SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 16 July 2025

Generated on 16 July 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-2025-53833	LaRecipe is an application that allows users to create documentation with Markdown inside a Laravel app. Versions prior to 2.8.1 are vulnerable to Server-Side Template Injection (SSTI), which could potentially lead to Remote Code Execution (RCE) in vulnerable configurations. Attackers could execute arbitrary commands on the server, access sensitive environment variables, and/or escalate access depending on server configuration. Users are strongly advised to upgrade to version v2.8.1 or later to receive a patch.	10.0	More Details
CVE-2025-3499	The device has two web servers that expose unauthenticated REST APIs on the management network (TCP ports 8084 and 8086). Exploiting OS command injection through these APIs, an attacker can send arbitrary commands that are executed with administrative permissions by the underlying operating system.	10.0	More Details
CVE-2025-53624	The Docusaurus gists plugin adds a page to your Docusaurus instance, displaying all public gists of a GitHub user. docusaurus-plugin-content-gists versions prior to 4.0.0 are vulnerable to exposing GitHub Personal Access Tokens in production build artifacts when passed through plugin configuration options. The token, intended for build-time API access only, is inadvertently included in client-side JavaScript bundles, making it accessible to anyone who can view the website's source code. This vulnerability is fixed in 4.0.0.	10.0	More Details
CVE-2025-47812	In Wing FTP Server before 7.4.4. the user and admin web interfaces mishandle '\0' bytes, ultimately allowing injection of arbitrary Lua code into user session files. This can be used to execute arbitrary system commands with the privileges of the FTP service (root or SYSTEM by default). This is thus a remote code execution vulnerability that guarantees a total server compromise. This is also exploitable via anonymous FTP accounts.	10.0	More Details
CVE-2025-53836	XWiki Rendering is a generic rendering system that converts textual input in a given syntax (wiki syntax, HTML, etc) into another syntax (XHTML, etc). Starting in version 4.2-milestone-1 and prior to versions 13.10.11, 14.4.7, and 14.10, the default macro content parser doesn't preserve the restricted attribute of the transformation context when executing nested macros. This allows executing macros that are normally forbidden in restricted mode, in particular script macros. The cache and chart macros that are bundled in XWiki use the vulnerable feature. This has been patched in XWiki 13.10.11, 14.4.7 and 14.10. To avoid the exploitation of this bug, comments can be disabled for untrusted users until an upgrade to a patched version has been performed. Note that users with edit rights will still be able to add comments via the object editor even if comments have been disabled.	9.9	More Details
CVE-2025-3498	An unauthenticated user with management network access can get and modify the Radiflow iSAP Smart Collector (CentOS 7 - VSAP 1.20) configuration. The device has two web servers that expose unauthenticated REST APIs on the management network (TCP ports 8084 and 8086). An attacker can use these APIs to get access to all system settings, modify the configuration and execute some commands (e.g., system reboot).	9.9	More Details
CVE-2025-4855	The Support Board plugin for WordPress is vulnerable to unauthorized access/modification/deletion of data due to use of hardcoded default secrets in the sb_encryption() function in all versions up to, and including, 3.8.0. This makes it possible for unauthenticated attackers to bypass authorization and execute arbitrary AJAX actions defined in the sb_ajax_execute() function. An attacker can use this vulnerability to exploit CVE-2025-4828 and various other functions unauthenticated.	9.8	More Details
CVE-2020-36849	The AIT CSV import/export plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the /wp-content/plugins/ait-csv-import-export/admin/upload-handler.php file in versions up to, and including, 3.0.3. This makes it possible for unauthorized attackers to upload arbitrary files on the affected sites server which may make remote code execution possible.	9.8	More Details
CVE-2025-7451	The iSherlock developed by Hgiga has an OS Command Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary OS commands and execute them on the server. This vulnerability has already been exploited. Please	9.8	More Details

	update immediately.		
CVE-2025-7574	A vulnerability, which was classified as critical, was found in LB-LINK BL-AC1900, BL-AC2100_AZ3, BL-AC3600, BL-AX1800, BL-AX5400P and BL-WR9000 up to 20250702. Affected is the function reboot/restore of the file /cgi-bin/lighttpd.cgi of the component Web Interface. The manipulation leads to improper authentication. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2025-50756	Wavlink WN535K3 20191010 was found to contain a command injection vulnerability in the set_sys_adm function via the newpass parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2025-4828	The Support Board plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the sb_file_delete function in all versions up to, and including, 3.8.0. This makes it possible for attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). An attacker can leverage CVE-2025-4855 vulnerability to exploit this vulnerability unauthenticated.	9.8	More Details
CVE-2023-38036	A security vulnerability within Ivanti Avalanche Manager before version 6.4.1 may allow an unauthenticated attacker to create a buffer overflow that could result in service disruption or arbitrary code execution.	9.8	More Details
CVE-2025-53890	pyload is an open-source Download Manager written in pure Python. An unsafe JavaScript evaluation vulnerability in pyLoad's CAPTCHA processing code allows unauthenticated remote attackers to execute arbitrary code in the client browser and potentially the backend server. Exploitation requires no user interaction or authentication and can result in session hijacking, credential theft, and full system remote code execution. Commit 909e5c97885237530d1264cfceb5555870eb9546, the patch for the issue, is included in version 0.5.0b3.dev89.	9.8	More Details
CVE-2025-5394	The Alone – Charity Multipurpose Non-profit WordPress Theme theme for WordPress is vulnerable to arbitrary file uploads due to a missing capability check on the alone_import_pack_install_plugin() function in all versions up to, and including, 7.8.3. This makes it possible for unauthenticated attackers to upload zip files containing webshells disguised as plugins from remote locations to achieve remote code execution.	9.8	More Details
CVE-2025-7340	The HT Contact Form Widget For Elementor Page Builder & Gutenberg Blocks & Form Builder. plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the temp_file_upload function in all versions up to, and including, 2.2.1. 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-2025-52376	An authentication bypass vulnerability in the /web/um_open_telnet.cgi endpoint in Nexxt Solutions NCM-X1800 Mesh Router firmware UV1.2.7 and below, allowing an attacker to remotely enable the Telnet service without authentication, bypassing security controls. The Telnet server is then accessible with hard-coded credentials, allowing attackers to gain administrative shell access and execute arbitrary commands on the device.	9.8	More Details
CVE-2025-6058	The WPBookit plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the image_upload_handle() function hooked via the 'add_booking_type' route in all versions up to, and including, 1.0.4. 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-2020-36847	The Simple-File-List Plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 4.2.2 via the rename function which can be used to rename uploaded PHP code with a png extension to use a php extension. This allows unauthenticated attackers to execute code on the server.	9.8	More Details
CVE-2025-7401	The Premium Age Verification / Restriction for WordPress plugin for WordPress is vulnerable to arbitrary file read and write due to the existence of an insufficiently protected remote support functionality in remote_tunnel.php in all versions up to, and including, 3.0.2. This makes it possible for unauthenticated attackers to read from or write to arbitrary files on the affected site's server which may make the exposure of sensitive information or remote code execution possible.	9.8	More Details
CVE-2025-7206	A vulnerability, which was classified as critical, has been found in D-Link DIR-825 2.10. This issue affects the function sub_410DDC of the file switch_language.cgi of the component httpd. The manipulation of the argument Language leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2025-5392	The GB Forms DB plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.0.2 via the gbfdb_talk_to_front() function. This is due to the function accepting user input and then passing that through call_user_func(). This makes it possible for unauthenticated attackers to execute code on the server which can be leverage to inject backdoors or create new administrative user accounts to name a few things.	9.8	More Details
CVE-2025-4606	The Sala - Startup & SaaS WordPress Theme theme for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.1.4. This is due to the theme not properly validating a user's identity prior to updating their details like password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to gain access to their account.	9.8	More Details
CVE-2025-52950	A Missing Authorization vulnerability in Juniper Networks Security Director allows an unauthenticated network-based attacker to read or tamper with multiple sensitive resources via the web interface. Numerous endpoints on the Juniper Security Director appliance do not validate authorization and will deliver information to the caller that is outside their authorization level. An attacker can access data that is outside the user's authorization level. The information obtained can be used to gain access to additional information or perpetrate other attacks, impacting downstream managed devices. This issue affects Security Director version 24.4.1.	9.6	More Details
CVE-2025-3621	Vulnerabilities* in ActADUR local server product, developed and maintained by ProTNS, allows Remote Code Inclusion on host systems. * vulnerabilities: * Improper Neutralization of Special Elements used in a Command ('Command Injection') * Use of Hard-coded Credentials * Improper Authentication * Binding to an Unrestricted IP Address The vulnerability has been rated as critical.This issue affects ActADUR: from v2.0.1.9 before v2.0.2.0., hence updating to version v2.0.2.0. or above is required.	9.6	More Details
CVE-2025-6514	mcp-remote is exposed to OS command injection when connecting to untrusted MCP servers due to crafted input from the authorization_endpoint response URL	9.6	More Details

CVE-2025-52579	Emerson ValveLink Products store sensitive information in cleartext in memory. The sensitive memory might be saved to disk, stored in a core dump, or remain uncleared if the product crashes, or if the programmer does not properly clear the memory before freeing it.	9.4	More Details
CVE-2025-2523	The Honeywell Experion PKS and OneWireless WDM contains an Integer Underflow vulnerability in the component Control Data Access (CDA). An attacker could potentially exploit this vulnerability, leading to a Communication Channel Manipulation, which could result in a failure during subtraction allowing remote code execution. Honeywell recommends updating to the most recent version of Honeywell Experion PKS:520.2 TCU9 HF1 and 530.1 TCU3 HF1 and OneWireless: 322.5 and 331.1. The affected Experion PKS products are C300 PCNT02, C300 PCNT05, FIM4, FIM8, UOC, CN100, HCA, C300PM, and C200E. The Experion PKS versions affected are from 520.1 through 520.2 TCU9 and from 530 through 530 TCU3. The OneWireless WDM affected versions are 322.1 through 322.4 and 330.1 through 330.3.	9.4	More Details
CVE-2025-53825	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to version 0.24.3, an unauthenticated preview deployment vulnerability in Dokploy allows any user to execute arbitrary code and access sensitive environment variables by simply opening a pull request on a public repository. This exposes secrets and potentially enables remote code execution, putting all public Dokploy users using these preview deployments at risk. Version 0.24.3 contains a fix for the issue.	9.4	More Details
CVE-2025-41238	VMware ESXi, Workstation, and Fusion contain a heap-overflow vulnerability in the PVSCSI (Paravirtualized SCSI) controller that leads to an out of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox and exploitable only with configurations that are unsupported. On Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.	9.3	More Details
CVE-2025-41237	VMware ESXi, Workstation, and Fusion contain an integer-underflow in VMCI (Virtual Machine Communication Interface) that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox whereas, on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.	9.3	More Details
CVE-2025-41236	VMware ESXi, Workstation, and Fusion contain an integer-overflow vulnerability in the VMXNET3 virtual network adapter. A malicious actor with local administrative privileges on a virtual machine with VMXNET3 virtual network adapter may exploit this issue to execute code on the host. Non VMXNET3 virtual adapters are not affected by this issue.	9.3	More Details
CVE-2025-7360	The HT Contact Form Widget For Elementor Page Builder & Gutenberg Blocks & Form Builder. plugin for WordPress is vulnerable to arbitrary file moving due to insufficient file path validation in the handle_files_upload() function in all versions up to, and including, 2.2.1. 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).	9.1	More Details
CVE-2025-5393	The Alone – Charity Multipurpose Non-profit WordPress Theme theme for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the alone_import_pack_restore_data() function in all versions up to, and including, 7.8.3. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	9.1	More Details
CVE-2025-7341	The HT Contact Form Widget For Elementor Page Builder & Gutenberg Blocks & Form Builder. plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the temp_file_delete() function in all versions up to, and including, 2.2.1. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	9.1	More Details
CVE-2025-53546	Folo organizes feeds content into one timeline. Using pull_request_target on .github/workflows/auto-fix-lint-format-commit.yml can be exploited by attackers, since untrusted code can be executed having full access to secrets (from the base repo). By exploiting the vulnerability is possible to exfiltrate GITHUB_TOKEN which has high privileges. GITHUB_TOKEN can be used to completely overtake the repo since the token has content write privileges. This vulnerability is fixed in commit 585c6a591440cd39f92374230ac5d65d7dd23d6a.	9.1	More Details
CVE-2025-23048	In some mod_ssl configurations on Apache HTTP Server 2.4.35 through to 2.4.63, an access control bypass by trusted clients is possible using TLS 1.3 session resumption. Configurations are affected when mod_ssl is configured for multiple virtual hosts, with each restricted to a different set of trusted client certificates (for example with a different SSLCACertificateFile/Path setting). In such a case, a client trusted to access one virtual host may be able to access another virtual host, if SSLStrictSNIVHostCheck is not enabled in either virtual host.	9.1	More Details
CVE-2025-53371	DiscordNotifications is an extension for MediaWiki that sends notifications of actions in your Wiki to a Discord channel. DiscordNotifications allows sending requests via curl and file_get_contents to arbitrary URLs set via $wgDiscordIncomingWebhookUrl and $wgDiscordAdditionalIncomingWebhookUrls. This allows for DOS by causing the server to read large files. SSRF is also possible if there are internal unprotected APIs that can be accessed using HTTP POST requests, which could also possibly lead to RCE. This vulnerability is fixed in commit 1f20d850cbcce5b15951c7c6127b87b927a5415e.	9.1	More Details
CVE-2025-53835	XWiki Rendering is a generic rendering system that converts textual input in a given syntax (wiki syntax, HTML, etc) into another syntax (XHTML, etc). Starting in version 5.4.5 and prior to version 14.10, the XHTML syntax depended on the \`xdom+xml/current\` syntax which allows the creation of raw blocks that permit the insertion of arbitrary HTML content including JavaScript. This allows XSS attacks for users who can edit a document like their user profile (enabled by default). This has been fixed in version 14.10 by removing the dependency on the \`xdom+xml/current\` syntax from the XHTML syntax. Note that the \`xdom+xml\` syntax is still vulnerable to this attack. As it's main purpose is testing and its use is quite difficult, this syntax shouldn't be installed or used on a regular wiki. There are no known workarounds apart from upgrading.	9.0	More Details
CVE-2025-30023	The communication protocol used between client and server had a flaw that could lead to an authenticated user performing a remote code execution attack.	9.0	More Details
CVE-2025-50067	Vulnerability in Oracle Application Express (component: Strategic Planner Starter App). Supported versions that are affected are 24.2.4 and 24.2.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Express. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly impact additional products	9.0	More Details

	(scope change). Successful attacks of this vulnerability can result in takeover of Oracle Application Express. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H).		

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-7550	A vulnerability was found in Tenda FH1201 1.2.0.14(408). It has been classified as critical. Affected is the function fromGstDhcpSetSer of the file /goform/GstDhcpSetSer. The manipulation of the argument dips 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-2025-28244	Insecure Permissions vulnerability in the Local Storage in Alteryx Server 2023.1.1.460 allows remote attackers to obtain valid user session tokens from localStorage, leading to account takeover	8.8	More Details
CVE-2025-7530	A vulnerability, which was classified as critical, has been found in Tenda FH1202 1.2.0.14(408). Affected by this issue is the function fromPptpUserAdd of the file /goform/PPTPDClient. The manipulation of the argument Username 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-2025-7421	A vulnerability was found in Tenda O3V2 1.0.0.12(3880). It has been rated as critical. This issue affects the function fromMacFilterModify of the file /goform/operateMacFilter of the component httpd. The manipulation of the argument mac leads to stack-based 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-2025-7529	A vulnerability classified as critical was found in Tenda FH1202 1.2.0.14(408). Affected by this vulnerability is the function fromNatlimit of the file /goform/Natlimit. The manipulation of the argument page leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7420	A vulnerability was found in Tenda O3V2 1.0.0.12(3880). It has been declared as critical. This vulnerability affects the function formWifiBasicSet of the file /goform/setWrlBasicInfo of the component httpd. The manipulation of the argument extChannel leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-30751	Vulnerability in the Oracle Database component of Oracle Database Server. Supported versions that are affected are 19.3-19.27 and 23.4-23.8. Easily exploitable vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via Oracle Net to compromise Oracle Database. Successful attacks of this vulnerability can result in takeover of Oracle Database. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2025-1313	The Nokri - Job Board WordPress Theme theme for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.6.3. This is due to the plugin not properly validating a user's identity prior to updating their details like email address. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change arbitrary user's email addresses, including administrators, and leverage that to reset the user's password and gain access to their account.	8.8	More Details
CVE-2025-53515	A vulnerability exists in Advantech iView that allows for SQL injection and remote code execution through NetworkServlet.archiveTrap(). This issue requires an authenticated attacker with at least user-level privileges. Certain input parameters are not sanitized, allowing an attacker to perform SQL injection and potentially execute code in the context of the 'nt authority\local service' account.	8.8	More Details
CVE-2025-53475	A vulnerability exists in Advantech iView that could allow for SQL injection and remote code execution through NetworkServlet.getNextTrapPage(). This issue requires an authenticated attacker with at least user-level privileges. Certain parameters in this function are not properly sanitized, allowing an attacker to perform SQL injection and potentially execute code in the context of the 'nt authority\local service' account.	8.8	More Details
CVE-2025-7463	A vulnerability was found in Tenda FH1201 1.2.0.14. It has been declared as critical. This vulnerability affects the function formWrlsafeset of the file /goform/AdvSetWrlsafeset of the component HTTP POST Request Handler. The manipulation of the argument mit_ssid leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7465	A vulnerability classified as critical was found in Tenda FH1201 1.2.0.14. Affected by this vulnerability is the function fromRouteStatic of the file /goform/fromRouteStatic of the component HTTP POST Request Handler. The manipulation of the argument page leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-53823	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. Versions prior to 3.4.5 have a SQL Injection vulnerability in the endpoint `/WeGIA/html/socio/sistema/processa_deletar_socio.php`, in the `id_socio` parameter. This vulnerability allows the execution of arbitrary SQL commands, which can compromise the confidentiality, integrity, and availability of stored data. Version 3.4.5 fixes the issue.	8.8	More Details
CVE-2025-7656	Integer overflow in V8 in Google Chrome prior to 138.0.7204.157 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-6558	Insufficient validation of untrusted input in ANGLE and GPU in Google Chrome prior to 138.0.7204.157 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-52577	A vulnerability exists in Advantech iView that could allow SQL injection and remote code execution through NetworkServlet.archiveTrapRange(). This issue requires an authenticated attacker with at least user-level privileges. Certain input parameters are not properly sanitized, allowing an attacker to perform SQL injection and potentially execute code in the context of the 'nt authority\local service' account.	8.8	More Details
CVE-2025-6423	The BeeTeam368 Extensions plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the handle_submit_upload_file() function in all versions up to, and including, 2.3.5. This makes it possible for authenticated attackers with Subscriber-level access or higher to upload arbitrary files on the affected site's server which may make remote code execution	8.8	More Details

	possible.		
CVE-2025-7423	A vulnerability classified as critical was found in Tenda O3V2 1.0.0.12(3880). Affected by this vulnerability is the function formWifiMacFilterSet of the file /goform/setWrlFilterList of the component httpd. The manipulation of the argument macList leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7528	A vulnerability classified as critical has been found in Tenda FH1202 1.2.0.14(408). Affected is the function fromGstDhcpSetSer of the file /goform/GstDhcpSetSer. The manipulation of the argument dips 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-2025-7527	A vulnerability was found in Tenda FH1202 1.2.0.14(408). It has been rated as critical. This issue affects the function fromAdvSetWan of the file /goform/AdvSetWan. The manipulation of the argument PPPOEPassword leads to stack-based 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-2025-53689	Blind XXE Vulnerabilities in jackrabbit-spi-commons and jackrabbit-core in Apache Jackrabbit < 2.23.2 due to usage of an unsecured document build to load privileges. Users are recommended to upgrade to versions 2.20.17 (Java 8), 2.22.1 (Java 11) or 2.23.2 (Java 11, beta versions), which fix this issue. Earlier versions (up to 2.20.16) are not supported anymore, thus users should update to the respective supported version.	8.8	More Details
CVE-2025-7419	A vulnerability was found in Tenda O3V2 1.0.0.12(3880). It has been classified as critical. This affects the function fromSpeedTestSet of the file /goform/setRateTest of the component httpd. The manipulation of the argument destIP leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7418	A vulnerability was found in Tenda O3V2 1.0.0.12(3880) and classified as critical. Affected by this issue is the function fromPingResultGet of the file /goform/setPing of the component httpd. The manipulation of the argument destIP 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-2025-7468	A vulnerability has been found in Tenda FH1201 1.2.0.14 and classified as critical. This vulnerability affects the function fromSafeUrlFilter of the file /goform/fromSafeUrlFilter of the component HTTP POST Request Handler. The manipulation of the argument page leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7417	A vulnerability has been found in Tenda O3V2 1.0.0.12(3880) and classified as critical. Affected by this vulnerability is the function fromNetToolGet of the file /goform/setPingInfo of the component httpd. The manipulation of the argument ip leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7416	A vulnerability, which was classified as critical, was found in Tenda O3V2 1.0.0.12(3880). Affected is the function fromSysToolTime of the file /goform/setSysTimeInfo of the component httpd. The manipulation of the argument Time 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-2025-7505	A vulnerability classified as critical has been found in Tenda FH451 1.0.0.9. Affected is the function frmL7ProtForm of the file /goform/L7Prot of the component HTTP POST Request Handler. The manipulation of the argument page 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-2025-7506	A vulnerability classified as critical was found in Tenda FH451 1.0.0.9. Affected by this vulnerability is the function fromNatlimit of the file /goform/Natlimit of the component HTTP POST Request Handler. The manipulation of the argument page leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7596	A vulnerability was found in Tenda FH1205 2.0.0.7(775). It has been rated as critical. This issue affects the function formWifiExtraSet of the file /goform/WifiExtraSet. The manipulation of the argument wpapsk_crypto leads to stack-based 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-2025-7597	A vulnerability classified as critical has been found in Tenda AX1803 1.0.0.1. Affected is the function formSetMacFilterCfg of the file /goform/setMacFilterCfg. The manipulation of the argument deviceList 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-2025-7598	A vulnerability classified as critical was found in Tenda AX1803 1.0.0.1. Affected by this vulnerability is the function formSetWifiMacFilterCfg of the file /goform/setWifiFilterCfg. The manipulation of the argument deviceList leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7551	A vulnerability was found in Tenda FH1201 1.2.0.14(408). It has been declared as critical. Affected by this vulnerability is the function fromPptpUserAdd of the file /goform/PPTPDClient. The manipulation of the argument modino/username leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7422	A vulnerability classified as critical has been found in Tenda O3V2 1.0.0.12(3880). Affected is the function setAutoReboot of the file /goform/setNetworkService of the component httpd. The manipulation of the argument week 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-2025-7657	Use after free in WebRTC in Google Chrome prior to 138.0.7204.157 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-7620	The cross-browser document creation component produced by Digitware System Integration Corporation has a Remote Code Execution vulnerability. If a user visits a malicious website while the component is active, remote attackers can cause the system to download and execute arbitrary programs.	8.8	More Details
CVE-2025-7586	A vulnerability was found in Tenda AC500 2.0.1.9(1307). It has been declared as critical. Affected by this vulnerability is the function formSetAPCfg of the file /goform/setWtpData. The manipulation of the argument radio_2g_1 leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7570	A vulnerability was found in UTT HiPER 840G up to 3.1.1-190328. It has been rated as critical. Affected by this issue is some unknown functionality of the file /goform/aspRemoteApConfTempSend. The manipulation of the argument remoteSrcTemp leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-	BatchSignCS, a background Windows application developed by WellChoose, has an Arbitrary File Write vulnerability. If a user visits a		

