at kernel/trace/ftrace.c:2120 ftrace_bug+0x94/0x270 | Modules linked in: | CPU: 3 PID: 157 Comm: insmod Tainted: G O 6.0.0-rc6-00151-gcd722513a189-dirty #22 | Hardware name: linux,dummy-virt (DT) | pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) | pc : ftrace_bug+0x94/0x270 | lr : ftrace_bug+0x21c/0x270 | sp : ffff80000b2bbaf0 | x29: ffff80000b2bbaf0 x28: 0000000000000000 x27: ffff0000c4d38000 | x26: 0000000000000001 x25: ffff800009d7e000 x24: ffff0000c4d86e00 | x23: 0000000002000000 x22: ffff80000a62b000 x21: ffff8000098ebea8 | x20: ffff0000c4d38000 x19: ffff80000aa24158 x18: ffffffffffffffff | x17: 0000000000000000 x16: 0a0d2d2d2d2d2d2d x15: ffff800009aa9118 | x14: 0000000000000000 x13: 6333626532303830 x12: 3030303866666666 | x11: 203a706d61727420 x10: 6465746365707865 x9 : 3362653230383030 | x8 : c0000000ffffefff x7 : 0000000000017fe8 x6 : 000000000000bff4 | x5 : 0000000000057fa8 x4 : 0000000000000000 x3 : 0000000000000001 | x2 : ad2cb14bb5438900 x1 : 0000000000000000 x0 : 0000000000000022 | Call trace: | ftrace_bug+0x94/0x270 | ftrace_process_locs+0x308/0x430 | ftrace_module_init+0x44/0x60 | load_module+0x15b4/0x1ce8 | __do_sys_init_module+0x1ec/0x238 | __arm64_sys_init_module+0x24/0x30 | invoke_syscall+0x54/0x118 | el0_svc_common.constprop.4+0x84/0x100 | do_el0_svc+0x3c/0xd0 | el0_svc+0x1c/0x50 | el0t_64_sync_handler+0x90/0xb8 | el0t_64_sync+0x15c/0x160 | ---[end trace 0000000000000000]--- | ---------test_init---------- Fix this by reverting to the old behaviour of ignoring the old instruction when initialising an mcount callsite in a module, which was the behaviour prior to commit a6253579977e4c6f.	N/A	More Details
CVE-2025-12176	Undocumented administrative accounts were getting created to facilitate access for applications running on board.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: hfs: fix OOB Read in __hfs_brec_find Syzbot reported a OOB		

CVE-2022-50581	read bug: == BUG: KASAN: slab-out-of-bounds in hfs_strcmp+0x117/0x190 fs/hfs/string.c:84 Read of size 1 at addr ffff88807eb62c4e by task kworker/u4:1/11 CPU: 1 PID: 11 Comm: kworker/u4:1 Not tainted 6.1.0-rc6-syzkaller-00308-g644e9524388a #0 Workqueue: writeback wb_workfn (flush-7:0) Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x1b1/0x28e lib/dump_stack.c:106 print_address_description+0x74/0x340 mm/kasan/report.c:284 print_report+0x107/0x1f0 mm/kasan/report.c:395 kasan_report+0xcd/0x100 mm/kasan/report.c:495 hfs_strcmp+0x117/0x190 fs/hfs/string.c:84 __hfs_brec_find+0x213/0x5c0 fs/hfs/bfind.c:75 hfs_brec_find+0x276/0x520 fs/hfs/bfind.c:138 hfs_write_inode+0x34c/0xb40 fs/hfs/inode.c:462 write_inode fs/fs-writeback.c:1440 [inline] If the input inode of hfs_write_inode() is incorrect: struct inode struct hfs_inode_info struct hfs_cat_key struct hfs_name u8 len # len is greater than HFS_NAMELEN(31) which is the maximum length of an HFS filename OOB read occurred: hfs_write_inode() hfs_brec_find() __hfs_brec_find() hfs_cat_keycmp() hfs_strcmp() # OOB read occurred due to len is too large Fix this by adding a Check on len in hfs_write_inode() before calling hfs_brec_find().	N/A	More Details
CVE-2025-41009	SQL injection vulnerability in the DRED virtual campus platform. This vulnerability allows an attacker to retrieve, create, update, and delete data from the database by sending a POST request using the ‘buscame’ parameter in ‘/catalogo_c/catalogo.php’.	N/A	More Details
CVE-2022-50582	In the Linux kernel, the following vulnerability has been resolved: regulator: core: Prevent integer underflow By using a ratio of delay to poll_enabled_time that is not integer time_remaining underflows and does not exit the loop as expected. As delay could be derived from DT and poll_enabled_time is defined in the driver this can easily happen. Use a signed iterator to make sure that the loop exits once the remaining time is negative.	N/A	More Details
CVE-2025-22167	This High severity Path Traversal (Arbitrary Write) vulnerability was introduced in versions: 9.12.0, 10.3.0 and remain present in 11.0.0 of Jira Software Data Center and Server. This Path Traversal (Arbitrary Write) vulnerability, with a CVSS Score of 8.7, allows an attacker to modify any filesystem path writable by the Jira JVM process. Atlassian recommends that Jira Software Data Center and Server customers upgrade to the latest version; if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Jira Software Data Center and Server 9.12: Upgrade to a release greater than or equal to 9.12.28 Jira Software Data Center and Server 10.3: Upgrade to a release greater than or equal to 10.3.12 Jira Software Data Center and Server 11.0: Upgrade to a release greater than or equal to 11.1.0 See the release notes. You can download the latest version of Jira Software Data Center and Server from the download center. This vulnerability was reported via our Atlassian (Internal) program.	N/A	More Details