2025-7619	malicious website while the application is running, remote attackers can write arbitrary files to any path and potentially lead to arbitrary code execution.	8.8	More Details
CVE-2025-7548	A vulnerability has been found in Tenda FH1201 1.2.0.14(408) and classified as critical. This vulnerability affects the function formSafeEmailFilter of the file /goform/SafeEmailFilter. The manipulation of the argument page leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-52089	A hidden remote support feature protected by a static secret in TOTOLINK N300RB firmware version 8.54 allows an authenticated attacker to execute arbitrary OS commands with root privileges.	8.8	More Details
CVE-2025-7549	A vulnerability was found in Tenda FH1201 1.2.0.14(408) and classified as critical. This issue affects the function frmL7ProtForm of the file /goform/L7Prot. The manipulation of the argument page leads to stack-based 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-2025-7571	A vulnerability classified as critical has been found in UTT HiPER 840G up to 3.1.1-190328. This affects an unknown part of the file /goform/aspApBasicConfigUrcp. The manipulation of the argument Username leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-7532	A vulnerability has been found in Tenda FH1202 1.2.0.14(408) and classified as critical. This vulnerability affects the function fromwebExcptypemanFilter of the file /goform/webExcptypemanFilter. The manipulation of the argument page leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7460	A vulnerability has been found in TOTOLINK T6 4.1.5cu.748_B20211015 and classified as critical. Affected by this vulnerability is the function setWiFiAclRules of the file /cgi-bin/cstecgi.cgi of the component HTTP POST Request Handler. The manipulation of the argument mac leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7531	A vulnerability, which was classified as critical, was found in Tenda FH1202 1.2.0.14(408). This affects the function fromPptpUserSetting of the file /goform/PPTPUserSetting. The manipulation of the argument delno leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-6057	The WPBookit plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the handle_image_upload() function in all versions up to, and including, 1.0.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2025-7434	A vulnerability was found in Tenda FH451 up to 1.0.0.9 and classified as critical. Affected by this issue is the function fromAddressNat of the file /goform/addressNat of the component POST Request Handler. The manipulation of the argument page 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-2025-7544	A vulnerability was found in Tenda AC1206 15.03.06.23. It has been rated as critical. This issue affects the function formSetMacFilterCfg of the file /goform/setMacFilterCfg. The manipulation of the argument deviceList leads to stack-based 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-2025-6948	An issue has been discovered in GitLab CE/EE affecting all versions from 17.11 before 17.11.6, 18.0 before 18.0.4, and 18.1 before 18.1.2 that, under certain conditions, could have allowed a successful attacker to execute actions on behalf of users by injecting malicious content.	8.7	More Details
CVE-2025-3497	The Linux distribution underlying the Radiflow iSAP Smart Collector (CentOS 7 - VSAP 1.20) is obsolete and reached end of life (EOL) on June 30, 2024. Thus, any unmitigated vulnerability could be exploited to affect this product.	8.7	More Details
CVE-2025-27614	Gitk is a Tcl/Tk based Git history browser. Starting with 2.41.0, a Git repository can be crafted in such a way that with some social engineering a user who has cloned the repository can be tricked into running any script (e.g., Bourne shell, Perl, Python, ...) supplied by the attacker by invoking gitk filename, where filename has a particular structure. The script is run with the privileges of the user. This vulnerability is fixed in 2.43.7, 2.44.4, 2.45.4, 2.46.4, 2.47.3, 2.48.2, 2.49.1, and 2.50.	8.6	More Details
CVE-2025-50059	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	8.6	More Details
CVE-2025-46334	Git GUI allows you to use the Git source control management tools via a GUI. A malicious repository can ship versions of sh.exe or typical textconv filter programs such as astextplain. Due to the unfortunate design of Tcl on Windows, the search path when looking for an executable always includes the current directory. The mentioned programs are invoked when the user selects Git Bash or Browse Files from the menu. This vulnerability is fixed in 2.43.7, 2.44.4, 2.45.4, 2.46.4, 2.47.3, 2.48.2, 2.49.1, and 2.50.1.	8.6	More Details
CVE-2025-2521	The Honeywell Experion PKS and OneWireless WDM contains a Memory Buffer vulnerability in the component Control Data Access (CDA). An attacker could potentially exploit this vulnerability, leading to an Overread Buffers, which could result in improper index validation against buffer borders leading to remote code execution. Honeywell recommends updating to the most recent version of Honeywell Experion PKS: 520.2 TCU9 HF1 and 530.1 TCU3 HF1 and OneWireless: 322.5 and 331.1. The affected Experion PKS products are C300 PCNT02, C300 PCNT05, FIM4, FIM8, UOC, CN100, HCA, C300PM, and C200E. The Experion PKS versions affected are from 520.1 through 520.2 TCU9 and from 530 through 530 TCU3.The OneWireless WDM affected versions are 322.1 through	8.6	More Details

	322.4 and 330.1 through 330.3.		
CVE-2025-46835	Git GUI allows you to use the Git source control management tools via a GUI. When a user clones an untrusted repository and is tricked into editing a file located in a maliciously named directory in the repository, then Git GUI can create and overwrite files for which the user has write permission. This vulnerability is fixed in 2.43.7, 2.44.4, 2.45.4, 2.46.4, 2.47.3, 2.48.2, 2.49.1, and 2.50.1.	8.5	More Details
CVE-2013-3307	Linksys E1000 devices through 2.1.02, E1200 devices before 2.0.05, and E3200 devices through 1.0.04 allow OS command injection via shell metacharacters in the apply.cgi ping_ip parameter on TCP port 52000.	8.3	More Details
CVE-2025-53024	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2025-7027	A vulnerability in the Software SMI handler (SwSmiInputValue 0xB2) allows a local attacker to control both the read and write addresses used by the CommandRcx1 function. The write target is derived from an unvalidated UEFI NVRAM variable (SetupXtuBufferAddress), while the write content is read from an attacker-controlled pointer based on the RBX register. This dual-pointer dereference enables arbitrary memory writes within System Management RAM (SMRAM), leading to potential SMM privilege escalation and firmware compromise.	8.2	More Details
CVE-2025-7026	A vulnerability in the Software SMI handler (SwSmiInputValue 0xB2) allows a local attacker to control the RBX register, which is used as an unchecked pointer in the CommandRcx0 function. If the contents at RBX match certain expected values (e.g., 'DB' or '2DB$'), the function performs arbitrary writes to System Management RAM (SMRAM), leading to potential privilege escalation to System Management Mode (SMM) and persistent firmware compromise.	8.2	More Details
CVE-2025-44177	A directory traversal vulnerability was discovered in White Star Software Protop version 4.4.2-2024-11-27, specifically in the /pt3upd/ endpoint. An unauthenticated attacker can remotely read arbitrary files on the underlying OS using encoded traversal sequences.	8.2	More Details
CVE-2025-3947	The Honeywell Experion PKS contains an Integer Underflow vulnerability in the component Control Data Access (CDA). An attacker could potentially exploit this vulnerability, leading to Input Data Manipulation, which could result in improper integer data value checking during subtraction leading to a denial of service. Honeywell recommends updating to the most recent version of Honeywell Experion PKS:520.2 TCU9 HF1 and 530.1 TCU3 HF1. The affected Experion PKS products are C300 PCNT02, C300 PCNT05, FIM4, FIM8, UOC, CN100, HCA, C300PM, and C200E. The Experion PKS versions affected are from 520.1 through 520.2 TCU9 and from 530 through 530 TCU3.	8.2	More Details
CVE-2025-3946	The Honeywell Experion PKS and OneWireless WDM contains a Deployment of Wrong Handler vulnerability in the component Control Data Access (CDA). An attacker could potentially exploit this vulnerability, leading to Input Data Manipulation, which could result in incorrect handling of packets leading to remote code execution. Honeywell recommends updating to the most recent version of Honeywell Experion PKS:520.2 TCU9 HF1 and 530.1 TCU3 HF1 and OneWireless: 322.5 and 331.1. The affected Experion PKS products are C300 PCNT02, C300 PCNT05, FIM4, FIM8, UOC, CN100, HCA, C300PM, and C200E. The Experion PKS versions affected are from 520.1 through 520.2 TCU9 and from 530 through 530 TCU3. The OneWireless WDM affected versions are 322.1 through 322.4 and 330.1 through 330.3.	8.2	More Details
CVE-2025-53652	Jenkins Git Parameter Plugin 439.vb_0e46ca_14534 and earlier does not validate that the Git parameter value submitted to the build matches one of the offered choices, allowing attackers with Item/Build permission to inject arbitrary values into Git parameters.	8.2	More Details
CVE-2025-7029	A vulnerability in the Software SMI handler (SwSmiInputValue 0xB2) allows a local attacker to control the RBX register, which is used to derive pointers (OcHeader, OcData) passed into power and thermal configuration logic. These buffers are not validated before performing multiple structured memory writes based on OcSetup NVRAM values, enabling arbitrary SMRAM corruption and potential SMM privilege escalation.	8.2	More Details
CVE-2025-53027	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2025-53028	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2025-53641	Postiz is an AI social media scheduling tool. From 1.45.1 to 1.62.3, the Postiz frontend application allows an attacker to inject arbitrary HTTP headers into the middleware pipeline. This flaw enables a server-side request forgery (SSRF) condition, which can be exploited to initiate unauthorized outbound requests from the server hosting the Postiz application. This vulnerability is fixed in 1.62.3.	8.2	More Details
CVE-2025-30743	Vulnerability in the Oracle Lease and Finance Management product of Oracle E-Business Suite (component: Internal Operations). The supported version that is affected is 12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Lease and Finance Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Lease and Finance Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Lease and Finance Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2025-7667	The Restrict File Access plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the 'restrict-file-access' page. This makes it possible for unauthenticated attackers to to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php), via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.1	More Details

CVE-2025-50062	Vulnerability in the PeopleSoft Enterprise HCM Global Payroll Core product of Oracle PeopleSoft (component: Global Payroll for Core). Supported versions that are affected are 9.2.51 and 9.2.52. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Global Payroll Core. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise HCM Global Payroll Core accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise HCM Global Payroll Core accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2025-50060	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 7.6.0.0.0, 8.2.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle BI Publisher accessible data as well as unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2025-30749	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details
CVE-2025-6691	The SureForms – Drag and Drop Form Builder for WordPress plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_entry_files() function in all versions up to, and including, 1.7.3. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	8.1	More Details
CVE-2025-30744	Vulnerability in the Oracle Mobile Field Service product of Oracle E-Business Suite (component: Multiplatform Sync Errors). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Mobile Field Service. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Mobile Field Service accessible data as well as unauthorized access to critical data or complete access to all Oracle Mobile Field Service accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2025-50105	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Administration). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Universal Work Queue accessible data as well as unauthorized access to critical data or complete access to all Oracle Universal Work Queue accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2025-30403	A heap-buffer-overflow vulnerability is possible in mvfst via a specially crafted message during a QUIC session. This issue affects mvfst versions prior to v2025.07.07.00.	8.1	More Details
CVE-2025-26186	SQL Injection vulnerability in openSIS v.9.1 allows a remote attacker to execute arbitrary code via the id parameter in Ajax.php	8.1	More Details
CVE-2025-50106	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details
CVE-2025-30402	A heap-buffer-overflow vulnerability in the loading of ExecuTorch methods can cause the runtime to crash and potentially result in code execution or other undesirable effects. This issue affects ExecuTorch prior to commit 93b1a0c15f7eda49b2bc46b5b4c49557b4e9810f	8.1	More Details
CVE-2025-1727	The protocol used for remote linking over RF for End-of-Train and Head-of-Train (also known as a FRED) relies on a BCH checksum for packet creation. It is possible to create these EoT and HoT packets with a software defined radio and issue brake control commands to the EoT device, disrupting operations or potentially overwhelming the brake systems.	8.1	More Details
CVE-2024-51768	An hsqldb-related remote code execution vulnerability exists in HPE AutoPass License Server (APLS) prior to 9.17.	8.0	More Details
CVE-2025-28243	An issue in Alteryx Server v.2023.1.1.460 allows HTML injection via a crafted script to the pages component.	8.0	More Details
CVE-2025-53819	Nix is a package manager for Linux and other Unix systems. Builds with Nix 2.30.0 on macOS were executed with elevated privileges (root), instead of the build users. The fix was applied to Nix 2.30.1. No known workarounds are available.	7.9	More Details

CVE-2025-7425	A flaw was found in libxslt where the attribute type, atype, flags are modified in a way that corrupts internal memory management. When XSLT functions, such as the key() process, result in tree fragments, this corruption prevents the proper cleanup of ID attributes. As a result, the system may access freed memory, causing crashes or enabling attackers to trigger heap corruption.	7.8	More Details
CVE-2025-52837	Trend Micro Password Manager (Consumer) version 5.8.0.1327 and below is vulnerable to a Link Following Privilege Escalation Vulnerability that could allow an attacker the opportunity to abuse symbolic links and other methods to delete any file/folder and achieve privilege escalation.	7.8	More Details
CVE-2025-53503	Trend Micro Cleaner One Pro is vulnerable to a Privilege Escalation vulnerability that could allow a local attacker to unintentionally delete privileged Trend Micro files including its own.	7.8	More Details
CVE-2025-7424	A flaw was found in the libxslt library. The same memory field, psvi, is used for both stylesheet and input data, which can lead to type confusion during XML transformations. This vulnerability allows an attacker to crash the application or corrupt memory. In some cases, it may lead to denial of service or unexpected behavior.	7.8	More Details
CVE-2025-52521	Trend Micro Security 17.8 (Consumer) is vulnerable to a link following local privilege escalation vulnerability that could allow a local attacker to unintentionally delete privileged Trend Micro files including its own.	7.8	More Details
CVE-2025-6377	A remote code execution security issue exists in the Rockwell Automation Arena®. A crafted DOE file can force Arena Simulation to write beyond the boundaries of an allocated object. Exploitation requires user interaction, such as opening a malicious file within the software. If exploited, a threat actor could execute arbitrary code on the target system. The software must run under the context of the administrator in order to cause worse case impact. This is reflected in the Rockwell CVSS score, as AT:P.	7.8	More Details
CVE-2025-52954	A Missing Authorization vulnerability in the internal virtual routing and forwarding (VRF) of Juniper Networks Junos OS Evolved allows a local, low-privileged user to gain root privileges, leading to a system compromise. Any low-privileged user with the capability to send packets over the internal VRF can execute arbitrary Junos commands and modify the configuration, and thus compromise the system. This issue affects Junos OS Evolved: * All versions before 22.2R3-S7-EVO, * from 22.4 before 22.4R3-S7-EVO, * from 23.2 before 23.2R2-S4-EVO, * from 23.4 before 23.4R2-S5-EVO, * from 24.2 before 24.2R2-S1-EVO * from 24.4 before 24.4R1-S2-EVO, 24.4R2-EVO.	7.8	More Details
CVE-2025-6376	A remote code execution security issue exists in the Rockwell Automation Arena®. A crafted DOE file can force Arena Simulation to write beyond the boundaries of an allocated object. Exploitation requires user interaction, such as opening a malicious file within the software. If exploited, a threat actor could execute arbitrary code on the target system. The software must run under the context of the administrator in order to cause worse case impact. This is reflected in the Rockwell CVSS score, as AT:P.	7.8	More Details
CVE-2025-5040	A maliciously crafted RTE file, when parsed through Autodesk Revit, can force a Heap-Based Overflow vulnerability. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-0831	Out-Of-Bounds Read vulnerability exists in the JT file reading procedure in SOLIDWORKS eDrawings on Release SOLIDWORKS Desktop 2025. This vulnerability could allow an attacker to execute arbitrary code while opening a specially crafted JT file.	7.8	More Details
CVE-2025-25180	Software installed and run as a non-privileged user may conduct improper GPU system calls to subvert GPU HW to write to arbitrary physical memory pages. Under certain circumstances this exploit could be used to corrupt data pages not allocated by the GPU driver but memory pages in use by the kernel and drivers running on the platform altering their behaviour.	7.8	More Details
CVE-2025-5037	A maliciously crafted RFA, RTE, or RVT file, when parsed through Autodesk Revit, can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-6971	Use After Free vulnerability exists in the CATPRODUCT file reading procedure in SOLIDWORKS eDrawings on Release SOLIDWORKS Desktop 2025. This vulnerability could allow an attacker to execute arbitrary code while opening a specially crafted CATPRODUCT file.	7.8	More Details
CVE-2025-6972	Use After Free vulnerability exists in the CATPRODUCT file reading procedure in SOLIDWORKS eDrawings on Release SOLIDWORKS Desktop 2025. This vulnerability could allow an attacker to execute arbitrary code while opening a specially crafted CATPRODUCT file.	7.8	More Details
CVE-2025-6973	Use After Free vulnerability exists in the JT file reading procedure in SOLIDWORKS eDrawings on Release SOLIDWORKS Desktop 2025. This vulnerability could allow an attacker to execute arbitrary code while opening a specially crafted JT file.	7.8	More Details
CVE-2025-6974	Use of Uninitialized Variable vulnerability exists in the JT file reading procedure in SOLIDWORKS eDrawings on Release SOLIDWORKS Desktop 2025. This vulnerability could allow an attacker to execute arbitrary code while opening a specially crafted JT file.	7.8	More Details
CVE-2025-7042	Use After Free vulnerability exists in the IPT file reading procedure in SOLIDWORKS eDrawings on Release SOLIDWORKS Desktop 2025. This vulnerability could allow an attacker to execute arbitrary code while opening a specially crafted IPT file.	7.8	More Details
CVE-2025-7028	A vulnerability in the Software SMI handler (SwSmiInputValue 0x20) allows a local attacker to supply a crafted pointer (FuncBlock) through RBX and RCX register values. This pointer is passed unchecked into multiple flash management functions (ReadFlash, WriteFlash, EraseFlash, and GetFlashInfo) that dereference both the structure and its nested members, such as BufAddr. This enables arbitrary read/write access to System Management RAM (SMRAM), allowing an attacker to corrupt firmware memory, exfiltrate SMRAM content via flash, or install persistent implants.	7.8	More Details
CVE-2025-7564	A vulnerability, which was classified as critical, has been found in LB-LINK BL-AC3600 1.0.22. Affected by this issue is some unknown functionality of the file /etc/shadow. The manipulation with the input root:blinkadmin leads to hard-coded credentials. 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-2025-46358	Emerson ValveLink products do not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product.	7.7	More Details
CVE-2025-50109	Emerson ValveLink Products store sensitive information in cleartext within a resource that might be accessible to another control sphere.	7.7	More Details
CVE-2025-53542	Headlamp is an extensible Kubernetes web UI. A command injection vulnerability was discovered in the codeSign.js script used in the macOS packaging workflow of the Kubernetes Headlamp project. This issue arises due to the improper use of Node.js's execSync() function with unsanitized input derived from environment variables, which can be influenced by an attacker. The variables ${teamID}, ${entitlementsPath}, and ${config.app} are dynamically derived from the environment or application config and passed directly to the shell command without proper escaping or argument separation. This exposes the system to command injection if any of the values contain malicious input. This vulnerability is fixed in 0.31.1.	7.7	More Details
CVE-2025-50069	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.27 and 21.3-21.18. Easily exploitable vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via Oracle Net to compromise Java VM. While the vulnerability is in Java VM, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java VM accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	7.7	More Details
CVE-2025-48891	A vulnerability exists in Advantech iView that could allow for SQL injection through the CUtils.checkSQLInjection() function. This vulnerability can be exploited by an authenticated attacker with at least user-level privileges, potentially leading to information disclosure or a denial-of-service condition.	7.6	More Details
CVE-2025-53378	A missing authentication vulnerability in Trend Micro Worry-Free Business Security Services (WFBSS) agent could have allowed an unauthenticated attacker to remotely take control of the agent on affected installations. Also note: this vulnerability only affected the SaaS client version of WFBSS only, meaning the on-premise version of Worry-Free Business Security was not affected, and this issue was addressed in a WFBSS monthly maintenance update. Therefore no other customer action is required to mitigate if the WFBSS agents are on the regular SaaS maintenance deployment schedule and this disclosure is for informational purposes only.	7.6	More Details
CVE-2025-27582	The Secure Password extension in One Identity Password Manager before 5.14.4 allows local privilege escalation. The issue arises from a flawed security hardening mechanism within the kiosk browser used to display the Password Self-Service site to end users. Specifically, the application attempts to restrict privileged actions by overriding the native window.print() function. However, this protection can be bypassed by an attacker who accesses the Password Self-Service site from the lock screen and navigates to an attacker-controlled webpage via the Help function. By hosting a crafted web page with JavaScript, the attacker can restore and invoke the window.print() function, launching a SYSTEM-privileged print dialog. From this dialog, the attacker can exploit standard Windows functionality - such as the Print to PDF or Add Printer wizard - to spawn a command prompt with SYSTEM privileges. Successful exploitation allows a local attacker (with access to a locked workstation) to gain SYSTEM-level privileges, granting full control over the affected device.	7.6	More Details
CVE-2025-53959	In JetBrains YouTrack before 2025.2.86069, 2024.3.85077, 2025.1.86199 email spoofing via an administrative API was possible	7.6	More Details
CVE-2024-43204	SSRF in Apache HTTP Server with mod_proxy loaded allows an attacker to send outbound proxy requests to a URL controlled by the attacker. Requires an unlikely configuration where mod_headers is configured to modify the Content-Type request or response header with a value provided in the HTTP request. Users are recommended to upgrade to version 2.4.64 which fixes this issue.	7.5	More Details
CVE-2024-42516	HTTP response splitting in the core of Apache HTTP Server allows an attacker who can manipulate the Content-Type response headers of applications hosted or proxied by the server can split the HTTP response. This vulnerability was described as CVE-2023-38709 but the patch included in Apache HTTP Server 2.4.59 did not address the issue. Users are recommended to upgrade to version 2.4.64, which fixes this issue.	7.5	More Details
CVE-2025-44251	Ecovacs Deebot T10 1.7.2 transmits Wi-Fi credentials in cleartext during the pairing process.	7.5	More Details
CVE-2024-43394	Server-Side Request Forgery (SSRF) in Apache HTTP Server on Windows allows to potentially leak NTLM hashes to a malicious server via mod_rewrite or apache expressions that pass unvalidated request input. This issue affects Apache HTTP Server: from 2.4.0 through 2.4.63. Note: The Apache HTTP Server Project will be setting a higher bar for accepting vulnerability reports regarding SSRF via UNC paths. The server offers limited protection against administrators directing the server to open UNC paths. Windows servers should limit the hosts they will connect over via SMB based on the nature of NTLM authentication.	7.5	More Details
CVE-2024-47252	Insufficient escaping of user-supplied data in mod_ssl in Apache HTTP Server 2.4.63 and earlier allows an untrusted SSL/TLS client to insert escape characters into log files in some configurations. In a logging configuration where CustomLog is used with "%{varname}x" or "%{varname}c" to log variables provided by mod_ssl such as SSL_TLS_SNI, no escaping is performed by either mod_log_config or mod_ssl and unsanitized data provided by the client may appear in log files.	7.5	More Details
CVE-2024-42646	A segmentation fault in NanoMQ v0.21.10 allows attackers to cause a Denial of Service (DoS) via crafted messages.	7.5	More Details
CVE-2024-51770	An information disclosure vulnerability exists in HPE AutoPass License Server (APLS) prior to 9.17.	7.5	More Details
CVE-2024-51769	An information disclosure vulnerability exists in HPE AutoPass License Server (APLS) prior to 9.17.	7.5	More Details
CVE-2025-	Late Release of Memory after Effective Lifetime vulnerability in Apache HTTP Server. This issue affects Apache HTTP Server: from 2.4.17 up to 2.4.63. Users are recommended to upgrade to version 2.4.64, which fixes the issue.	7.5	More Details

53020			
CVE-2025-49630	In certain proxy configurations, a denial of service attack against Apache HTTP Server versions 2.4.26 through to 2.4.63 can be triggered by untrusted clients causing an assertion in mod_proxy_http2. Configurations affected are a reverse proxy is configured for an HTTP/2 backend, with ProxyPreserveHost set to "on".	7.5	More Details
CVE-2025-52980	A Use of Incorrect Byte Ordering vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS on SRX300 Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). When a BGP update is received over an established BGP session which contains a specific, valid, optional, transitive path attribute, rpd will crash and restart. This issue affects eBGP and iBGP over IPv4 and IPv6. This issue affects: Junos OS: * 22.1 versions from 22.1R1 before 22.2R3-S4, * 22.3 versions before 22.3R3-S3, * 22.4 versions before 22.4R3-S2, * 23.2 versions before 23.2R2, * 23.4 versions before 23.4R2.	7.5	More Details
CVE-2025-53629	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.23.0, incoming requests using Transfer-Encoding: chunked in the header can allocate memory arbitrarily in the server, potentially leading to its exhaustion. This vulnerability is fixed in 0.23.0. NOTE: This vulnerability is related to CVE-2025-53628.	7.5	More Details
CVE-2025-53645	Zimbra Collaboration Suite (ZCS) before 9.0.0 Patch 46, 10.0.x before 10.0.15, and 10.1.x before 10.1.9 is vulnerable to a denial of service condition due to improper handling of excessive, comma-separated path segments in both the Webmail interface and the Admin Console. An unauthenticated remote attacker can send specially crafted GET requests that trigger redundant processing and inflated responses. This leads to uncontrolled resource consumption, resulting in denial of service.	7.5	More Details
CVE-2025-52364	Insecure Permissions vulnerability in Tenda CP3 Pro Firmware V22.5.4.93 allows the telnet service (telnetd) by default at boot via the initialization script /etc/init.d/eth.sh. This allows remote attackers to connect to the device s shell over the network, potentially without authentication if default or weak credentials are present	7.5	More Details
CVE-2025-30762	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2025-7504	The Friends plugin for WordPress is vulnerable to PHP Object Injection in version 3.5.1 via deserialization of untrusted input of the query_vars parameter This makes it possible for authenticated attackers, with subscriber-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present. This requires access to the sites SALT_NONCE and and SALT_KEY to exploit.	7.5	More Details
CVE-2020-36848	The Total Upkeep – WordPress Backup Plugin plus Restore & Migrate by BoldGrid plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.14.9 via the env-info.php and restore-info.json files. This makes it possible for unauthenticated attackers to find the location of back-up files and subsequently download them.	7.5	More Details
CVE-2025-6742	The SureForms – Drag and Drop Form Builder for WordPress plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.7.3 via the use of file_exists() in the delete_entry_files() function without restriction on the path provided. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	7.5	More Details
CVE-2025-53506	Uncontrolled Resource Consumption vulnerability in Apache Tomcat if an HTTP/2 client did not acknowledge the initial settings frame that reduces the maximum permitted concurrent streams. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.8, from 10.1.0-M1 through 10.1.42, from 9.0.0.M1 through 9.0.106. Users are recommended to upgrade to version 11.0.9, 10.1.43 or 9.0.107, which fix the issue.	7.5	More Details
CVE-2025-2520	The Honeywell Experion PKS contains an Uninitialized Variable in the common Epic Platform Analyzer (EPA) communications. An attacker could potentially exploit this vulnerability, leading to a Communication Channel Manipulation, which results in a dereferencing of an uninitialized pointer leading to a denial of service. Honeywell recommends updating to the most recent version of Honeywell Experion PKS: 520.2 TCU9 HF1and 530.1 TCU3 HF1. The affected Experion PKS products are C300 PCNT02, EHB, EHPM, ELMM, Classic ENIM, ETN, FIM4, FIM8, PGM, and RFIM. The Experion PKS versions affected are from 520.1 through 520.2 TCU9 and from 530 through 530 TCU3.	7.5	More Details
CVE-2025-7442	The WPGYM - Wordpress Gym Management System plugin for WordPress is vulnerable to SQL Injection via several parameters in the MJ_gmgt_delete_class_limit_for_member, MJ_gmgt_get_yearly_income_expense, MJ_gmgt_get_monthly_income_expense, MJ_gmgt_add_class_limit, MJ_gmgt_view_meeting_detail, and MJ_gmgt_create_meeting functions in all versions up to 67.8.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2024-41169	The attacker can use the raft server protocol in an unauthenticated way. The attacker can see the server's resources, including directories and files. This issue affects Apache Zeppelin: from 0.10.1 up to 0.12.0. Users are recommended to upgrade to version 0.12.0, which fixes the issue by removing the Cluster Interpreter.	7.5	More Details
CVE-2025-53548	Clerk helps developers build user management. Applications that use the verifyWebhook() helper to verify incoming Clerk webhooks are susceptible to accepting improperly signed webhook events. The issue was resolved in @clerk/backend 2.4.0.	7.5	More Details
CVE-2025-52946	A Use After Free vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Juniper Networks Junos OS Evolved allows an attacker sending a BGP update with a specifically malformed AS PATH to cause rpd to crash, resulting in a Denial of Service (DoS). Continuous receipt of the malformed AS PATH attribute will cause a sustained DoS condition. On all Junos OS and Junos OS Evolved platforms, the rpd process will crash and restart when a specifically malformed AS PATH is received within a BGP update and traceoptions are enabled. This issue only affects systems with BGP traceoptions enabled and requires a BGP session to be already established. Systems without BGP traceoptions enabled are not impacted by this issue. This issue affects: Junos OS: * All versions before 21.2R3-S9, * all versions of 21.4, * from 22.2 before 22.2R3-S6, * from 22.4 before 22.4R3-S5, * from 23.2 before 23.2R2-S3, * from 23.4 before 23.4R2-S4, * from 24.2 before 24.2R2; Junos OS Evolved: * All versions before 22.4R3-S5-EVO, *	7.5	More Details

	from 23.2-EVO before 23.2R2-S3-EVO, * from 23.4-EVO before 23.4R2-S4-EVO, * from 24.2-EVO before 24.2R2-EVO. This is a more complete fix for previously published CVE-2024-39549 (JSA83011).		
CVE-2025-52981	An Improper Check for Unusual or Exceptional Conditions vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX1600, SRX2300, SRX 4000 Series, and SRX5000 Series with SPC3 allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). If a sequence of specific PIM packets is received, this will cause a flowd crash and restart. This issue affects Junos OS: * all versions before 21.2R3-S9, * 21.4 versions before 21.4R3-S11, * 22.2 versions before 22.2R3-S7, * 22.4 versions before 22.4R3-S6, * 23.2 versions before 23.2R2-S4, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R2. This is a similar, but different vulnerability than the issue reported as CVE-2024-47503, published in JSA88133.	7.5	More Details
CVE-2025-52434	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in Apache Tomcat when using the APR/Native connector. This was particularly noticeable with client initiated closes of HTTP/2 connections. This issue affects Apache Tomcat: from 9.0.0.M1 through 9.0.106. Users are recommended to upgrade to version 9.0.107, which fixes the issue.	7.5	More Details
CVE-2025-52520	For some unlikely configurations of multipart upload, an Integer Overflow vulnerability in Apache Tomcat could lead to a DoS via bypassing of size limits. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.8, from 10.1.0-M1 through 10.1.42, from 9.0.0.M1 through 9.0.106. Users are recommended to upgrade to version 11.0.9, 10.1.43 or 9.0.107, which fix the issue.	7.5	More Details
CVE-2025-6970	The Events Manager – Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to time-based SQL Injection via the ‘orderby’ parameter in all versions up to, and including, 7.0.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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-2024-42650	NanoMQ 0.17.5 was discovered to contain a segmentation fault via the component /nanomq/pub_handler.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted PUBLISH message.	7.5	More Details
CVE-2025-53015	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions prior to 7.1.2-0, infinite lines occur when writing during a specific XMP file conversion command. Version 7.1.2-0 fixes the issue.	7.5	More Details
CVE-2025-46788	Improper certificate validation in Zoom Workplace for Linux before version 6.4.13 may allow an unauthorized user to conduct an information disclosure via network access.	7.4	More Details
CVE-2025-53101	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions prior to 7.1.2-0 and 6.9.13-26, in ImageMagick's `magick mogrify` command, specifying multiple consecutive `%d` format specifiers in a filename template causes internal pointer arithmetic to generate an address below the beginning of the stack buffer, resulting in a stack overflow through `vsnprintf()`. Versions 7.1.2-0 and 6.9.13-26 fix the issue.	7.4	More Details
CVE-2025-49812	In some mod_ssl configurations on Apache HTTP Server versions through to 2.4.63, an HTTP desynchronisation attack allows a man-in-the-middle attacker to hijack an HTTP session via a TLS upgrade. Only configurations using "SSLEngine optional" to enable TLS upgrades are affected. Users are recommended to upgrade to version 2.4.64, which removes support for TLS upgrade.	7.4	More Details
CVE-2025-7454	A vulnerability classified as critical has been found in Campcodes Online Movie Theater Seat Reservation System 1.0. Affected is an unknown function of the file /admin/manage_theater.php. The manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7540	A vulnerability, which was classified as critical, was found in code-projects Online Appointment Booking System 1.0. Affected is an unknown function of the file /getclinic.php. The manipulation of the argument townid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	7.3	More Details
CVE-2025-7542	A vulnerability was found in PHPGurukul User Registration & Login and User Management System 3.3 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/user-profile.php. The manipulation of the argument uid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-5199	In Canonical Multipass up to and including version 1.15.1 on macOS, incorrect default permissions allow a local attacker to escalate privileges by modifying files executed with administrative privileges by a Launch Daemon during system startup.	7.3	More Details
CVE-2025-7459	A vulnerability classified as critical was found in code-projects Mobile Shop 1.0. This vulnerability affects unknown code of the file /EditMobile.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7457	A vulnerability, which was classified as critical, was found in Campcodes Online Movie Theater Seat Reservation System 1.0. This affects an unknown part of the file /admin/manage_movie.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7541	A vulnerability has been found in code-projects Online Appointment Booking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /get_town.php. The manipulation of the argument countryid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	7.3	More Details
CVE-2025-7533	A vulnerability was found in code-projects Job Diary 1.0 and classified as critical. This issue affects some unknown processing of the file /view-details.php. The manipulation of the argument job_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7535	A vulnerability was found in Campcodes Sales and Inventory System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /pages/reprint_cash.php. The manipulation of the argument sid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7534	A vulnerability was found in PHPGurukul Student Result Management System 2.0. It has been classified as critical. Affected is an unknown function of the file /notice-details.php of the component GET Parameter Handler. The manipulation of the argument nid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details

CVE-2025-7539	A vulnerability, which was classified as critical, has been found in code-projects Online Appointment Booking System 1.0. This issue affects some unknown processing of the file /getdoctordaybooking.php. The manipulation of the argument cid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7536	A vulnerability was found in Campcodes Sales and Inventory System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /pages/receipt_credit.php. The manipulation of the argument sid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7537	A vulnerability classified as critical has been found in Campcodes Sales and Inventory System 1.0. This affects an unknown part of the file /pages/product_update.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-30661	An Incorrect Permission Assignment for Critical Resource vulnerability in line card script processing of Juniper Networks Junos OS allows a local, low-privileged user to install scripts to be executed as root, leading to privilege escalation. A local user with access to the local file system can copy a script to the router in a way that will be executed as root, as the system boots. Execution of the script as root can lead to privilege escalation, potentially providing the adversary complete control of the system. This issue only affects specific line cards, such as the MPC10, MPC11, LC4800, LC9600, MX304-LMIC16, SRX4700, and EX9200-15C. This issue affects Junos OS: * from 23.2 before 23.2R2-S4, * from 23.4 before 23.4R2-S5, * from 24.2 before 24.2R2-S1, * from 24.4 before 24.4R1-S3, 24.4R2. This issue does not affect versions prior to 23.1R2.	7.3	More Details
CVE-2025-7456	A vulnerability, which was classified as critical, has been found in Campcodes Online Movie Theater Seat Reservation System 1.0. Affected by this issue is some unknown functionality of the file /reserve.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7436	A vulnerability was found in Campcodes Online Recruitment Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/ajax.php?action=delete_vacancy. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7455	A vulnerability classified as critical was found in Campcodes Online Movie Theater Seat Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file /manage_reserve.php. The manipulation of the argument mid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7461	A vulnerability was found in code-projects Modern Bag 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /action.php. The manipulation of the argument proId leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7538	A vulnerability classified as critical was found in Campcodes Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /pages/product_update.php. The manipulation of the argument image leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7409	A vulnerability was found in code-projects Mobile Shop 1.0 and classified as critical. This issue affects some unknown processing of the file /LoginAsAdmin.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7466	A vulnerability, which was classified as critical, has been found in 1000projects ABC Courier Management 1.0. Affected by this issue is some unknown functionality of the file /add_dealerrequest.php. The manipulation of the argument Name leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7523	A vulnerability was found in Jinher OA 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /c6/Jhsoft.Web.message/ToolBar/DelTemp.aspx. The manipulation leads to xml external entity reference. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7410	A vulnerability was found in code-projects LifeStyle Store 1.0. It has been classified as critical. Affected is an unknown function of the file /cart_remove.php. The manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7508	A vulnerability, which was classified as critical, has been found in code-projects Modern Bag 1.0. Affected by this issue is some unknown functionality of the file /admin/product-update.php. The manipulation of the argument idProduct leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7509	A vulnerability, which was classified as critical, was found in code-projects Modern Bag 1.0. This affects an unknown part of the file /admin/slide.php. The manipulation of the argument idSlide leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7510	A vulnerability has been found in code-projects Modern Bag 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/productadd_back.php. The manipulation of the argument namepro 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-2025-7512	A vulnerability was found in code-projects Modern Bag 1.0. It has been classified as critical. Affected is an unknown function of the file /contact-back.php. The manipulation of the argument contact-name leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7513	A vulnerability was found in code-projects Modern Bag 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/slideupdate.php. The manipulation of the argument idSlide leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7411	A vulnerability was found in code-projects LifeStyle Store 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /success.php. The 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.	7.3	More Details
CVE-2025-7483	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13. It has been rated as critical. This issue affects some unknown processing of the file /users/forgot-password.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-	A vulnerability was found in code-projects Modern Bag 1.0. It has been rated as critical. Affected by this issue is some unknown		More

2025-7514	functionality of the file /admin/contact-list.php. The manipulation of the argument idStatus leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	Details
CVE-2025-7515	A vulnerability classified as critical has been found in code-projects Online Appointment Booking System 1.0. This affects an unknown part of the file /ulocateus.php. The manipulation of the argument doctorname leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7516	A vulnerability classified as critical was found in code-projects Online Appointment Booking System 1.0. This vulnerability affects unknown code of the file /cancelbookingpatient.php. The manipulation of the argument appointment 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-2025-7480	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13 and classified as critical. Affected by this issue is some unknown functionality of the file /users/signup.php. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7478	A vulnerability, which was classified as critical, was found in code-projects Modern Bag 1.0. Affected is an unknown function of the file /admin/category-list.php. The manipulation of the argument idCate leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7517	A vulnerability, which was classified as critical, has been found in code-projects Online Appointment Booking System 1.0. This issue affects some unknown processing of the file /getDay.php. The manipulation of the argument cidval leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7476	A vulnerability classified as critical was found in code-projects Simple Car Rental System 1.0. This vulnerability affects unknown code of the file /admin/approve.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7475	A vulnerability classified as critical has been found in code-projects Simple Car Rental System 1.0. This affects an unknown part of the file /pay.php. The manipulation of the argument mpesa leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7474	A vulnerability was found in code-projects Job Diary 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /search.php. The manipulation of the argument Search leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7471	A vulnerability was found in code-projects Modern Bag 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/login-back.php. The manipulation of the argument user-name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7470	A vulnerability was found in Campcodes Sales and Inventory System 1.0. It has been classified as critical. Affected is an unknown function of the file /pages/product_add.php. The manipulation of the argument image leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7467	A vulnerability, which was classified as critical, was found in code-projects Modern Bag 1.0. This affects an unknown part of the file /product-detail.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7521	A vulnerability, which was classified as critical, was found in PHPGurukul Vehicle Parking Management System 1.13. Affected is an unknown function of the file /admin/index.php. The manipulation of the argument Username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7469	A vulnerability was found in Campcodes Sales and Inventory System 1.0 and classified as critical. This issue affects some unknown processing of the file /pages/product_add.php. The manipulation of the argument prod_name leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7547	A vulnerability, which was classified as critical, was found in Campcodes Online Movie Theater Seat Reservation System 1.0. This affects the function save_movie of the file /admin/admin_class.php. The manipulation of the argument cover leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7606	A vulnerability classified as critical has been found in code-projects AVL Rooms 1.0. This affects an unknown part of the file /city.php. The manipulation of the argument city leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7220	A vulnerability was found in Campcodes Payroll Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=save_deductions. The 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.	7.3	More Details
CVE-2025-7217	A vulnerability has been found in Campcodes Payroll Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /ajax.php?action=save_position. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7604	A vulnerability was found in PHPGurukul Hospital Management System 4.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /user-login.php. The manipulation of the argument Username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7605	A vulnerability was found in code-projects AVL Rooms 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /profile.php. The manipulation of the argument first_name leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7576	A vulnerability was found in Teledyne FLIR FB-Series O and FLIR FH-Series ID 1.3.2.16 and classified as critical. Affected by this issue is some unknown functionality of the file /priv/production/production.html of the component Production Tools. The manipulation leads to improper access controls. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-	A vulnerability was found in code-projects Online Appointment Booking System 1.0. It has been rated as critical. Affected by this		More

2025-7587	issue is some unknown functionality of the file /cover.php. The manipulation of the argument uname/psw leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	Details
CVE-2025-7211	A vulnerability was found in code-projects LifeStyle Store 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /cart_add.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7218	A vulnerability was found in Campcodes Payroll Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /ajax.php?action=delete_position. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7219	A vulnerability was found in Campcodes Payroll Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /ajax.php?action=delete_allowances. The manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-51767	An authentication bypass vulnerability exists in HPE AutoPass License Server (APLS) prior to 9.17.	7.3	More Details
CVE-2025-7607	A vulnerability, which was classified as critical, has been found in code-projects Simple Shopping Cart 1.0. This issue affects some unknown processing of the file /Customers/save_order.php. The manipulation of the argument order_price leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7216	A vulnerability, which was classified as critical, was found in lty628 Aidigu up to 1.8.2. This affects the function checkUserCookie of the file /application/common.php of the component PHP Object Handler. The manipulation of the argument rememberMe leads to deserialization. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7595	A vulnerability was found in code-projects Job Diary 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /view-cad.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7608	A vulnerability, which was classified as critical, was found in code-projects Simple Shopping Cart 1.0. Affected is an unknown function of the file /userlogin.php. The manipulation of the argument user_email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7593	A vulnerability was found in code-projects Job Diary 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /view-all.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7609	A vulnerability has been found in code-projects Simple Shopping Cart 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /register.php. The manipulation of the argument ruser_email leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7610	A vulnerability was found in code-projects Electricity Billing System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /user/change_password.php. The manipulation of the argument new_password leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7611	A vulnerability was found in code-projects Wedding Reservation 1.0. It has been classified as critical. This affects an unknown part of the file /global.php. The manipulation of the argument lu leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7612	A vulnerability was found in code-projects Mobile Shop 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /login.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-2025-50063	Vulnerability in Oracle Java SE (component: Install). Supported versions that are affected are Oracle Java SE: 8u451 and 8u451-perf. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Java SE executes to compromise Oracle Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Java SE. Note: Applies to installation process on client deployment of Java. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H).	7.3	More Details
CVE-2025-53650	Jenkins Credentials Binding Plugin 687.v619cb_15e923f and earlier does not properly mask (i.e., replace with asterisks) credentials present in exception error messages that are written to the build log.	7.3	More Details
CVE-2025-7594	A vulnerability was found in code-projects Job Diary 1.0. It has been classified as critical. This affects an unknown part of the file /view-emp.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7603	A vulnerability was found in D-Link DI-8100 16.07.26A1. It has been classified as critical. Affected is an unknown function of the file /jingx.asp of the component HTTP Request Handler. The manipulation 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.	7.2	More Details
CVE-2025-7602	A vulnerability was found in D-Link DI-8100 16.07.26A1 and classified as critical. This issue affects some unknown processing of the file /arp_sys.asp of the component HTTP Request Handler. The manipulation leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.2	More Details
CVE-2025-6851	The Broken Link Notifier plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.3.0 via the ajax_blinks() function which ultimately calls the check_url_status_code() function. 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.	7.2	More Details
CVE-2024-58258	SugarCRM before 13.0.4 and 14.x before 14.0.1 allows SSRF in the API module because a limited type of code injection can occur.	7.2	More Details

CVE-2025-52983	A UI Discrepancy for Security Feature vulnerability in the UI of Juniper Networks Junos OS on VM Host systems allows a network-based, unauthenticated attacker to access the device. On VM Host Routing Engines (RE), even if the configured public key for root has been removed, remote users which are in possession of the corresponding private key can still log in as root. This issue affects Junos OS: * all versions before 22.2R3-S7, * 22.4 versions before 22.4R3-S5, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S3, * 24.2 versions before 24.2R1-S2, 24.2R2.	7.2	More Details
CVE-2025-6265	A path traversal vulnerability in the file_upload-cgi CGI program of Zyxel NWA50AX PRO firmware version 7.10(ACGE.2) and earlier could allow an authenticated attacker with administrator privileges to access specific directories and delete files, such as the configuration file, on the affected device.	7.2	More Details
CVE-2025-41239	VMware ESXi, Workstation, Fusion, and VMware Tools contains an information disclosure vulnerability due to the usage of an uninitialised memory in vSockets. A malicious actor with local administrative privileges on a virtual machine may be able to exploit this issue to leak memory from processes communicating with vSockets.	7.1	More Details
CVE-2025-5023	Use of Hard-coded Credentials vulnerability in Mitsubishi Electric Corporation photovoltaic system monitor “EcoGuideTAB” PV-DR004J all versions and PV-DR004JA all versions allows an attacker within the Wi-Fi communication range between the units of the product (measurement unit and display unit) to disclose information such as generated power and electricity sold back to the grid stored in the product, tamper with or destroy stored or configured information in the product, or cause a Denial-of-Service (DoS) condition on the product, by using hardcoded user ID and password common to the product series obtained by exploiting CVE-2025-5022. However, the product is not affected by this vulnerability when it remains unused for a certain period of time (default: 5 minutes) and enters the power-saving mode with the display unit's LCD screen turned off. The affected products discontinued in 2015, support ended in 2020.	7.1	More Details
CVE-2025-50819	Directory traversal vulnerability in beiyuouo arxiv-daily thru 2025-05-06 (commit fad168770b0e68aef3e5acfa16bb2e7a7765d687) when parsing the the topic.yml file in the generation logic in daily_arxiv.py.	7.1	More Details
CVE-2025-1384	Least Privilege Violation (CWE-272) Vulnerability exists in the communication function between the NJ/NX-series Machine Automation Controllers and the Sysmac Studio Software. An attacker may use this vulnerability to perform unauthorized access and to execute unauthorized code remotely to the controller products.	7.0	More Details
CVE-2025-53621	DSpace open source software is a repository application which provides durable access to digital resources. Two related XML External Entity (XXE) injection possibilities impact all versions of DSpace prior to 7.6.4, 8.2, and 9.1. External entities are not disabled when parsing XML files during import of an archive (in Simple Archive Format), either from command-line (`./dspace import` command) or from the "Batch Import (Zip)" user interface feature. External entities are also not explicitly disabled when parsing XML responses from some upstream services (ArXiv, Crossref, OpenAIRE, Creative Commons) used in import from external sources via the user interface or REST API. An XXE injection in these files may result in a connection being made to an attacker's site or a local path readable by the Tomcat user, with content potentially being injected into a metadata field. In the latter case, this may result in sensitive content disclosure, including retrieving arbitrary files or configurations from the server where DSpace is running. The Simple Archive Format (SAF) importer / Batch Import (Zip) is only usable by site administrators (from user interface / REST API) or system administrators (from command-line). Therefore, to exploit this vulnerability, the malicious payload would have to be provided by an attacker and trusted by an administrator, who would trigger the import. The fix is included in DSpace 7.6.4, 8.2, and 9.1. Please upgrade to one of these versions. For those who cannot upgrade immediately, it is possible to manually patch the DSpace backend. One may also apply some best practices, though the protection provided is not as complete as upgrading. Administrators must carefully inspect any SAF archives (they did not construct themselves) before importing. As necessary, affected external services can be disabled to mitigate the ability for payloads to be delivered via external service APIs.	6.9	More Details
CVE-2025-30024	The communication protocol used between client and server had a flaw that could be leveraged to execute a man in the middle attack.	6.8	More Details
CVE-2024-38327	IBM Analytics Content Hub 2.0, 2.1, 2.2, and 2.3 is vulnerable to information exposure and further attacks due to an exposed JavaScript source map which could assist an attacker to read and debug JavaScript used in the application's API.	6.8	More Details
CVE-2025-27028	The Linux deprivileged user vpuser in Radiflow iSAP Smart Collector (CentOS 7 - VSAP 1.20) can read the entire file system content, including files belonging to other users and having restricted access (like, for example, the root password hash).	6.8	More Details
CVE-2024-39752	IBM Analytics Content Hub 2.0, 2.1, 2.2, and 2.3 could be vulnerable to malicious file upload by not validating the type of file uploaded to Explore Content. Attackers can make use of this weakness and upload malicious executable files into the system, and it can be sent to victim for performing further attacks.	6.8	More Details
CVE-2025-52363	Tenda CP3 Pro Firmware V22.5.4.93 contains a hardcoded root password hash in the /etc/passwd file and /etc/passwd-. An attacker with access to the firmware image can extract and attempt to crack the root password hash, potentially obtaining administrative access	6.8	More Details
CVE-2025-7519	A flaw was found in polkit. When processing an XML policy with 32 or more nested elements in depth, an out-of-bounds write can be triggered. This issue can lead to a crash or other unexpected behavior, and arbitrary code execution is not discarded. To exploit this flaw, a high-privilege account is needed as it's required to place the malicious policy file properly.	6.7	More Details
CVE-2025-52988	An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in the CLI of Juniper Networks Junos OS and Junos OS Evolved allows a high privileged, local attacker to escalated their privileges to root. When a user provides specifically crafted arguments to the 'request system logout' command, these will be executed as root on the shell, which can completely compromise the device. This issue affects: Junos OS: * all versions before 21.2R3-S9, * 21.4 versions before 21.4R3-S8, * 22.2 versions before 22.2R3-S6, * 22.3 versions before 22.3R3-S3, * 22.4 versions before 22.4R3-S6, * 23.2 versions before 23.2R2-S1, * 23.4 versions before 23.4R1-S2, 23.4R2; Junos OS Evolved: * all versions before 22.4R3-S6-EVO, * 23.2-EVO versions before 23.2R2-S1-EVO, * 23.4-EVO versions before 23.4R1-S2-EVO, 23.4R2-EVO.	6.7	More Details
CVE-2025-50068	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Cluster executes to compromise MySQL Cluster. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	6.7	More Details

	(CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).		
CVE-2025-53659	Jenkins QMetry Test Management Plugin 1.13 and earlier stores Qmetry Automation API Keys unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	6.5	More Details
CVE-2025-53742	Jenkins Applitools Eyes Plugin 1.16.5 and earlier stores Applitools API keys unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	6.5	More Details
CVE-2025-53662	Jenkins IFTTT Build Notifier Plugin 1.2 and earlier stores IFTTT Maker Channel Keys unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	6.5	More Details
CVE-2025-53672	Jenkins Kryptowire Plugin 0.2 and earlier stores the Kryptowire API key unencrypted in its global configuration file on the Jenkins controller, where it can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2021-27961	evesys 7.1 (2152) through 8.0 (2202) allows Reflected XSS via the indexeva.php action parameter.	6.5	More Details
CVE-2025-44525	Texas Instruments CC2652RB LaunchPad SimpleLink CC13XX CC26XX SDK 7.41.00.17 was discovered to utilize insufficient permission checks on critical fields within Bluetooth Low Energy (BLE) data packets. This issue allows attackers to cause a Denial of Service (DoS) via a crafted LL_Length_Req packet.	6.5	More Details
CVE-2025-53678	Jenkins User1st uTester Plugin 1.1 and earlier stores the uTester JWT token unencrypted in its global configuration file on the Jenkins controller, where it can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2025-53676	Jenkins Xooa Plugin 0.0.7 and earlier stores the Xooa Deployment Token unencrypted in its global configuration file on the Jenkins controller, where it can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2025-53675	Jenkins Warrior Framework Plugin 1.2 and earlier stores passwords unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	6.5	More Details
CVE-2025-53673	Jenkins Sensedia Api Platform tools Plugin 1.0 stores the Sensedia API Manager integration token unencrypted in its global configuration file on the Jenkins controller, where it can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2025-53671	Jenkins Nouvola DiveCloud Plugin 1.08 and earlier does not mask DiveCloud API Keys and Credentials Encryption Keys displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	6.5	More Details
CVE-2025-53663	Jenkins IBM Cloud DevOps Plugin 2.0.16 and earlier stores SonarQube authentication tokens unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	6.5	More Details
CVE-2025-53670	Jenkins Nouvola DiveCloud Plugin 1.08 and earlier stores DiveCloud API Keys and Credentials Encryption Keys unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	6.5	More Details
CVE-2025-36104	IBM Storage Scale 5.2.3.0 and 5.2.3.1 could allow an authenticated user to obtain sensitive information from files due to the insecure permissions inherited through the SMB protocol.	6.5	More Details
CVE-2025-53668	Jenkins VAddy Plugin 1.2.8 and earlier stores Vaddy API Auth Keys unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	6.5	More Details
CVE-2025-2522	The Honeywell Experion PKS and OneWireless WDM contains Sensitive Information in Resource vulnerability in the component Control Data Access (CDA). An attacker could potentially exploit this vulnerability, leading to a Communication Channel Manipulation, which could result in buffer reuse which may cause incorrect system behavior. Honeywell also recommends updating to the most recent version of Honeywell Experion PKS:520.2 TCU9 HF1 and 530.1 TCU3 HF1 and OneWireless: 322.5 and 331.1. The affected Experion PKS products are C300, FIM4, FIM8, UOC, CN100, HCA, C300PM, and C200E. The Experion PKS versions affected are 520.1 before 520.2 TCU9 HF1 and 530 before 530 TCU3. The OneWireless WDM affected versions are 322.1 through 322.4 and 330.1 through 330.3.	6.5	More Details
CVE-2025-53666	Jenkins Dead Man's Snitch Plugin 0.1 stores Dead Man's Snitch tokens unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	6.5	More Details
CVE-2025-53664	Jenkins Apica Loadtest Plugin 1.10 and earlier stores Apica Loadtest LTP authentication tokens unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	6.5	More Details
CVE-2025-53656	Jenkins ReadyAPI Functional Testing Plugin 1.11 and earlier stores SLM License Access Keys, client secrets, and passwords unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	6.5	More Details
CVE-2025-52081	In Netgear XR300 V1.0.3.38_10.3.30, a stack-based buffer overflow vulnerability exists in the HTTPD service through the usb_device.cgi endpoint. The vulnerability occurs when processing POST requests containing the usb_folder parameter.	6.5	More Details

CVE-2025-53654	Jenkins Statistics Gatherer Plugin 2.0.3 and earlier stores the AWS Secret Key unencrypted in its global configuration file on the Jenkins controller, where it can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2025-4593	The WP Register Profile With Shortcode plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.6.2 via the 'rp_user_data' shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive data from user meta like hashed passwords, usernames, and more.	6.5	More Details
CVE-2025-52955	An Incorrect Calculation of Buffer Size vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause a memory corruption that leads to a rpd crash. When the logical interface using a routing instance flaps continuously, specific updates are sent to the jflow/sflow modules. This results in memory corruption, leading to an rpd crash and restart. Continued receipt of these specific updates will cause a sustained Denial of Service condition. This issue affects Junos OS: * All versions before 21.2R3-S9, * All versions of 21.4, * All versions of 22.2, * from 22.4 before 22.4R3-S7, * from 23.2 before 23.2R2-S3, * from 23.4 before 23.4R2-S4, * from 24.2 before 24.2R2. Junos OS Evolved: * All versions of 21.2-EVO, * All versions of 21.4-EVO, * All versions of 22.2-EVO, * from 22.4 before 22.4R3-S7-EVO, * from 23.2 before 23.2R2-S3-EVO, * from 23.4 before 23.4R2-S4-EVO, * from 24.2 before 24.2R2-EVO.	6.5	More Details
CVE-2025-52953	An Expected Behavior Violation vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker sending a valid BGP UPDATE packet to cause a BGP session reset, resulting in a Denial of Service (DoS). Continuous receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects iBGP and eBGP and both IPv4 and IPv6 are affected by this vulnerability. This issue affects Junos OS: * All versions before 21.2R3-S9, * from 21.4 before 21.4R3-S11, * from 22.2 before 22.2R3-S7, * from 22.4 before 22.4R3-S7, * from 23.2 before 23.2R2-S4, * from 23.4 before 23.4R2-S4, * from 24.2 before 24.2R2, * from 24.4 before 24.4R1-S3, 24.4R2 Junos OS Evolved: * All versions before 22.2R3-S7-EVO, * from 22.4-EVO before 22.4R3-S7-EVO, * from 23.2-EVO before 23.2R2-S4-EVO, * from 23.4-EVO before 23.4R2-S4-EVO, * from 24.2-EVO before 24.2R2-EVO, * from 24.4-EVO before 24.4R1-S3-EVO, 24.4R2-EVO.	6.5	More Details
CVE-2025-52952	An Out-of-bounds Write vulnerability in the connectivity fault management (CFM) daemon of Juniper Networks Junos OS on MX Series with MPC-BUILTIN, MPC1 through MPC9 line cards allows an unauthenticated adjacent attacker to send a malformed packet to the device, leading to an FPC crash and restart, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks: Junos OS: * All versions before 22.2R3-S1, * from 22.4 before 22.4R2. This feature is not enabled by default.	6.5	More Details
CVE-2025-52949	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a logically adjacent BGP peer sending a specifically malformed BGP packet to cause rpd to crash and restart, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Only systems configured for Ethernet Virtual Private Networking (EVPN) signaling are vulnerable to this issue. This issue affects iBGP and eBGP, and both IPv4 and IPv6 are affected by this vulnerability.This issue affects: Junos OS: * all versions before 21.4R3-S11, * from 22.2 before 22.2R3-S7, * from 22.4 before 22.4R3-S7, * from 23.2 before 23.2R2-S4, * from 23.4 before 23.4R2-S5, * from 24.2 before 24.2R2-S1, * from 24.4 before 24.4R1-S3, 24.4R2; Junos OS Evolved: * all versions before 22.2R3-S7-EVO, * from 22.4-EVO before 22.4R3-S7-EVO, * from 23.2-EVO before 23.2R2-S4-EVO, * from 23.4-EVO before 23.4R2-S5-EVO, * from 24.2-EVO before 24.2R2-S1-EVO, * from 24.4-EVO before 24.4R1-S3-EVO, 24.4R2-EVO.	6.5	More Details
CVE-2025-52947	An Improper Handling of Exceptional Conditions vulnerability in route processing of Juniper Networks Junos OS on specific end-of-life (EOL) ACX Series platforms allows an attacker to crash the Forwarding Engine Board (FEB) by flapping an interface, leading to a Denial of Service (DoS). On ACX1000, ACX1100, ACX2000, ACX2100, ACX2200, ACX4000, ACX5048, and ACX5096 devices, FEB0 will crash when the primary path port of the L2 circuit IGP (Interior Gateway Protocol) on the local device goes down. This issue is seen only when 'hot-standby' mode is configured for the L2 circuit. This issue affects Junos OS on ACX1000, ACX1100, ACX2000, ACX2100, ACX2200, ACX4000, ACX5048, and ACX5096: * all versions before 21.2R3-S9.	6.5	More Details
CVE-2025-51591	A Server-Side Request Forgery (SSRF) in JGM Pandoc v3.6.4 allows attackers to gain access to and compromise the whole infrastructure via injecting a crafted iframe.	6.5	More Details
CVE-2025-6549	An Incorrect Authorization vulnerability in the web server of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to reach the Juniper Web Device Manager (J-Web). When Juniper Secure connect (JSC) is enabled on specific interfaces, or multiple interfaces are configured for J-Web, the J-Web UI is reachable over more than the intended interfaces. This issue affects Junos OS: * all versions before 21.4R3-S9, * 22.2 versions before 22.2R3-S5, * 22.4 versions before 22.4R3-S5, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S5, * 24.2 versions before 24.2R2.	6.5	More Details
CVE-2025-50083	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2025-50082	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2025-3631	An IBM MQ 9.3 and 9.4 Client connecting to an MQ Queue Manager can cause a SIGSEGV in the AMQRMPPA channel process terminating it.	6.5	More Details
CVE-2025-44526	Realtek RTL8762EKF-EVB RTL8762E SDK V1.4.0 was discovered to utilize insufficient permission checks on critical fields within Bluetooth Low Energy (BLE) data packets. This issue allows attackers to cause a Denial of Service (DoS) via a crafted LL_Length_Req packet.	6.5	More Details
CVE-2025-50078	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector:	6.5	More Details

	(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).		
CVE-2025-50076	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.0-8.0.25. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2025-30753	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2025-53509	A vulnerability exists in Advantech iView that allows for argument injection in the NetworkServlet.restoreDatabase(). This issue requires an authenticated attacker with at least user-level privileges. An input parameter can be used directly in a command without proper sanitization, allowing arbitrary arguments to be injected. This can result in information disclosure, including sensitive database credentials.	6.5	More Details
CVE-2025-52082	In Netgear XR300 V1.0.3.38_10.3.30, a stack-based buffer overflow exists in the HTTPD service through the usb_device.cgi endpoint. The vulnerability occurs when processing POST requests containing the read_access parameter.	6.5	More Details
CVE-2025-52459	A vulnerability exists in Advantech iView that allows for argument injection in NetworkServlet.backupDatabase(). This issue requires an authenticated attacker with at least user-level privileges. Certain parameters can be used directly in a command without proper sanitization, allowing arbitrary arguments to be injected. This can result in information disclosure, including sensitive database credentials.	6.5	More Details
CVE-2025-53822	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the `relatorio_geracao.php` endpoint of the WeGIA application prior to version 3.4.5. This vulnerability allows attackers to inject malicious scripts in the `tipo_relatorio` parameter. Version 3.4.5 has a patch for the issue.	6.5	More Details
CVE-2025-52080	In Netgear XR300 V1.0.3.38_10.3.30, a stack-based buffer overflow vulnerability exists in the HTTPD service through the usb_device.cgi endpoint. The vulnerability occurs when processing POST requests containing the share_name parameter.	6.5	More Details
CVE-2025-7204	In ConnectWise PSA versions older than 2025.9, a vulnerability exists where authenticated users could gain access to sensitive user information. Specific API requests were found to return an overly verbose user object, which included encrypted password hashes for other users. Authenticated users could then retrieve these hashes. An attacker or privileged user could then use these exposed hashes to conduct offline brute-force or dictionary attacks. Such attacks could lead to credential compromise, allowing unauthorized access to accounts, and potentially privilege escalation within the system.	6.5	More Details
CVE-2025-53889	Directus is a real-time API and App dashboard for managing SQL database content. Starting in version 9.12.0 and prior to version 11.9.0, Directus Flows with a manual trigger are not validating whether the user triggering the Flow has permissions to the items provided as payload to the Flow. Depending on what the Flow is set up to do this can lead to the Flow executing potential tasks on the attacker's behalf without authenticating. Bad actors could execute the manual trigger Flows without authentication, or access rights to the said collection(s) or item(s). Users with manual trigger Flows configured are impacted as these endpoints do not currently validate if the user has read access to `directus_flows` or to the relevant collection/items. The manual trigger Flows should have tighter security requirements as compared to webhook Flows where users are expected to perform do their own checks. Version 11.9.0 fixes the issue. As a workaround, implement permission checks for read access to Flows and read access to relevant collection/items.	6.5	More Details
CVE-2025-3780	The WCFM – Frontend Manager for WooCommerce along with Bookings Subscription Listings Compatible plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the wcfm_redirect_to_setup function in all versions up to, and including, 6.7.16. This makes it possible for unauthenticated attackers to view and modify the plugin settings, including payment details and API keys	6.5	More Details
CVE-2025-49464	Classic buffer overflow in certain Zoom Clients for Windows may allow an authorised user to conduct a denial of service via network access.	6.5	More Details
CVE-2025-35983	Improper Certificate Validation (CWE-295) in the Controller 7000 OneLink implementation could allow an unprivileged attacker to perform a limited denial of service or perform privileged overrides during the initial configuration of the Controller, there is no risk for Controllers once they are connected. This issue affects Controller 7000: 9.30 prior to vCR9.30.250624a (distributed in 9.30.1871 (MR1)).	6.5	More Details
CVE-2025-5022	Weak Password Requirements vulnerability in Mitsubishi Electric Corporation photovoltaic system monitor “EcoGuideTAB” PV-DR004J all versions and PV-DR004JA all versions allows an attacker within the Wi-Fi communication range between the units of the product (measurement unit and display unit) to derive the password from the SSID. However, the product is not affected by this vulnerability when it remains unused for a certain period of time (default: 5 minutes) and enters the power-saving mode with the display unit's LCD screen turned off. The affected products discontinued in 2015, support ended in 2020.	6.5	More Details
CVE-2025-53820	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the `index.php` endpoint of the WeGIA application prior to version 3.4.5. This vulnerability allows attackers to inject malicious scripts in the `erro` parameter. Version 3.4.5 contains a patch for the issue.	6.5	More Details
CVE-2025-32988	A flaw was found in GnuTLS. A double-free vulnerability exists in GnuTLS due to incorrect ownership handling in the export logic of Subject Alternative Name (SAN) entries containing an otherName. If the type-id OID is invalid or malformed, GnuTLS will call asn1_delete_structure() on an ASN.1 node it does not own, leading to a double-free condition when the parent function or caller later attempts to free the same structure. This vulnerability can be triggered using only public GnuTLS APIs and may result in denial of service or memory corruption, depending on allocator behavior.	6.5	More Details
CVE-	Classic buffer overflow in certain Zoom Clients for Windows may allow an authorized user to conduct a denial of service via network		More

2025-46789	access.	6.5	Details
CVE-2025-6395	A NULL pointer dereference flaw was found in the GnuTLS software in _gnutls_figure_common_ciphersuite().	6.5	More Details
CVE-2024-42648	NanoMQ v0.22.10 was discovered to contain a heap overflow which allows attackers to cause a Denial of Service (DoS) via a crafted CONNECT message.	6.5	More Details
CVE-2024-42649	NanoMQ v0.22.10 was discovered to contain a memory leak which allows attackers to cause a Denial of Service (DoS) via a crafted PUBLISH message.	6.5	More Details
CVE-2025-49463	Insufficient control flow management in certain Zoom Clients for iOS before version 6.4.5 may allow an unauthenticated user to conduct a disclosure of information via network access.	6.5	More Details
CVE-2025-32990	A heap-buffer-overflow (off-by-one) flaw was found in the GnuTLS software in the template parsing logic within the certtool utility. When it reads certain settings from a template file, it allows an attacker to cause an out-of-bounds (OOB) NULL pointer write, resulting in memory corruption and a denial-of-service (DoS) that could potentially crash the system.	6.5	More Details
CVE-2025-52964	A Reachable Assertion vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When the device receives a specific BGP UPDATE packet, the rpd crashes and restarts. Continuous receipt of this specific packet will cause a sustained DoS condition. For the issue to occur, BGP multipath with "pause-computation-during-churn" must be configured on the device, and the attacker must send the paths via a BGP UPDATE from a established BGP peer. This issue affects: Junos OS: * All versions before 21.4R3-S7, * from 22.3 before 22.3R3-S3, * from 22.4 before 22.4R3-S5, * from 23.2 before 23.2R2, * from 23.4 before 23.4R2. Junos OS Evolved: * All versions before 21.4R3-S7-EVO, * from 22.3 before 22.3R3-S3-EVO, * from 22.4 before 22.4R3-S5-EVO, * from 23.2 before 23.2R2-EVO, * from 23.4 before 23.4R2-EVO.	6.5	More Details
CVE-2025-5678	The Gutenberg Blocks with AI by Kadence WP – Page Builder Features plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘redirectURL’ parameter in all versions up to, and including, 3.5.10 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-2025-5530	The WPC Smart Compare for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'shortcode_btn' shortcode in all versions up to, and including, 6.4.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-33097	IBM QRadar SIEM 7.5 - 7.5.0 UP12 IF02 is vulnerable to stored cross-site scripting. This vulnerability allows authenticated users 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-2025-7367	The Strong Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Testimonial Custom Fields in all versions up to, and including, 3.2.11 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-6976	The Events Manager – Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes in all versions up to, and including, 7.0.3 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-2025-50071	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Web Utilities). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Framework. While the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data as well as unauthorized read access to a subset of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N).	6.4	More Details
CVE-2025-7059	The Simple Featured Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘slideshow’ parameter in all versions up to, and including, 1.3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-7213	A vulnerability classified as critical has been found in FNKvision FNK-GU2 up to 40.1.7. Affected is an unknown function of the component UART Interface. The manipulation leads to on-chip debug and test interface with improper access control. It is possible to launch the attack on the physical device. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used.	6.4	More Details
CVE-2025-6716	The Photos, Files, YouTube, Twitter, Instagram, TikTok, Ecommerce Contest Gallery – Upload, Vote, Sell via PayPal or Stripe, Social Share Buttons, OpenAI plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'upload[1][title]' parameter in all versions up to, and including, 26.0.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-53865	In Roundup before 2.5.0, XSS can occur via interaction between URLs and issue tracker templates (devel and responsive).	6.4	More Details

CVE-2025-6068	The FooGallery – Responsive Photo Gallery, Image Viewer, Justified, Masonry & Carousel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `data-caption-title` & `data-caption-description` HTML attributes in all versions up to, and including, 2.4.31 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-2025-7559	A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2. It has been classified as critical. This affects an unknown part of the file /admin/bwdates-report-result.php. The manipulation of the argument fromdate/todate leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7585	A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2. It has been classified as critical. Affected is an unknown function of the file /admin/manage-site.php. The manipulation of the argument webtitle leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7525	A vulnerability was found in TOTOLINK T6 4.1.5cu.748_B20211015. It has been declared as critical. This vulnerability affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi of the component HTTP POST Request Handler. The manipulation of the argument command leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7558	A vulnerability was found in code-projects Voting System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/positions_add.php. The manipulation of the argument description leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7524	A vulnerability was found in TOTOLINK T6 4.1.5cu.748_B20211015. It has been classified as critical. This affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi of the component HTTP POST Request Handler. The manipulation of the argument ip leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7591	A vulnerability, which was classified as critical, was found in PHPGurukul Dairy Farm Shop Management System 1.3. Affected is an unknown function of the file view-invoice.php. The manipulation of the argument invid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7592	A vulnerability has been found in PHPGurukul Dairy Farm Shop Management System 1.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the file invoices.php. The manipulation of the argument del 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-2025-7557	A vulnerability has been found in code-projects Voting System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/voters_row.php. The 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-2025-7590	A vulnerability, which was classified as critical, has been found in PHPGurukul Dairy Farm Shop Management System 1.3. This issue affects some unknown processing of the file edit-category.php. The manipulation of the argument categorycode leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7522	A vulnerability has been found in PHPGurukul Vehicle Parking Management System 1.13 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/bwdates-reports-details.php. The manipulation of the argument fromdate/todate 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-2025-7589	A vulnerability classified as critical was found in PHPGurukul Dairy Farm Shop Management System 1.3. This vulnerability affects unknown code of the file edit-company.php. The manipulation of the argument companyname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7556	A vulnerability, which was classified as critical, was found in code-projects Voting System 1.0. Affected is an unknown function of the file /admin/voters_edit.php. The manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7588	A vulnerability classified as critical has been found in PHPGurukul Dairy Farm Shop Management System 1.3. This affects an unknown part of the file edit-product.php. The manipulation of the argument productname leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7210	A vulnerability was found in code-projects/Fabian Ros Library Management System 2.0 and classified as critical. Affected by this issue is some unknown functionality of the file admin/profile_update.php. The manipulation of the argument photo leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7584	A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2 and classified as critical. This issue affects some unknown processing of the file /admin/add-team.php. The manipulation of the argument teammember leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7583	A vulnerability has been found in PHPGurukul Online Fire Reporting System 1.2 and classified as critical. This vulnerability affects unknown code of the file /admin/all-requests.php. The manipulation of the argument teamid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7582	A vulnerability, which was classified as critical, was found in PHPGurukul Online Fire Reporting System 1.2. This affects an unknown part of the file /admin/assigned-requests.php. The manipulation of the argument teamid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7581	A vulnerability, which was classified as critical, has been found in code-projects Voting System 1.0. Affected by this issue is some unknown functionality of the file /admin/positions_edit.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7560	A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2. It has been declared as critical. This vulnerability affects unknown code of the file /admin/workin-progress-requests.php. The manipulation of the argument teamid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE-2025-7580	A vulnerability classified as critical was found in code-projects Voting System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/positions_row.php. The 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-2025-7520	A vulnerability, which was classified as critical, has been found in PHPGurukul Vehicle Parking Management System 1.13. This issue affects some unknown processing of the file /admin/manage-category.php. The manipulation of the argument del leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7543	A vulnerability was found in PHPGurukul User Registration & Login and User Management System 3.3. It has been classified as critical. This affects an unknown part of the file /admin/manage-users.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7452	A vulnerability was found in kone-net go-chat up to f9e58d0afa9bbdb31faf25e7739da330692c4c63. It has been declared as critical. This vulnerability affects the function GetFile of the file go-chat/api/v1/file_controller.go of the component Endpoint. The manipulation of the argument fileName leads to path traversal. The attack can be initiated 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.	6.3	More Details
CVE-2025-7212	A vulnerability was found in itsourcecode Insurance Management System up to 1.0. It has been rated as critical. This issue affects some unknown processing of the file /insertAgent.php. The manipulation of the argument agent_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7568	A vulnerability was found in qianfox FoxCMS up to 1.2.5. It has been classified as critical. Affected is the function batchCope of the file app/admin/controller/Video.php. The manipulation of the argument ids leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-7563	A vulnerability classified as critical was found in PHPGurukul Online Fire Reporting System 1.2. Affected by this vulnerability is an unknown functionality of the file /admin/completed-requests.php. The manipulation of the argument teamid 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-2025-7562	A vulnerability classified as critical has been found in PHPGurukul Online Fire Reporting System 1.2. Affected is an unknown function of the file /admin/new-requests.php. The manipulation of the argument teamid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-47963	No cwe for this issue in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	6.3	More Details
CVE-2025-7561	A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2. It has been rated as critical. This issue affects some unknown processing of the file /admin/team-ontheway-requests.php. The manipulation of the argument teamid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-53834	Caido is a web security auditing toolkit. A reflected cross-site scripting (XSS) vulnerability was discovered in Caido's toast UI component in versions prior to 0.49.0. Toast messages may reflect unsanitized user input in certain tools such as Match&Replace and Scope. This could allow an attacker to craft input that results in arbitrary script execution. Version 0.49.0 fixes the issue.	6.3	More Details
CVE-2025-7555	A vulnerability, which was classified as critical, has been found in code-projects Voting System 1.0. This issue affects some unknown processing of the file /admin/voters_add.php. The manipulation of the argument firstname/lastname leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7599	A vulnerability, which was classified as critical, has been found in PHPGurukul Dairy Farm Shop Management System 1.3. Affected by this issue is some unknown functionality of the file /invoice.php. The manipulation of the argument del leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7627	A vulnerability was found in YiJiuSmile kkFileViewOfficeEdit up to 5fbc57c48e8fe6c1b91e0e7995e2d59615f37abd and classified as critical. Affected by this issue is the function fileUpload of the file /fileUpload. The manipulation of the argument File leads to unrestricted upload. The attack may be launched 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.	6.3	More Details
CVE-2025-7479	A vulnerability has been found in PHPGurukul Vehicle Parking Management System 1.13 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /users/view--detail.php. The manipulation of the argument viewid 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-2025-7412	A vulnerability was found in code-projects Library System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /user/student/profile.php. The manipulation of the argument image leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7552	A vulnerability was found in Dromara Northstar up to 7.3.5. It has been rated as critical. Affected by this issue is the function preHandle of the file northstar-main/src/main/java/org/dromara/northstar/web/interceptor/AuthorizationInterceptor.java of the component Path Handler. The manipulation of the argument Request leads to improper access controls. The attack may be launched remotely. Upgrading to version 7.3.6 is able to address this issue. The patch is identified as 8d521bbf531de59b09b8629a9cbf667870ad2541. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2025-7413	A vulnerability classified as critical has been found in code-projects Library System 1.0. This affects an unknown part of the file /user/teacher/profile.php. The manipulation of the argument image leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7481	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13. It has been classified as critical. This affects an unknown part of the file /users/profile.php. The manipulation of the argument firstname leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	6.3	More Details
CVE-2025-	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13. It has been declared as critical. This vulnerability affects unknown code of the file /users/print.php. The manipulation of the argument vid leads to sql injection. The	6.3	More

7482	attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		Details
CVE-2025-7414	A vulnerability classified as critical was found in Tenda O3V2 1.0.0.12(3880). This vulnerability affects the function fromNetToolGet of the file /goform/setPingInfo of the component httpd. The manipulation of the argument domain leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7415	A vulnerability, which was classified as critical, has been found in Tenda O3V2 1.0.0.12(3880). This issue affects the function fromTraceroutGet of the file /goform/getTraceroute of the component httpd. The manipulation of the argument dest leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7615	A vulnerability classified as critical was found in TOTOLINK T6 4.1.5cu.748. Affected by this vulnerability is the function clearPairCfg of the file /cgi-bin/cstecgi.cgi of the component HTTP POST Request Handler. The manipulation of the argument ip leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7614	A vulnerability classified as critical has been found in TOTOLINK T6 4.1.5cu.748. Affected is the function delDevice of the file /cgi-bin/cstecgi.cgi of the component HTTP POST Request Handler. The manipulation of the argument ipAddr leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7484	A vulnerability classified as critical has been found in PHPGurukul Vehicle Parking Management System 1.13. Affected is an unknown function of the file /admin/view-outgoingvehicle-detail.php. The manipulation of the argument viewid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7487	A vulnerability, which was classified as critical, was found in JoeyBling SpringBoot_MyBatisPlus up to a6a825513bd688f717dbae3a196bc9c9622fea26. This affects the function SysFileController of the file /file/upload. The manipulation of the argument portraitFile 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 takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	6.3	More Details
CVE-2025-7613	A vulnerability was found in TOTOLINK T6 4.1.5cu.748. It has been rated as critical. This issue affects the function CloudSrvVersionCheck of the file /cgi-bin/cstecgi.cgi of the component HTTP POST Request Handler. The manipulation of the argument ip leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7489	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13 and classified as critical. This issue affects some unknown processing of the file /admin/search-vehicle.php. The manipulation of the argument searchdata leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-53651	Jenkins HTML Publisher Plugin 425 and earlier displays log messages that include the absolute paths of files archived during the Publish HTML reports post-build step, exposing information about the Jenkins controller file system in the build log.	6.3	More Details
CVE-2025-7511	A vulnerability was found in code-projects Chat System 1.0 and classified as critical. This issue affects some unknown processing of the file /user/update_account.php. The manipulation of the argument musername leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7490	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13. It has been classified as critical. Affected is an unknown function of the file /admin/reg-users.php. The manipulation of the argument del leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7600	A vulnerability, which was classified as critical, was found in PHPGurukul Online Library Management System 3.0. This affects an unknown part of the file /admin/student-history.php. The manipulation of the argument stdid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7491	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/manage-outgoingvehicle.php. The manipulation of the argument del 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-2025-7407	A vulnerability, which was classified as critical, was found in Netgear D6400 1.0.0.114. This affects an unknown part of the file diag.cgi. The manipulation of the argument host_name leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early and confirmed the existence of the vulnerability. They reacted very quickly, professional and kind. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2025-7492	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/manage-incomingvehicle.php. The manipulation of the argument del leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2023-38329	An issue was discovered in eGroupWare 17.1.20190111. A cross-site scripting Reflected (XSS) vulnerability exists in calendar/freebusy.php, which allows unauthenticated remote attackers to inject arbitrary web script or HTML into the "user" HTTP/GET parameter, which reflects its input without sanitization.	6.1	More Details
CVE-2025-50107	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Request handling). Supported versions that are affected are 12.2.5-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Universal Work Queue, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Universal Work Queue accessible data as well as unauthorized read access to a subset of Oracle Universal Work Queue accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2025-53626	pdfme is a TypeScript-based PDF generator and React-based UI. The expression evaluation feature in pdfme 5.2.0 to 5.4.0 contains critical vulnerabilities allowing sandbox escape leading to XSS and prototype pollution attacks. This vulnerability is fixed in 5.4.1.	6.1	More Details
CVE-			

2025- 28245	Cross-site scripting (XSS) vulnerability in Alteryx Server 2023.1.1.460 allows remote attackers to inject arbitrary web script or HTML via the notification body.	6.1	More Details
CVE- 2025- 6975	The Events Manager – Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'calendar_header' parameter in all versions up to, and including, 7.0.3 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- 45662	A cross-site scripting (XSS) vulnerability in the component /master/login.php of mpgram-web commit 94baadb allows attackers to execute arbitrary Javascript in the context of a user's browser via a crafted payload.	6.1	More Details
CVE- 2025- 30746	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iStore accessible data as well as unauthorized read access to a subset of Oracle iStore accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE- 2025- 5807	The Gwolle Guestbook plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'gwolle_gb_content' parameter in all versions up to, and including, 4.9.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.1	More Details
CVE- 2025- 6234	The Hostel WordPress plugin before 1.1.5.8 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	6.1	More Details
CVE- 2025- 30745	Vulnerability in the Oracle MES for Process Manufacturing product of Oracle E-Business Suite (component: Device Integration). Supported versions that are affected are 12.2.12-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle MES for Process Manufacturing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle MES for Process Manufacturing, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle MES for Process Manufacturing accessible data as well as unauthorized read access to a subset of Oracle MES for Process Manufacturing accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE- 2024- 36697	A cross-site scripting (XSS) vulnerability in the Admin Login page of Allworx System Software v9.1.9.12 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the SessionID parameter at query.asp.	6.1	More Details
CVE- 2025- 30748	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 8.60, 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE- 2025- 30756	Vulnerability in Oracle REST Data Services (component: General). The supported version that is affected is 24.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle REST Data Services. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle REST Data Services, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle REST Data Services accessible data as well as unauthorized read access to a subset of Oracle REST Data Services accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE- 2025- 30759	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Platform Security). Supported versions that are affected are 7.6.0.0.0, 8.2.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE- 2025- 50073	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE- 2025- 53030	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected		

CVE-2025-53026	is 7.1.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2025-53025	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2025-30761	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf and 11.0.27; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	5.9	More Details
CVE-2025-52948	An Improper Handling of Exceptional Conditions vulnerability in Berkeley Packet Filter (BPF) processing of Juniper Networks Junos OS allows an attacker, in rare cases, sending specific, unknown traffic patterns to cause the FPC and system to crash and restart. BPF provides a raw interface to data link layers in a protocol independent fashion. Internally within the Junos kernel, due to a rare timing issue (race condition), when a BPF instance is cloned, the newly created interface causes an internal structure leakage, leading to a system crash. The precise content and timing of the traffic patterns is indeterminate, but has been seen in a lab environment multiple times. This issue is more likely to occur when packet capturing is enabled. See required configuration below. This issue affects Junos OS: * all versions before 21.2R3-S9, * from 21.4 before 21.4R3-S10, * from 22.2 before 22.2R3-S6, * from 22.4 before 22.4R3-S7, * from 23.2 before 23.2R2-S3, * from 23.4 before 23.4R2-S3, * from 24.2 before 24.2R1-S1, 24.2R2.	5.9	More Details
CVE-2025-52982	An Improper Resource Shutdown or Release vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series with MS-MPC allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). When an MX Series device with an MS-MPC is configured with two or more service sets which are both processing SIP calls, a specific sequence of call events will lead to a crash and restart of the MS-MPC. This issue affects Junos OS: * all versions before 21.2R3-S9, * 21.4 versions from 21.4R1, * 22.2 versions before 22.2R3-S6, * 22.4 versions before 22.4R3-S6. As the MS-MPC is EoL after Junos OS 22.4, later versions are not affected. This issue does not affect MX-SPC3 or SRX Series devices.	5.9	More Details
CVE-2025-52473	liboqs is a C-language cryptographic library that provides implementations of post-quantum cryptography algorithms. Multiple secret-dependent branches have been identified in the reference implementation of the HQC key encapsulation mechanism when it is compiled with Clang for optimization levels above -O0 (-O1, -O2, etc). A proof-of-concept local attack exploits this secret-dependent information to recover the entire secret key. This vulnerability is fixed in 0.14.0.	5.9	More Details
CVE-2025-1735	In PHP versions:8.1.* before 8.1.33, 8.2.* before 8.2.29, 8.3.* before 8.3.23, 8.4.* pgsql and pdo_pgsql escaping functions do not check if the underlying quoting functions returned errors. This could cause crashes if Postgres server rejects the string as invalid.	5.9	More Details
CVE-2025-52984	A NULL Pointer Dereference vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause impact to the availability of the device. When static route points to a reject next hop and a gNMI query is processed for that static route, rpd crashes and restarts. This issue affects: Junos OS: * all versions before 21.2R3-S9, * 21.4 versions before 21.4R3-S10, * 22.2 versions before 22.2R3-S6, * 22.4 versions before 22.4R3-S6, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R1-S2, 24.2R2; Junos OS Evolved: * all versions before 22.4R3-S7-EVO, * 23.2-EVO versions before 23.2R2-S3-EVO, * 23.4-EVO versions before 23.4R2-S4-EVO, * 24.2-EVO versions before 24.2R2-EVO.	5.9	More Details
CVE-2025-6491	In PHP versions:8.1.* before 8.1.33, 8.2.* before 8.2.29, 8.3.* before 8.3.23, 8.4.* before 8.4.10 when parsing XML data in SOAP extensions, overly large (>2Gb) XML namespace prefix may lead to null pointer dereference. This may lead to crashes and affect the availability of the target server.	5.9	More Details
CVE-2021-4458	The Modern Events Calendar Lite plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter of the 'wp_ajax_mec_load_single_page' AJAX action in all versions up to, and including, 6.3.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This is only exploitable on sites with addslashes disabled.	5.9	More Details
CVE-2025-6200	The GeoDirectory WordPress plugin before 2.8.120 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.9	More Details
CVE-2025-53864	Connect2id Nimbus JOSE + JWT before 10.0.2 allows a remote attacker to cause a denial of service via a deeply nested JSON object supplied in a JWT claim set, because of uncontrolled recursion. NOTE: this is independent of the Gson 2.11.0 issue because the Connect2id product could have checked the JSON object nesting depth, regardless of what limits (if any) were imposed by Gson.	5.8	More Details
CVE-2025-52951	A Protection Mechanism Failure vulnerability in kernel filter processing of Juniper Networks Junos OS allows an attacker sending IPv6 traffic destined to the device to effectively bypass any firewall filtering configured on the interface. Due to an issue with Junos OS kernel filter processing, the 'payload-protocol' match is not being supported, causing any term containing it to accept all packets without taking any other action. In essence, these firewall filter terms were being processed as an 'accept' for all traffic on the interface destined for the control plane, even when used in combination with other match criteria. This issue only affects firewall filters protecting the device's control plane. Transit firewall filtering is unaffected by this vulnerability. This issue affects Junos OS: * all versions before 21.2R3-S9, * from 21.4 before 21.4R3-S11, * from 22.2 before 22.2R3-S7, * from 22.4 before 22.4R3-S7, * from 23.2 before 23.2R2-S4, * from 23.4 before 23.4R2-S5, * from 24.2 before 24.2R2-S1, * from 24.4 before 24.4R1-S2, 24.4R2. This is a more complete fix for previously published CVE-2024-21607 (JSA75748).	5.8	More Details

CVE-2025-48795	Apache CXF stores large stream based messages as temporary files on the local filesystem. A bug was introduced which means that the entire temporary file is read into memory and then logged. An attacker might be able to exploit this to cause a denial of service attack by causing an out of memory exception. In addition, it is possible to configure CXF to encrypt temporary files to prevent sensitive credentials from being cached unencrypted on the local filesystem, however this bug means that the cached files are written out to logs unencrypted. Users are recommended to upgrade to versions 3.5.11, 3.6.6, 4.0.7 or 4.1.1, which fixes this issue.	5.6	More Details
CVE-2025-47182	Improper input validation in Microsoft Edge (Chromium-based) allows an authorized attacker to bypass a security feature locally.	5.6	More Details
CVE-2025-51650	An arbitrary file upload vulnerability in the component /controller/PicManager.php of FoxCMS v1.2.6 allows attackers to execute arbitrary code via uploading a crafted template file.	5.6	More Details
CVE-2025-46406	A Privilege Context Switching Error (CWE-270) in the Command Center Server could allow a privileged Operator with high level access in one Division to perform limited privileged activities across the Division boundary. This issue affects Command Centre Server: 9.30 prior to 9.30.1874 (MR1), 9.20 prior to 9.20.2337 (MR3), 9.10 prior to 9.10.3194 (MR6), 9.00 prior to 9.00.3371 (MR7), all versions of 8.90 and prior.	5.6	More Details
CVE-2025-30739	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.2.11-12.2.13. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. While the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data as well as unauthorized read access to a subset of Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N).	5.5	More Details
CVE-2025-7616	A vulnerability, which was classified as critical, has been found in gmg137 snap7-rs up to 1.142.1. Affected by this issue is the function pthread_cond_destroy of the component Public API. The manipulation leads to memory corruption. The exploit has been disclosed to the public and may be used.	5.5	More Details
CVE-2025-50085	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2025-30483	Dell ECS versions prior to 3.8.1.5/ ObjectScale version 4.0.0.0 contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	5.5	More Details
CVE-2025-51651	An authenticated arbitrary file download vulnerability in the component /admin/Backups.php of Mccms v2.7.0 allows attackers to download arbitrary files via a crafted GET request.	5.5	More Details
CVE-2025-4369	The Companion Auto Update plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘update_delay_days’ parameter in all versions up to, and including, 3.9.2 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.	5.5	More Details
CVE-2025-52986	A Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a local, low privileged user to cause an impact to the availability of the device. When RIB sharding is enabled and a user executes one of several routing related 'show' commands, a certain amount of memory is leaked. When all available memory has been consumed rpd will crash and restart. The leak can be monitored with the CLI command: show task memory detail | match task_shard_mgmt_cookie where the allocated memory in bytes can be seen to continuously increase with each exploitation. This issue affects: Junos OS: * all versions before 21.2R3-S9, * 21.4 versions before 21.4R3-S11, * 22.2 versions before 22.2R3-S7, * 22.4 versions before 22.4R3-S7, * 23.2 versions before 23.2R2-S4, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R2, * 24.4 versions before 24.4R1-S2, 24.4R2; Junos OS Evolved: * all versions before 22.2R3-S7-EVO * 22.4-EVO versions before 22.4R3-S7-EVO, * 23.2-EVO versions before 23.2R2-S4-EVO, * 23.4-EVO versions before 23.4R2-S4-EVO, * 24.2-EVO versions before 24.2R2-EVO, * 24.4-EVO versions before 24.4R2-EVO.	5.5	More Details
CVE-2025-7387	The Lana Downloads Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the endpoint parameters in versions up to, and including, 1.10.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with administrator-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details
CVE-2025-52963	An Improper Access Control vulnerability in the User Interface (UI) of Juniper Networks Junos OS allows a local, low-privileged attacker to bring down an interface, leading to a Denial-of-Service. Users with "view" permissions can run a specific request interface command which allows the user to shut down the interface. This issue affects Junos OS: * All versions before 21.2R3-S9, * from 21.4 before 21.4R3-S11, * from 22.2 before 22.2R3-S7, * from 22.4 before 22.4R3-S7, * from 23.2 before 23.2R2-S4, * from 23.4 before 23.4R2-S5, * from 24.2 before 24.2R2-S1, * from 24.4 before 24.4R1-S3, 24.4R2.	5.5	More Details
CVE-2025-7208	A vulnerability was found in 9fans plan9port up to 9da5b44. It has been classified as critical. This affects the function edump in the library /src/plan9port/src/libsec/port/x509.c. The manipulation leads to heap-based buffer overflow. The exploit has been disclosed to the public and may 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 identifier of the patch is b3e06559475b0130a7a2fb56ac4d131d13d2012f. It is recommended to apply a patch to fix this issue.	5.5	More Details
CVE-2025-51659	SemCms v5.0 was discovered to contain a SQL injection vulnerability via the ID parameter at SEMCMS_Products.php.	5.4	More Details

CVE-2025-51658	SemCms v5.0 was discovered to contain a SQL injection vulnerability via the ID parameter at SEMCMS_InquiryView.php.	5.4	More Details
CVE-2025-51657	SemCms v5.0 was discovered to contain a SQL injection vulnerability via the lgid parameter at SEMCMS_Link.php.	5.4	More Details
CVE-2025-30760	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are 9.2.0.0-9.2.9.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2025-50108	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Workspace). The supported version that is affected is 11.2.20.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Financial Reporting, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Reporting accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2025-51656	SemCms v5.0 was discovered to contain a SQL injection vulnerability via the ID parameter at SEMCMS_Link.php.	5.4	More Details
CVE-2025-51655	SemCms v5.0 was discovered to contain a SQL injection vulnerability via the pid parameter at SEMCMS_Quanxian.php.	5.4	More Details
CVE-2025-51654	SemCms v5.0 was discovered to contain a SQL injection vulnerability via the pid parameter at SEMCMS_Infocategories.php.	5.4	More Details
CVE-2025-53636	Open OnDemand is an open-source HPC portal. Users can flood logs by interacting with the shell app and generating many errors. Users who flood logs can create very large log files causing a Denial of Service (DoS) to the ondemand system. This vulnerability is fixed in 3.1.14 and 4.0.6.	5.4	More Details
CVE-2025-50061	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 20.12.0-20.12.21, 21.12.0-21.12.21, 22.12.0-22.12.19, 23.12.0-23.12.13 and 24.12.0-24.12.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera P6 Enterprise Project Portfolio Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera P6 Enterprise Project Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2025-53824	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the editar_permissoes.php endpoint of the WeGIA application prior to version 3.4.4. This vulnerability allows attackers to inject malicious scripts in the msg_c parameter. Version 3.4.4 fixes the issue.	5.4	More Details
CVE-2025-53519	A vulnerability exists in Advantech iView versions prior to 5.7.05 build 7057, which could allow a reflected cross-site scripting (XSS) attack. By manipulating specific parameters, an attacker could execute unauthorized scripts in the user's browser, potentially leading to information disclosure or other malicious activities.	5.4	More Details
CVE-2025-7365	A flaw was found in Keycloak. When an authenticated attacker attempts to merge accounts with another existing account during an identity provider (IdP) login, the attacker will subsequently be prompted to "review profile" information. This vulnerability allows the attacker to modify their email address to match that of a victim's account, triggering a verification email sent to the victim's email address. The attacker's email address is not present in the verification email content, making it a potential phishing opportunity. If the victim clicks the verification link, the attacker can gain access to the victim's account.	5.4	More Details
CVE-2025-53397	A vulnerability exists in Advantech iView versions prior to 5.7.05 build 7057, which could allow a reflected cross-site scripting (XSS) attack. By exploiting this flaw, an attacker could execute unauthorized scripts in the user's browser, potentially leading to information disclosure or other malicious activities.	5.4	More Details
CVE-2025-41442	A vulnerability exists in Advantech iView versions prior to 5.7.05 build 7057, which could allow a reflected cross-site scripting (XSS) attack. By manipulating certain input parameters, an attacker could execute unauthorized scripts in the user's browser, potentially leading to information disclosure or other malicious activities.	5.4	More Details
CVE-2025-53709	Secure-upload is a data submission service that validates single-use tokens when accepting submissions to channels. The service only installed on a small number of environments. Under specific circumstances, privileged users of secure-upload could have selected email templates not necessarily created for their enrollment when sending data upload requests. Authenticated and privileged users of one enrollment could have abused an endpoint to redirect existing submission channels to a dataset they control. An endpoint handling domain validation allowed unauthenticated users to enumerate existing enrollments. Finally, other endpoints allowed enumerating if a resource with a known RID exists across enrollments. The affected service has been patched with version 0.815.0 and automatically deployed to all Apollo-managed Foundry instances.	5.4	More Details
CVE-2025-51652	SemCms v5.0 was discovered to contain a SQL injection vulnerability via the pid parameter at SEMCMS_Categories.php.	5.4	More Details

CVE-2025-51653	SemCms v5.0 was discovered to contain a SQL injection vulnerability via the pid parameter at SEMCMS_ct.php.	5.4	More Details
CVE-2025-51660	SemCms v5.0 was discovered to contain a SQL injection vulnerability via the lgid parameter at SEMCMS_Products.php.	5.4	More Details
CVE-2025-50090	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Personalization). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data as well as unauthorized read access to a subset of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2025-52379	Nexxt Solutions NCM-X1800 Mesh Router firmware UV1.2.7 and below contains an authenticated command injection vulnerability in the firmware update feature. The /web/um_fileName_set.cgi and /web/um_web_upgrade.cgi endpoints fail to properly sanitize the upgradeFileName parameter, allowing authenticated attackers to execute arbitrary OS commands on the device, resulting in remote code execution.	5.4	More Details
CVE-2025-47964	Microsoft Edge (Chromium-based) Spoofing Vulnerability	5.4	More Details
CVE-2025-53658	Jenkins Applitools Eyes Plugin 1.16.5 and earlier does not escape the Applitools URL on the build page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2025-7628	A vulnerability was found in YiJiuSmile kkFileViewOfficeEdit up to 5fbc57c48e8fe6c1b91e0e7995e2d59615f37abd. It has been classified as critical. This affects the function deleteFile of the file /deleteFile. The manipulation of the argument fileName leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may 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.	5.4	More Details
CVE-2025-4406	The wpForo Forum plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.4.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	5.4	More Details
CVE-2025-49604	For Realtek AmebaD devices, a heap-based buffer overflow was discovered in Ameba-AIoT ameba-arduino-d before version 3.1.9 and ameba-rtos-d before commit c2bfd8216a1cbc19ad2ab5f48f372ecea756d67a on 2025/07/03. In the WLAN driver defragment function, lack of validation of the size of fragmented Wi-Fi frames may lead to a heap-based buffer overflow.	5.4	More Details
CVE-2025-52377	Command injection vulnerability in Nexxt Solutions NCM-X1800 Mesh Router versions UV1.2.7 and below, allowing authenticated attackers to execute arbitrary commands on the device. The vulnerability is present in the web management interface's ping and traceroute functionality, specifically in the /web/um_ping_set.cgi endpoint. The application fails to properly sanitize user input in the \`Ping_host_text\` parameter before passing it to the underlying system command, allowing attackers to inject and execute arbitrary shell commands as the root user.	5.4	More Details
CVE-2025-52378	Cross-Site Scripting (XSS) vulnerability in Nexxt Solutions NCM-X1800 Mesh Router firmware UV1.2.7 and below allowing attackers to inject JavaScript code that is executed in the context of administrator sessions when viewing the device management page via the DEVICE_ALIAS parameter to the /web/um_device_set_aliasname endpoint.	5.4	More Details
CVE-2025-7450	A vulnerability was found in letseeqiji gorobbs up to 1.0.8. It has been classified as critical. This affects the function ResetUserAvatar of the file controller/api/v1/user.go of the component API. The manipulation of the argument filename leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	5.4	More Details
CVE-2025-52985	A Use of Incorrect Operator vulnerability in the Routing Engine firewall of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to bypass security restrictions. When a firewall filter which is applied to the lo0 or re:mgmt interface references a prefix list with 'from prefix-list', and that prefix list contains more than 10 entries, the prefix list doesn't match and packets destined to or from the local device are not filtered. This issue affects firewall filters applied to the re:mgmt interfaces as input and output, but only affects firewall filters applied to the lo0 interface as output. This issue is applicable to IPv4 and IPv6 as a prefix list can contain IPv4 and IPv6 prefixes. This issue affects Junos OS Evolved: * 23.2R2-S3-EVO versions before 23.2R2-S4-EVO, * 23.4R2-S3-EVO versions before 23.4R2-S5-EVO, * 24.2R2-EVO versions before 24.2R2-S1-EVO, * 24.4-EVO versions before 24.4R1-S3-EVO, 24.4R2-EVO. This issue doesn't not affect Junos OS Evolved versions before 23.2R1-EVO.	5.3	More Details
CVE-2025-53667	Jenkins Dead Man's Snitch Plugin 0.1 does not mask Dead Man's Snitch tokens displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	5.3	More Details
CVE-2024-37524	IBM Analytics Content Hub 2.0, 2.1, 2.2, and 2.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser.	5.3	More Details
CVE-2025-53887	Directus is a real-time API and App dashboard for managing SQL database content. Starting in version 9.0.0 and prior to version 11.9.0, the exact Directus version number is incorrectly being used as OpenAPI Spec version this means that it is being exposed by the \`/server/specs/oas\` endpoint without authentication. With the exact version information a malicious attacker can look for known vulnerabilities in Directus core or any of its shipped dependencies in that specific running version. Version 11.9.0 fixes the issue.	5.3	More Details
CVE-2025-5241	Overly Restrictive Account Lockout Mechanism vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series allows a remote unauthenticated attacker to lockout legitimate users for a certain period by repeatedly attempting to login with incorrect passwords. The legitimate users will be unable to login until a certain period has passed after the lockout or until the product is reset.	5.3	More Details

CVE-2025-24294	The attack vector is a potential Denial of Service (DoS). The vulnerability is caused by an insufficient check on the length of a decompressed domain name within a DNS packet. An attacker can craft a malicious DNS packet containing a highly compressed domain name. When the resolv library parses such a packet, the name decompression process consumes a large amount of CPU resources, as the library does not limit the resulting length of the name. This resource consumption can cause the application thread to become unresponsive, resulting in a Denial of Service condition.	5.3	More Details
CVE-2025-50070	Vulnerability in the JDBC component of Oracle Database Server. Supported versions that are affected are 23.4-23.8. Difficult to exploit vulnerability allows low privileged attacker having Authenticated OS User privilege with logon to the infrastructure where JDBC executes to compromise JDBC. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JDBC, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all JDBC accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:N/A:N).	5.3	More Details
CVE-2025-24391	A vulnerability in the External Interface of OTRS allows conclusions to be drawn about the existence of user accounts through different HTTP response codes and messages. This enables an attacker to systematically identify valid email addresses. This issue affects: * OTRS 7.0.X * OTRS 8.0.X * OTRS 2023.X * OTRS 2024.X * OTRS 2025.X	5.3	More Details
CVE-2023-38327	An issue was discovered in eGroupWare 17.1.20190111. A User Enumeration vulnerability exists under calendar/freebusy.php, which allows unauthenticated remote attackers to enumerate the users of web applications based on server response.	5.3	More Details
CVE-2025-48924	Uncontrolled Recursion vulnerability in Apache Commons Lang. This issue affects Apache Commons Lang: Starting with commons-lang:commons-lang 2.0 to 2.6, and, from org.apache.commons:commons-lang3 3.0 before 3.18.0. The methods ClassUtils.getClass(...) can throw StackOverflowError on very long inputs. Because an Error is usually not handled by applications and libraries, a StackOverflowError could cause an application to stop. Users are recommended to upgrade to version 3.18.0, which fixes the issue.	5.3	More Details
CVE-2025-7572	A vulnerability classified as critical was found in LB-LINK BL-AC1900, BL-AC2100_AZ3, BL-AC3600, BL-AX1800, BL-AX5400P and BL-WR9000 up to 20250702. This vulnerability affects the function bs_GetHostInfo in the library libblinkapi.so of the file /cgi-bin/lighttpd.cgi. The manipulation leads to information disclosure. 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.	5.3	More Details
CVE-2025-52958	A Reachable Assertion vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent, unauthenticated attacker to cause a Denial of Service (DoS).On all Junos OS and Junos OS Evolved devices, when route validation is enabled, a rare condition during BGP initial session establishment can lead to an rpd crash and restart. This occurs specifically when the connection request fails during error-handling scenario. Continued session establishment failures leads to a sustained DoS condition. This issue affects Junos OS: * All versions before 22.2R3-S6, * from 22.4 before 22.4R3-S6, * from 23.2 before 23.2R2-S3, * from 23.4 before 23.4R2-S4, * from 24.2 before 24.2R2; Junos OS Evolved: * All versions before 22.2R3-S6-EVO, * from 22.4 before 22.4R3-S6-EVO, * from 23.2 before 23.2R2-S3-EVO, * from 23.4 before 23.4R2-S4-EVO, * from 24.2 before 24.2R2-EVO.	5.3	More Details
CVE-2025-32989	A heap-buffer-overread vulnerability was found in GnuTLS in how it handles the Certificate Transparency (CT) Signed Certificate Timestamp (SCT) extension during X.509 certificate parsing. This flaw allows a malicious user to create a certificate containing a malformed SCT extension (OID 1.3.6.1.4.1.11129.2.4.2) that contains sensitive data. This issue leads to the exposure of confidential information when GnuTLS verifies certificates from certain websites when the certificate (SCT) is not checked correctly.	5.3	More Details
CVE-2025-7565	A vulnerability, which was classified as critical, was found in LB-LINK BL-AC3600 up to 1.0.22. This affects the function geteasycfg of the file /cgi-bin/lighttpd.cgi of the component Web Management Interface. The manipulation of the argument Password leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-53364	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Starting in 5.3.0 and before 7.5.3 and 8.2.2, the Parse Server GraphQL API previously allowed public access to the GraphQL schema without requiring a session token or the master key. While schema introspection reveals only metadata and not actual data, this metadata can still expand the potential attack surface. This vulnerability is fixed in 7.5.3 and 8.2.2.	5.3	More Details
CVE-2025-53031	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.8, 8.0.8.5, 8.0.8.6, 8.1.1.4 and 8.1.2.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2025-30758	Vulnerability in the Siebel CRM End User product of Oracle Siebel CRM (component: User Interface). Supported versions that are affected are 25.0-25.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM End User. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Siebel CRM End User accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2025-6745	The WoodMart plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 8.2.5 via the woodmart_get_posts_by_query() function due to insufficient restrictions on which posts can be included. This makes it possible for unauthenticated attackers to extract data from password protected, private, or draft posts that they should not have access to.	5.3	More Details
CVE-2025-53674	Jenkins Sensedia Api Platform tools Plugin 1.0 does not mask the Sensedia API Manager integration token on the global configuration form, increasing the potential for attackers to observe and capture it.	5.3	More Details
CVE-2025-53677	Jenkins Xooa Plugin 0.0.7 and earlier does not mask the Xooa Deployment Token on the global configuration form, increasing the potential for attackers to observe and capture it.	5.3	More Details
CVE-2025-53743	Jenkins Applitools Eyes Plugin 1.16.5 and earlier does not mask Applitools API keys displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	5.3	More Details

CVE-2025-7545	A vulnerability classified as problematic was found in GNU Binutils 2.45. Affected by this vulnerability is the function copy_section of the file binutils/objcopy.c. The manipulation leads to heap-based buffer overflow. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The patch is named 08c3cbe5926e4d355b5cb70bbec2b1eeb40c2944. It is recommended to apply a patch to fix this issue.	5.3	More Details
CVE-2025-7573	A vulnerability, which was classified as critical, has been found in LB-LINK BL-AC1900, BL-AC2100_AZ3, BL-AC3600, BL-AX1800, BL-AX5400P and BL-WR9000 up to 20250702. This issue affects the function bs_GetManPwd in the library libblinkapi.so of the file /cgi-bin/lighttpd.cgi. The manipulation leads to information disclosure. The attack may 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.	5.3	More Details
CVE-2025-7546	A vulnerability, which was classified as problematic, has been found in GNU Binutils 2.45. Affected by this issue is the function bfd_elf_set_group_contents of the file bfd/elf.c. The manipulation leads to out-of-bounds write. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The name of the patch is 41461010eb7c79fee7a9d5f6209accdaac66cc6b. It is recommended to apply a patch to fix this issue.	5.3	More Details
CVE-2025-53655	Jenkins Statistics Gatherer Plugin 2.0.3 and earlier does not mask the AWS Secret Key on the global configuration form, increasing the potential for attackers to observe and capture it.	5.3	More Details
CVE-2025-7381	ImpactThis is an information disclosure vulnerability originating from PHP's base image. This vulnerability exposes the PHP version through an X-Powered-By header, which attackers could exploit to fingerprint the server and identify potential weaknesses. WorkaroundsThe mitigation requires changing the expose_php variable from "On" to "Off" in the file located at /usr/local/etc/php/php.ini.	5.3	More Details
CVE-2025-53622	DSpace open source software is a repository application which provides durable access to digital resources. Prior to versions 7.6.4, 8.2, and 9.1, a path traversal vulnerability is possible during the import of an archive (in Simple Archive Format), either from command-line (`./dspace import` command) or from the "Batch Import (Zip)" user interface feature. An attacker may craft a malicious Simple Archive Format (SAF) package where the `contents` file references any system files (using relative traversal sequences) which are readable by the Tomcat user. If such a package is imported, this will result in sensitive content disclose, including retrieving arbitrary files or configurations from the server where DSpace is running. The Simple Archive Format (SAF) importer / Batch Import (Zip) is only usable by site administrators (from user interface / REST API) or system administrators (from command-line). Therefore, to exploit this vulnerability, the malicious payload would have to be provided by an attacker and trusted by an administrator (who would trigger the import). The fix is included in DSpace 7.6.4, 8.2 and 9.1. For those who cannot upgrade immediately, it is possible to manually patch the DSpace backend. (No changes are necessary to the frontend.) A pull request exists which can be used to patch systems running DSpace 7.6.x, 8.x or 9.0. Although it is not possible to fully protect the system via workarounds, one may can apply a best practice. Administrators must carefully inspect any SAF archives (they did not construct themselves) before importing, paying close attention to the `contents` file to validate it does not reference files outside of the SAF archives.	5.2	More Details
CVE-2025-53471	Emerson ValveLink products receive input or data, but it do not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.	5.1	More Details
CVE-2025-52989	An Improper Neutralization of Delimiters vulnerability in the UI of Juniper Networks Junos OS and Junos OS Evolved allows a local, authenticated attacker with high privileges to modify the system configuration. A user with limited configuration and commit permissions, using a specifically crafted annotate configuration command, can change any part of the device configuration. This issue affects: Junos OS: * all versions before 22.2R3-S7, * 22.4 versions before 22.4R3-S7, * 23.2 versions before 23.2R2-S4, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R2-S1, * 24.4 versions before 24.4R1-S2, 24.4R2; Junos OS Evolved: * all versions before 22.4R3-S7-EVO, * 23.2-EVO versions before 23.2R2-S4-EVO, * 23.4-EVO versions before 23.4R2-S5-EVO, * 24.2-EVO versions before 24.2R2-S1-EVO * 24.4-EVO versions before 24.4R2-EVO.	5.1	More Details
CVE-2025-48496	Emerson ValveLink products use a fixed or controlled search path to find resources, but one or more locations in that path can be under the control of unintended actors.	5.1	More Details
CVE-2025-7578	A vulnerability was found in Teledyne FLIR FB-Series O and FLIR FH-Series ID 1.3.2.16. It has been declared as critical. This vulnerability affects the function sendCommand of the file runcmd.sh. The manipulation of the argument cmd leads to command injection. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The researcher highlights, that "[a]lthough this functionality is currently disabled due to server CGI configuration errors, it is essentially a 'time bomb' waiting to be activated". The vendor was contacted early about this disclosure but did not respond in any way.	5.0	More Details
CVE-2025-50079	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-50077	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-50080	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a	4.9	More Details

50091	hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).		
CVE-2025-50084	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-50086	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-50087	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N).	4.9	More Details
CVE-2025-50088	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-50089	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 9.0.0-9.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-52994	gif_outputAsJpeg in phpThumb through 1.7.23 allows phpthumb.gif.php OS Command Injection via a crafted parameter value. This is fixed in 1.7.23-202506081709.	4.9	More Details
CVE-2025-50092	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-50101	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-50093	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-50094	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.42, 8.4.5 and 9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-50095	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-50097	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-50102	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-50099	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:	4.9	More Details

	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).		
CVE-2025-7518	The RSFirewall! plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.1.42 via the get_local_filename() function. This makes it possible for authenticated attackers, with Administrator-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	4.9	More Details
CVE-2025-53023	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.0-8.0.42. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-53032	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 9.0.0-9.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-6236	The Hostel WordPress plugin before 1.1.5.9 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2025-30754	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	4.8	More Details
CVE-2025-53642	haxcms-nodejs and haxcms-php are backends for HAXcms. The logout function within the application does not terminate a user's session or clear their cookies. Additionally, the application issues a refresh token when logging out. This vulnerability is fixed in 11.0.6.	4.8	More Details
CVE-2025-50064	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N).	4.8	More Details
CVE-2025-7575	A vulnerability has been found in Zavy86 WikiDocs up to 1.0.77 and classified as critical. Affected by this vulnerability is the function image_drop_upload_ajax/image_delete_ajax of the file submit.php. The manipulation leads to path traversal. The attack can be launched remotely. Upgrading to version 1.0.78 is able to address this issue. The identifier of the patch is 98ea9ee4a2052c4327f89d2f7688cc1b5749450d. It is recommended to upgrade the affected component.	4.7	More Details
CVE-2025-7566	A vulnerability has been found in jshERP up to 3.5 and classified as critical. This vulnerability affects the function exportExcelByParam of the file /src/main/java/com/jsh/erp/controller/SystemConfigController.java. The manipulation of the argument Title leads to path traversal. 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.	4.7	More Details
CVE-2025-7553	A vulnerability classified as critical has been found in D-Link DIR-818LW up to 20191215. This affects an unknown part of the component System Time Page. The manipulation of the argument NTP Server leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	4.7	More Details
CVE-2025-53821	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. An Open Redirect vulnerability exists in the web application prior to version 3.4.5. The control.php endpoint allows to specify an arbitrary URL via the \`nextPage\` parameter, leading to an uncontrolled redirection. Version 3.4.5 contains a fix for the issue.	4.7	More Details
CVE-2025-7477	A vulnerability, which was classified as critical, has been found in code-projects Simple Car Rental System 1.0. This issue affects some unknown processing of the file /admin/add_cars.php. The manipulation of the argument image leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2025-31267	An authentication issue was addressed with improved state management. This issue is fixed in App Store Connect 3.0. An attacker with physical access to an unlocked device may be able to view sensitive user information.	4.6	More Details
CVE-2025-53886	Directus is a real-time API and App dashboard for managing SQL database content. Starting in version 9.0.0 and prior to version 11.9.0, when using Directus Flows with the WebHook trigger all incoming request details are logged including security sensitive data like access and refresh tokens in cookies. Malicious admins with access to the logs can hijack the user sessions within the token expiration time of them triggering the Flow. Version 11.9.0 fixes the issue.	4.5	More Details
CVE-2025-50096	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details

CVE-2025-50103	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 9.0.0-9.3.0. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2025-2942	The Order Delivery Date WordPress plugin before 12.6.0 discloses arbitrary post title (such as from draft and private posts) via an unauthenticated AJAX action, allowing attackers to retrieve such information	4.3	More Details
CVE-2025-53665	Jenkins Apica Loadtest Plugin 1.10 and earlier does not mask Apica Loadtest LTP authentication tokens displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	4.3	More Details
CVE-2025-53661	Jenkins Testsigma Test Plan run Plugin 1.6 and earlier does not mask Testsigma API keys displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	4.3	More Details
CVE-2025-53660	Jenkins QMetry Test Management Plugin 1.13 and earlier does not mask Qmetry Automation API Keys displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	4.3	More Details
CVE-2025-36599	Dell PowerFlex Manager VM, versions prior to 4.6.2.1, contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the system with privileges of the compromised account.	4.3	More Details
CVE-2025-53891	The timelineofficial/Time-Line- repository contains the source code for the TIME LINE website. A vulnerability was found in the TIME LINE website where uploaded files (instruction/message media) are not strictly validated for type and size. A user may upload renamed or oversized files that can disrupt performance or bypass restrictions. This could result in malicious file upload, denial of service, or client-side crashes. Version 1.0.5 contains a fix for the issue.	4.3	More Details
CVE-2025-30747	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 8.60, 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2025-7672	The improper default setting in JiranSoft CrossEditor4 on Windows, Linux, Unix (API modules) potentaily allows Stored XSS. This issue affects CrossEditor4: from 4.0.0.01 before 4.6.0.23.	4.3	More Details
CVE-2025-7579	A vulnerability was found in chinese-poetry 0.1. It has been rated as problematic. This issue affects some unknown processing of the file rank/server.js. The manipulation leads to inefficient regular expression complexity. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-53657	Jenkins ReadyAPI Functional Testing Plugin 1.11 and earlier does not mask SLM License Access Keys, client secrets, and passwords displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	4.3	More Details
CVE-2025-7625	A vulnerability, which was classified as critical, was found in YiJiuSmile kkFileViewOfficeEdit up to 5fbc57c48e8fe6c1b91e0e7995e2d59615f37abd. Affected is the function Download of the file /download. The manipulation of the argument url leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	4.3	More Details
CVE-2025-53653	Jenkins Aqua Security Scanner Plugin 3.2.8 and earlier stores Scanner Tokens for Aqua API unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	4.3	More Details
CVE-2025-7626	A vulnerability has been found in YiJiuSmile kkFileViewOfficeEdit up to 5fbc57c48e8fe6c1b91e0e7995e2d59615f37abd and classified as critical. Affected by this vulnerability is the function onlinePreview of the file /onlinePreview. The manipulation of the argument url leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	4.3	More Details
CVE-2025-2670	IBM OpenPages 9.0 is vulnerable to information disclosure of sensitive information due to a weaker than expected security for certain REST end points related to workflow feature of OpenPages. An authenticated user is able to obtain certain information about Workflow related configuration and internal state.	4.3	More Details
CVE-2025-29606	py-libp2p before 0.2.3 allows a peer to cause a denial of service (resource consumption) via a large RSA key.	4.3	More Details
CVE-2025-44003	Missing Release of Resource after Effective Lifetime (CWE-772) in the Gallagher T-Series Reader allows an attacker with physical access to the reader to perform a limited denial of service when 125 kHz Card Technology is enabled. This issue affects T-Series Readers: 9.20 prior to vCR9.20.250213a (distributed in 9.20.1827 (MR2)), 9.10 prior to vCR9.10.250213a (distributed in 9.10.2692(MR5)), 9.00 prior to vCR9.00.250619a (distributed in vEL9.00.3371 (MR7)), all versions of 8.90 and prior.	4.3	More Details
CVE-2025-1112	IBM OpenPages with Watson 8.3 and 9.0 could allow an authenticated user to obtain sensitive information that should only be available to privileged users.	4.3	More Details
CVE-	A vulnerability was found in ShopXO up to 6.5.0 and classified as problematic. This issue affects some unknown processing of the		

2025-7567	file header.html. The manipulation of the argument lang/system_type leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-53669	Jenkins VAddy Plugin 1.2.8 and earlier does not mask Vaddy API Auth Keys displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	4.3	More Details
CVE-2025-46704	A vulnerability exists in Advantech iView in NetworkServlet.processImportRequest() that could allow for a directory traversal attack. This issue requires an authenticated attacker with at least user-level privileges. A specific parameter is not properly sanitized or normalized, potentially allowing an attacker to determine the existence of arbitrary files on the server.	4.3	More Details
CVE-2025-7462	A vulnerability was found in Artifex GhostPDL up to 3989415a5b8e99b9d1b87cc9902bde9b7cdea145. It has been classified as problematic. This affects the function pdf_ferror of the file devices/vector/gdevpdf.c of the component New Output File Open Error Handler. The manipulation leads to null pointer dereference. It is possible to initiate the attack remotely. The identifier of the patch is 619a106ba4c4abed95110f84d5efcd7aee38c7cb. It is recommended to apply a patch to fix this issue.	4.3	More Details
CVE-2025-47813	loginok.html in Wing FTP Server before 7.4.4 discloses the full local installation path of the application when using a long value in the UID cookie.	4.3	More Details
CVE-2025-24798	Meshtastic is an open source mesh networking solution. From 1.2.1 until 2.6.2, a packet sent to the routing module that contains want_response==true causes a crash. This can lead to a degradation of service for nodes within range of a malicious sender, or via MQTT if downlink is enabled. This vulnerability is fixed in 2.6.2.	4.3	More Details
CVE-2025-7488	A vulnerability has been found in JoeyBling SpringBoot_MyBatisPlus up to a6a825513bd688f717dbae3a196bc9c9622fea26 and classified as critical. This vulnerability affects the function Download of the file /file/download. The manipulation of the argument Name leads to path traversal. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	4.3	More Details
CVE-2025-36090	IBM Analytics Content Hub 2.0, 2.1, 2.2, and 2.3 could allow a remote attacker to obtain information about the application framework which could be used in reconnaissance to gather information for future attacks from a detailed technical error message.	4.3	More Details
CVE-2025-3396	An issue has been discovered in GitLab EE affecting all versions from 13.3 before 17.11.6, 18.0 before 18.0.4, and 18.1 before 18.1.2 that could have allowed authenticated project owners to bypass group-level forking restrictions by manipulating API requests.	4.3	More Details
CVE-2025-24477	A heap-based buffer overflow in Fortinet FortiOS versions 7.6.0 through 7.6.2, 7.4.0 through 7.4.7, 7.2.4 through 7.2.11 allows an attacker to escalate its privileges via a specially crafted CLI command	4.2	More Details
CVE-2025-53885	Directus is a real-time API and App dashboard for managing SQL database content. Starting in version 9.0.0 and prior to version 11.9.0, when using Directus Flows to handle CRUD events for users it is possible to log the incoming data to console using the "Log to Console" operation and a template string. Malicious admins can log sensitive data from other users when they are created or updated. Version 11.9.0 contains a fix for the issue. As a workaround, avoid logging sensitive data to the console outside the context of development.	4.2	More Details
CVE-2025-45582	GNU Tar through 1.35 allows file overwrite via directory traversal in crafted TAR archives, with a certain two-step process. First, the victim must extract an archive that contains a ../ symlink to a critical directory. Second, the victim must extract an archive that contains a critical file, specified via a relative pathname that begins with the symlink name and ends with that critical file's name. Here, the extraction follows the symlink and overwrites the critical file. This bypasses the protection mechanism of "Member name contains '..'" that would occur for a single TAR archive that attempted to specify the critical file via a ../ approach. For example, the first archive can contain "x -> ../../../../../home/victim/.ssh" and the second archive can contain x/authorized_keys. This can affect server applications that automatically extract any number of user-supplied TAR archives, and were relying on the blocking of traversal. This can also affect software installation processes in which "tar xf" is run more than once (e.g., when installing a package can automatically install two dependencies that are set up as untrusted tarballs instead of official packages).	4.1	More Details
CVE-2025-53905	Vim is an open source, command line text editor. Prior to version 9.1.1552, a path traversal issue in Vim’s tar.vim plugin can allow overwriting of arbitrary files when opening specially crafted tar archives. Impact is low because this exploit requires direct user interaction. However, successfully exploitation can lead to overwriting sensitive files or placing executable code in privileged locations, depending on the permissions of the process editing the archive. The victim must edit such a file using Vim which will reveal the filename and the file content, a careful user may suspect some strange things going on. Successful exploitation could results in the ability to execute arbitrary commands on the underlying operating system. Version 9.1.1552 contains a patch for the vulnerability.	4.1	More Details
CVE-2025-53906	Vim is an open source, command line text editor. Prior to version 9.1.1551, a path traversal issue in Vim’s zip.vim plugin can allow overwriting of arbitrary files when opening specially crafted zip archives. Impact is low because this exploit requires direct user interaction. However, successfully exploitation can lead to overwriting sensitive files or placing executable code in privileged locations, depending on the permissions of the process editing the archive. The victim must edit such a file using Vim which will reveal the filename and the file content, a careful user may suspect some strange things going on. Successful exploitation could results in the ability to execute arbitrary commands on the underlying operating system. Version 9.1.1551 contains a patch for the vulnerability.	4.1	More Details
CVE-2025-27027	A user with vpuser credentials that opens an SSH connection to the device, gets a restricted shell rbash that allows only a small list of allowed commands. This vulnerability enables the user to get a full-featured Linux shell, bypassing the rbash restrictions.	4.1	More Details
CVE-2025-53637	Meshtastic is an open source mesh networking solution. The main_matrix.yml GitHub Action is triggered by the pull_request_target event, which has extensive permissions, and can be initiated by an attacker who forked the repository and created a pull request. In the shell code execution part, user-controlled input is interpolated unsafely into the code. If this were to be exploited, attackers could inject unauthorized code into the repository. This vulnerability is fixed in 2.6.6.	4.1	More Details

CVE-2025-52357	Cross-Site Scripting (XSS) vulnerability exists in the ping diagnostic feature of FiberHome FD602GW-DX-R410 router (firmware V2.2.14), allowing an authenticated attacker to execute arbitrary JavaScript code in the context of the router s web interface. The vulnerability is triggered via user-supplied input in the ping form field, which fails to sanitize special characters. This can be exploited to hijack sessions or escalate privileges through social engineering or browser-based attacks.	4.1	More Details
CVE-2025-47811	In Wing FTP Server through 7.4.4, the administrative web interface (listening by default on port 5466) runs as root or SYSTEM by default. The web application itself offers several legitimate ways to execute arbitrary system commands (i.e., through the web console or the task scheduler), and they are automatically executed in the highest possible privilege context. Because administrative users of the web interface are not necessarily also system administrators, one might argue that this is a privilege escalation. (If a privileged application role is not available to an attacker, CVE-2025-47812 can be leveraged.) NOTE: the vendor reportedly considers this behavior "fine to keep."	4.1	More Details
CVE-2025-6838	The Broken Link Notifier plugin for WordPress is vulnerable to CSV Injection in all versions up to, and including, 1.3.0 via broken links that are later exported. This makes it possible for authenticated attackers, with Contributor-level access and above, 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.	4.1	More Details
CVE-2025-50072	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle WebLogic Server executes to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 4.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	4.0	More Details
CVE-2025-53839	DRACOON is a file sharing service, and the DRACOON Branding Service allows customers to customize their DRACOON interface with their brand. Versions of the DRACOON Branding Service prior to 2.10.0 are vulnerable to cross-site scripting. Improper neutralization of input from administrative users could inject HTML code into the workflow for newly onboarded users. A fix was made available in version 2.10.0 and rolled out to the DRACOON service. DRACOON customers do not need to take action.	4.0	More Details
CVE-2025-7464	A vulnerability classified as problematic has been found in osrg GoBGP up to 3.37.0. Affected is the function SplitRTR of the file pkg/packet/rtr/rtr.go. The manipulation leads to out-of-bounds read. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The name of the patch is e748f43496d74946d14fed85c776452e47b99d64. It is recommended to apply a patch to fix this issue.	3.7	More Details
CVE-2025-7577	A vulnerability was found in Teledyne FLIR FB-Series O and FLIR FH-Series ID 1.3.2.16. It has been classified as problematic. This affects an unknown part. The manipulation leads to use of hard-coded password. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2025-53014	ImageMagick is free and open-source software used for editing and manipulating digital images. Versions prior to 7.1.2-0 and 6.9.13-26 have a heap buffer overflow in the `InterpretImageFilename` function. The issue stems from an off-by-one error that causes out-of-bounds memory access when processing format strings containing consecutive percent signs (`%%`). Versions 7.1.2-0 and 6.9.13-26 fix the issue.	3.7	More Details
CVE-2025-30752	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). The supported version that is affected is Oracle Java SE: 24.0.1; Oracle GraalVM for JDK: 24.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details
CVE-2025-7453	A vulnerability was found in saltbo zpan up to 1.6.5/1.7.0-beta2. It has been rated as problematic. This issue affects the function NewToken of the file zpan/internal/app/service/token.go of the component JSON Web Token Handler. The manipulation with the input 123 leads to use of hard-coded password. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used.	3.7	More Details
CVE-2025-1220	In PHP versions:8.1.* before 8.1.33, 8.2.* before 8.2.29, 8.3.* before 8.3.23, 8.4.* before 8.4.10 some functions like fsockopen() lack validation that the hostname supplied does not contain null characters. This may lead to other functions like parse_url() treat the hostname in different way, thus opening way to security problems if the user code implements access checks before access using such functions.	3.7	More Details
CVE-2025-53019	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions prior to 7.1.2-0 and 6.9.13-26, in ImageMagick's `magick stream` command, specifying multiple consecutive `%d` format specifiers in a filename template causes a memory leak. Versions 7.1.2-0 and 6.9.13-26 fix the issue.	3.7	More Details
CVE-2025-50065	Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Native Image). The supported version that is affected is Oracle GraalVM for JDK: 24.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle GraalVM for JDK. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details
CVE-2025-27613	Gitk is a Tcl/Tk based Git history browser. Starting with 1.7.0, when a user clones an untrusted repository and runs gitk without additional command arguments, files for which the user has write permission can be created and truncated. The option Support per-file encoding must have been enabled before in Gitk's Preferences. This option is disabled by default. The same happens when Show origin of this line is used in the main window (regardless of whether Support per-file encoding is enabled or not). This vulnerability is fixed in 2.43.7, 2.44.4, 2.45.4, 2.46.4, 2.47.3, 2.48.2, 2.49.1, and 2.50.1.	3.6	More Details
CVE-2025-	A vulnerability was found in LiveHelperChat lhc-php-resque Extension up to ee1270b35625f552425e32a6a3061cd54b5085c4. It has been classified as problematic. This affects an unknown part of the file /site_admin/lhcphpresque/list/ of the component List Handler. The manipulation of the argument queue name 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. This product takes the approach of rolling releases to provide continious delivery.	3.5	More Details

7435	Therefore, version details for affected and updated releases are not available. The identifier of the patch is 542aa8449b5aa889b3a54f419e794afe19f56d5d/0ce7b4f1193c0ed6c6e31a960fafededf979eef2. It is recommended to apply a patch to fix this issue.		
CVE-2025-7408	A vulnerability has been found in SourceCodester Zoo Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/templates/animal_form_template.php. The manipulation of the argument msg leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7601	A vulnerability has been found in PHPGurukul Online Library Management System 3.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/student-history.php. The manipulation of the argument stdid leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-49462	Cross-site scripting in certain Zoom Clients before version 6.4.5 may allow an authenticated user to conduct a disclosure of information via network access.	3.5	More Details
CVE-2025-53862	A flaw was found in Ansible. Three API endpoints are accessible and return verbose, unauthenticated responses. This flaw allows a malicious user to access data that may contain important information.	3.5	More Details
CVE-2023-50458	In Dradis before 4.11.0, the Output Console shows a job queue that may contain information about other users' jobs.	3.5	More Details
CVE-2025-7569	A vulnerability was found in Bigotry OneBase up to 1.3.6. It has been declared as problematic. Affected by this vulnerability is the function parse_args of the file /tpl/think_exception.tpl. The manipulation of the argument args leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-27889	Wing FTP Server before 7.4.4 does not properly validate and sanitize the url parameter of the downloadpass.html endpoint, allowing injection of an arbitrary link. If a user clicks a crafted link, this discloses a cleartext password to the attacker.	3.4	More Details
CVE-2025-7485	A vulnerability classified as problematic was found in Open5GS up to 2.7.3. Affected by this vulnerability is the function ngap_recv_handler/s1ap_recv_handler/recv_handler of the component SCTP Partial Message Handler. The manipulation leads to reachable assertion. The attack needs to be approached locally. The patch is named cfa44575020f3fb045fd971358442053c8684d3d. It is recommended to apply a patch to fix this issue.	3.3	More Details
CVE-2025-7207	A vulnerability, which was classified as problematic, was found in mruby up to 3.4.0-rc2. Affected is the function scope_new of the file mrbgems/mruby-compiler/core/codegen.c of the component nregs Handler. The manipulation leads to heap-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The name of the patch is 1fdd96104180cc0fb5d3cb086b05ab6458911bb9. It is recommended to apply a patch to fix this issue.	3.3	More Details
CVE-2025-7209	A vulnerability has been found in 9fans plan9port up to 9da5b44 and classified as problematic. Affected by this vulnerability is the function value_decode in the library src/libsec/port/x509.c. The manipulation leads to null pointer dereference. Local access is required to approach this attack. The exploit has been disclosed to the public and may 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 identifier of the patch is deae8939583d83fd798fca97665e0e94656c3ee8. It is recommended to apply a patch to fix this issue.	3.3	More Details
CVE-2025-53861	A flaw was found in Ansible. Sensitive cookies without security flags over non-encrypted channels can lead to Man-in-the-Middle (MitM) and Cross-site scripting (XSS) attacks allowing attackers to read transmitted data.	3.1	More Details
CVE-2025-50081	Vulnerability in the MySQL Client product of Oracle MySQL (component: Client: mysqldump). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Client accessible data as well as unauthorized read access to a subset of MySQL Client accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N).	3.1	More Details
CVE-2025-50066	Vulnerability in the Oracle Database Materialized View component of Oracle Database Server. Supported versions that are affected are 19.3-19.27, 21.3-21.18 and 23.4-23.8. Easily exploitable vulnerability allows high privileged attacker having Execute on DBMS_REDEFINITION privilege with network access via Oracle Net to compromise Oracle Database Materialized View. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database Materialized View accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2.7	More Details
CVE-2025-50104	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.7	More Details
CVE-2025-4972	An issue has been discovered in GitLab EE affecting all versions from 18.0 before 18.0.4 and 18.1 before 18.1.2 that could have allowed authenticated users with invitation privileges to bypass group-level user invitation restrictions by manipulating group invitation functionality.	2.7	More Details
CVE-2025-6168	An issue has been discovered in GitLab EE affecting all versions from 18.0 before 18.0.4 and 18.1 before 18.1.2 that could have allowed authenticated maintainers to bypass group-level user invitation restrictions by sending crafted API requests.	2.7	More Details
CVE-2025-50098	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector:	2.7	More Details

	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).		
CVE-2025-7554	A vulnerability classified as problematic was found in Sapido RB-1802 1.0.32. This vulnerability affects unknown code of the file urlfilter.asp of the component URL Filtering Page. The manipulation of the argument URL address leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2025-30750	Vulnerability in the Unified Audit component of Oracle Database Server. Supported versions that are affected are 19.3-19.27, 21.3-21.18 and 23.4-23.8. Easily exploitable vulnerability allows high privileged attacker having Create User privilege with network access via Oracle Net to compromise Unified Audit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Unified Audit accessible data. CVSS 3.1 Base Score 2.4 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N).	2.4	More Details
CVE-2025-53029	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 2.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2.3	More Details
CVE-2025-50100	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.2	More Details
CVE-2025-7214	A vulnerability classified as problematic was found in FNKvision FNK-GU2 up to 40.1.7. Affected by this vulnerability is an unknown functionality of the file /etc/shadow of the component MD5. The manipulation leads to risky cryptographic algorithm. It is possible to launch the attack on the physical device. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used.	1.6	More Details
CVE-2025-7215	A vulnerability, which was classified as problematic, has been found in FNKvision FNK-GU2 up to 40.1.7. Affected by this issue is some unknown functionality of the file /rom/wpa_supplicant.conf. The manipulation leads to cleartext storage of sensitive information. It is possible to launch the attack on the physical device. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used.	1.6	More Details
CVE-2025-34103	An unauthenticated command injection vulnerability exists in WePresent WiPG-1000 firmware versions prior to 2.2.3.0, due to improper input handling in the undocumented /cgi-bin/rdfs.cgi endpoint. The Client parameter is not sanitized before being passed to a system call, allowing an unauthenticated remote attacker to execute arbitrary commands as the web server user.	N/A	More Details
CVE-2025-34068	An unauthenticated remote command execution vulnerability exists in Samsung WLAN AP WEA453e firmware prior to version 5.2.4.T1 via improper input validation in the “Tech Support” diagnostic functionality. The command1 and command2 POST or GET parameters accept arbitrary shell commands that are executed with root privileges on the underlying operating system. An attacker can exploit this by crafting a request that injects shell commands to create output files in writable directories and then access their contents via the download endpoint. This flaw allows complete compromise of the device without authentication.	N/A	More Details
CVE-2025-6965	There exists a vulnerability in SQLite versions before 3.50.2 where the number of aggregate terms could exceed the number of columns available. This could lead to a memory corruption issue. We recommend upgrading to version 3.50.2 or above.	N/A	More Details
CVE-2025-34110	A directory traversal vulnerability exists in ColoradoFTP Server ≤ 1.3 Build 8 for Windows, allowing unauthenticated attackers to read or write arbitrary files outside the configured FTP root directory. The flaw is due to insufficient sanitation of user-supplied file paths in the FTP GET and PUT command handlers. Exploitation is possible by submitting traversal sequences during FTP operations, enabling access to system-sensitive files. This issue affects only the Windows version of ColoradoFTP.	N/A	More Details
CVE-2025-53620	@builder.io/qwik-city is the meta-framework for Qwik. When a Qwik Server Action QRL is executed it dynamically load the file containing the symbol. When an invalid qfunc is sent, the server does not handle the thrown error. The error then causes Node JS to exit. This vulnerability is fixed in 1.13.0.	N/A	More Details
CVE-2025-34111	An unauthenticated arbitrary file upload vulnerability exists in Tiki Wiki CMS Groupware version 15.1 and earlier via the ELFinder component's default connector (connector.minimal.php), which allows remote attackers to upload and execute malicious PHP scripts in the context of the web server. The vulnerable component does not enforce file type validation, allowing attackers to craft a POST request to upload executable PHP payloads through the ELFinder interface exposed at /vendor_extra/elfinder/.	N/A	More Details
CVE-2025-34112	An authenticated multi-stage remote code execution vulnerability exists in Riverbed SteelCentral NetProfiler and NetExpress 10.8.7 virtual appliances. A SQL injection vulnerability in the '/api/common/1.0/login' endpoint can be exploited to create a new user account in the appliance database. This user can then trigger a command injection vulnerability in the '/index.php?page=licenses' endpoint to execute arbitrary commands. The attacker may escalate privileges to root by exploiting an insecure sudoers configuration that allows the 'mazu' user to execute arbitrary commands as root via SSH key extraction and command chaining. Successful exploitation allows full remote root access to the virtual appliance.	N/A	More Details
CVE-2024-10391	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-53818	GitHub Kanban MCP Server is a Model Context Protocol (MCP) server for managing GitHub issues in Kanban board format and streamlining LLM task management. Version 0.3.0 of the MCP Server is written in a way that is vulnerable to command injection vulnerability attacks as part of some of its MCP Server tool definition and implementation. The MCP Server exposes the tool \`add_comment\` which relies on Node.js child process API \`exec\` to execute the GitHub (\`gh\`) command, is an unsafe and vulnerable API if concatenated with untrusted user input. As of time of publication, no known patches are available.	N/A	More Details
CVE-2025-34113	An authenticated command injection vulnerability exists in Tiki Wiki CMS versions ≤14.1, ≤12.4 LTS, ≤9.10 LTS, and ≤6.14 via the \`viewmode\` GET parameter in \`tiki-calendar.php\`. When the calendar module is enabled and an authenticated user has permission to access it, an attacker can inject and execute arbitrary PHP code. Successful exploitation leads to remote code execution in the context of the web server user.	N/A	More Details

CVE-2025-0140	An incorrect privilege assignment vulnerability in the Palo Alto Networks GlobalProtect™ App on macOS and Linux devices enables a locally authenticated non administrative user to disable the app even if the GlobalProtect app configuration would not normally permit them to do so. The GlobalProtect app on Windows, iOS, Android, Chrome OS and GlobalProtect UWP app are not affected.	N/A	More Details
CVE-2025-34107	A buffer overflow vulnerability exists in the WinaXe FTP Client version 7.7 within the FTP banner parsing functionality, WCMDPA10.dll. When the client connects to a remote FTP server and receives an overly long '220 Server Ready' response, the vulnerable component responsible for parsing the banner overflows a stack buffer, leading to arbitrary code execution under the context of the user.	N/A	More Details
CVE-2025-34115	An authenticated command injection vulnerability exists in OP5 Monitor through version 7.1.9 via the 'cmd_str' parameter in the command_test.php endpoint. A user with access to the web interface can exploit the 'Test this command' feature to execute arbitrary shell commands as the unprivileged web application user. The vulnerability resides in the configuration section of the application and requires valid login credentials with access to the command testing functionality. This issue is fixed in version 7.2.0.	N/A	More Details
CVE-2025-0139	An incorrect privilege assignment vulnerability in Palo Alto Networks Autonomous Digital Experience Manager allows a locally authenticated low privileged user on macOS endpoints to escalate their privileges to root.	N/A	More Details
CVE-2025-34106	A buffer overflow vulnerability exists in PDF Shaper versions 3.5 and 3.6 when converting a crafted PDF file to an image using the 'Convert PDF to Image' functionality. An attacker can exploit this vulnerability by tricking a user into opening a maliciously crafted PDF file, leading to arbitrary code execution under the context of the user. This vulnerability has been verified on Windows XP, 7, 8, and 10 platforms using the PDFTools.exe component.	N/A	More Details
CVE-2025-34105	A stack-based buffer overflow vulnerability exists in the built-in web interface of DiskBoss Enterprise versions 7.4.28, 7.5.12, and 8.2.14. The vulnerability arises from improper bounds checking on the path component of HTTP GET requests. By sending a specially crafted long URI, a remote unauthenticated attacker can trigger a buffer overflow, potentially leading to arbitrary code execution with SYSTEM privileges on vulnerable Windows hosts.	N/A	More Details
CVE-2025-34116	A remote command execution vulnerability exists in IPFire before version 2.19 Core Update 101 via the 'proxy.cgi' CGI interface. An authenticated attacker can inject arbitrary shell commands through crafted values in the NCSA user creation form fields, leading to command execution with web server privileges.	N/A	More Details
CVE-2025-34109	PSEvents.exe in multiple Panda Security products runs hourly with SYSTEM privileges and loads DLL files from a user-writable directory without proper validation. An attacker with low-privileged access who can write DLL files to the monitored directory can achieve arbitrary code execution with SYSTEM privileges. Affected products include Panda Global Protection 2016, Panda Antivirus Pro 2016, Panda Small Business Protection, and Panda Internet Security 2016 (all versions up to 16.1.2).	N/A	More Details
CVE-2025-34104	An authenticated remote code execution vulnerability exists in Piwik (now Matomo) versions prior to 3.0.3 via the plugin upload mechanism. In vulnerable versions, an authenticated user with Superuser privileges can upload and activate a malicious plugin (ZIP archive), leading to arbitrary PHP code execution on the underlying system. Starting with version 3.0.3, plugin upload functionality is disabled by default unless explicitly enabled in the configuration file.	N/A	More Details
CVE-2025-34108	A stack-based buffer overflow vulnerability exists in the login functionality of Disk Pulse Enterprise version 9.0.34. An attacker can send a specially crafted HTTP POST request to the /login endpoint with an overly long username parameter, causing a buffer overflow in the libspp.dll component. Successful exploitation allows arbitrary code execution with SYSTEM privileges.	N/A	More Details
CVE-2025-49827	Conjur provides secrets management and application identity for infrastructure. Conjur OSS versions 1.19.5 through 1.22.0 and Secrets Manager, Self-Hosted (formerly known as Conjur Enterprise) 13.1 through 13.5 and 13.6 are vulnerable to bypass of the IAM authenticator. An attacker who can manipulate the headers signed by AWS can take advantage of a malformed regular expression to redirect the authentication validation request that Secrets Manager, Self-Hosted sends to AWS to a malicious server controlled by the attacker. This redirection could result in a bypass of the Secrets Manager, Self-Hosted IAM Authenticator, granting the attacker the permissions granted to the client whose request was manipulated. This issue affects both Secrets Manager, Self-Hosted (formerly Conjur Enterprise) and Conjur OSS. Conjur OSS version 1.22.1 and Secrets Manager, Self-Hosted versions 13.5.1 and 13.6.1 fix the issue.	N/A	More Details
CVE-2025-38264	In the Linux kernel, the following vulnerability has been resolved: nvme-tcp: sanitize request list handling Validate the request in nvme_tcp_handle_r2t() to ensure it's not part of any list, otherwise a malicious R2T PDU might inject a loop in request list processing.	N/A	More Details
CVE-2025-38243	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix invalid inode pointer dereferences during log replay In a few places where we call read_one_inode(), if we get a NULL pointer we end up jumping into an error path, or fallthrough in case of __add_inode_ref(), where we then do something like this: iput(&inode->vfs_inode); which results in an invalid inode pointer that triggers an invalid memory access, resulting in a crash. Fix this by making sure we don't do such dereferences.	N/A	More Details
CVE-2025-38241	In the Linux kernel, the following vulnerability has been resolved: mm/shmem, swap: fix softlockup with mTHP swapin Following softlockup can be easily reproduced on my test machine with: echo always > /sys/kernel/mm/transparent_hugepage/hugepages-64kB/enabled swapon /dev/zram0 # zram0 is a 48G swap device mkdir -p /sys/fs/cgroup/memory/test echo 1G > /sys/fs/cgroup/test/memory.max echo $BASHPID > /sys/fs/cgroup/test/cgroup.procs while true; do dd if=/dev/zero of=/tmp/test.img bs=1M count=5120 cat /tmp/test.img > /dev/null rm /tmp/test.img done Then after a while: watchdog: BUG: soft lockup - CPU#0 stuck for 763s! [cat:5787] Modules linked in: zram virtiofs CPU: 0 UID: 0 PID: 5787 Comm: cat Kdump: loaded Tainted: G L 6.15.0.orig-gf3021d9246bc-dirty #118 PREEMPT(voluntary)· Tainted: [L]=SOFTLOCKUP Hardware name: Red Hat KVM/RHEL-AV, BIOS 0.0.0 02/06/2015 RIP: 0010:mpol_shared_policy_lookup+0xd/0x70 Code: e9 b8 b4 ff ff 31 c0 c3 cc cc cc cc 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 66 0f 1f 00 0f 1f 44 00 00 41 54 55 53 <48> 8b 1f 48 85 db 74 41 4c 8d 67 08 48 89 fb 48 89 f5 4c 89 e7 e8 RSP: 0018:ffffc90002b1fc28 EFLAGS: 00000202 RAX: 00000000001c20ca RBX: 0000000000724e1e RCX: 0000000000000001 RDX: ffff888118e214c8 RSI: 0000000000057d42 RDI: ffff888118e21518 RBP: 000000000002bec8 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000000000bf4 R11: 0000000000000000 R12: 0000000000000001 R13: 00000000001c20ca R14: 00000000001c20ca R15: 0000000000000000 FS: 00007f03f995c740(0000) GS:ffff88a07ad9a000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f03f98f1000 CR3: 0000000144626004 CR4: 0000000000770eb0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> shmem_alloc_folio+0x31/0xc0 shmem_swapin_folio+0x309/0xcf0 ? filemap_get_entry+0x117/0x1e0 ? xas_load+0xd/0xb0 ? filemap_get_entry+0x101/0x1e0 shmem_get_folio_gfp+0x2ed/0x5b0 shmem_file_read_iter+0x7f/0x2e0 vfs_read+0x252/0x330 ksys_read+0x68/0xf0 do_syscall_64+0x4c/0x1c0 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7f03f9a46991 Code: 00 48 8b 15 81 14 10 00 f7 d8 64 89 02 b8 ff ff ff ff eb bd e8 20 ad 01 00 f3 0f 1e fa 80 3d 35 97 10 00 00 74 13 31 c0 0f 05 <48> 3d 00 f0 ff ff 77 4f c3 66	N/A	More Details

	0f 1f 44 00 00 55 48 89 e5 48 83 ec RSP: 002b:00007fff3c52bd28 EFLAGS: 00000246 ORIG_RAX: 0000000000000000 RAX: ffffffffffffffda RBX: 0000000000040000 RCX: 00007f03f9a46991 RDX: 0000000000040000 RSI: 00007f03f98ba000 RDI: 0000000000000003 RBP: 00007fff3c52bd50 R08: 0000000000000000 R09: 00007f03f9b9a380 R10: 0000000000000022 R11: 0000000000000246 R12: 0000000000040000 R13: 00007f03f98ba000 R14: 0000000000000003 R15: 0000000000000000 </TASK> The reason is simple, readahead brought some order 0 folio in swap cache, and the swapin mTHP folio being allocated is in conflict with it, so swapcache_prepare fails and causes shmem_swap_alloc_folio to return -EEXIST, and shmem simply retries again and again causing this loop. Fix it by applying a similar fix for anon mTHP swapin. The performance change is very slight, time of swapin 10g zero folios with shmem (test for 12 times): Before: 2.47s After: 2.48s [kasong@tencent.com: add comment]		
CVE-2025-38239	In the Linux kernel, the following vulnerability has been resolved: scsi: megaraid_sas: Fix invalid node index On a system with DRAM interleave enabled, out-of-bound access is detected: megaraid_sas 0000:3f:00.0: requested/available msix 128/128 poll_queue 0 ------------[cut here]------------ UBSAN: array-index-out-of-bounds in ./arch/x86/include/asm/topology.h:72:28 index -1 is out of range for type 'cpumask *[1024]' dump_stack_lvl+0x5d/0x80 ubsan_epilogue+0x5/0x2b __ubsan_handle_out_of_bounds.cold+0x46/0x4b megasas_alloc_irq_vectors+0x149/0x190 [megaraid_sas] megasas_probe_one.cold+0xa4d/0x189c [megaraid_sas] local_pci_probe+0x42/0x90 pci_device_probe+0xdc/0x290 really_probe+0xdb/0x340 __driver_probe_device+0x78/0x110 driver_probe_device+0x1f/0xa0 __driver_attach+0xba/0x1c0 bus_for_each_dev+0x8b/0xe0 bus_add_driver+0x142/0x220 driver_register+0x72/0xd0 megasas_init+0xdf/0xff0 [megaraid_sas] do_one_initcall+0x57/0x310 do_init_module+0x90/0x250 init_module_from_file+0x85/0xc0 idempotent_init_module+0x114/0x310 __x64_sys_finit_module+0x65/0xc0 do_syscall_64+0x82/0x170 entry_SYSCALL_64_after_hwframe+0x76/0x7e Fix it accordingly.	N/A	More Details
CVE-2025-38238	In the Linux kernel, the following vulnerability has been resolved: scsi: fnic: Fix crash in fnic_wq_cmpl_handler when FDMI times out When both the RHBA and RPA FDMI requests time out, fnic reuses a frame to send ABTS for each of them. On send completion, this causes an attempt to free the same frame twice that leads to a crash. Fix crash by allocating separate frames for RHBA and RPA, and modify ABTS logic accordingly. Tested by checking MDS for FDMI information. Tested by using instrumented driver to: - Drop PLOGI response - Drop RHBA response - Drop RPA response - Drop RHBA and RPA response - Drop PLOGI response + ABTS response - Drop RHBA response + ABTS response - Drop RPA response + ABTS response - Drop RHBA and RPA response + ABTS response for both of them	N/A	More Details
CVE-2025-7379	A security bypass vulnerability allows exploitation via Reverse Tabnabbing, a type of phishing attack where attackers can manipulate the content of the original tab, leading to credential theft and other security risks. This issue affects DataSync Center: from 1.1.0 before 1.1.0.r207, and from 1.2.0 before 1.2.0.r206.	N/A	More Details
CVE-2025-7378	An improper Input Validation vulnerability allows injecting arbitrary values of the NAS configuration file in ASUSTOR ADM. This could potentially lead to system misconfiguration and break the format of the configuation file, causing the NAS to exhibit unexpected behavior. This issue affects ADM: from 4.1 before 4.3.1.R5A1.	N/A	More Details
CVE-2025-53688	Rejected reason: Not used	N/A	More Details
CVE-2025-53687	Rejected reason: Not used	N/A	More Details
CVE-2025-53686	Rejected reason: Not used	N/A	More Details
CVE-2025-53685	Rejected reason: Not used	N/A	More Details
CVE-2025-53684	Rejected reason: Not used	N/A	More Details
CVE-2025-53683	Rejected reason: Not used	N/A	More Details
CVE-2025-53682	Rejected reason: Not used	N/A	More Details
CVE-2025-34085	An unrestricted file upload vulnerability in the WordPress Simple File List plugin prior to version 4.2.3 allows unauthenticated remote attackers to achieve remote code execution. The plugin's upload endpoint (ee-upload-engine.php) restricts file uploads based on extension, but lacks proper validation after file renaming. An attacker can first upload a PHP payload disguised as a .png file, then use the plugin’s ee-file-engine.php rename functionality to change the extension to .php. This bypasses upload restrictions and results in the uploaded payload being executable on the server.	N/A	More Details
CVE-2025-34084	An unauthenticated information disclosure vulnerability exists in the WordPress Total Upkeep plugin (also known as BoldGrid Backup) prior to version 1.14.10. The plugin exposes multiple endpoints that allow unauthenticated users to retrieve detailed server configuration (env-info.php) and discover backup metadata (restore-info.json). These backups, which may include full SQL database dumps, are accessible without authentication if their paths are known or guessed. The restore-info.json endpoint discloses the absolute filesystem path of the latest backup, which attackers can convert into a web-accessible URL under wp-content/uploads/ and download. Extracting the database archive may yield credential hashes from the wp_users table, facilitating offline password cracking or credential stuffing attacks.	N/A	More Details
CVE-2025-34083	An unrestricted file upload vulnerability exists in the WordPress AIT CSV Import/Export plugin ≤ 3.0.3. The plugin exposes an upload handler at upload-handler.php that allows arbitrary file upload via a multipart/form-data POST request. This endpoint does not enforce authentication or content-type validation, enabling attackers to upload malicious PHP code directly to the server. Although the upload may produce an error related to CSV parsing, the malicious file is still saved under wp-content/uploads/ and remains executable. Notably, the plugin does not need to be active for exploitation to succeed.	N/A	More Details

CVE-2025-49831	An attacker of Secrets Manager, Self-Hosted installations that route traffic from Secrets Manager to AWS through a misconfigured network device can reroute authentication requests to a malicious server under the attacker’s control. CyberArk believes there to be very few installations where this issue can be actively exploited, though Secrets Manager, Self-Hosted (formerly Conjur Enterprise) prior to versions 13.5.1 and 13.6.1 and Conjur OSS prior to version 1.22.1 may be affected. Conjur OSS version 1.22.1 and Secrets Manager, Self-Hosted versions 13.5.1 and 13.6.1 fix the issue.	N/A	More Details
CVE-2025-49833	GPT-SoVITS-WebUI is a voice conversion and text-to-speech webUI. In versions 20250228v3 and prior, there is a command injection vulnerability in the webui.py open_slice function. slice_opt_root and slice-inp-path takes user input, which is passed to the open_slice function, which concatenates the user input into a command and runs it on the server, leading to arbitrary command execution. At time of publication, no known patched versions are available.	N/A	More Details
CVE-2025-49834	GPT-SoVITS-WebUI is a voice conversion and text-to-speech webUI. In versions 20250228v3 and prior, there is a command injection vulnerability in webui.py open_denoise function. denoise_inp_dir and denoise_opt_dir take user input, which is passed to the open_denoise function, which concatenates the user input into a command and runs it on the server, leading to arbitrary command execution. At time of publication, no known patched versions are available.	N/A	More Details
CVE-2025-49835	GPT-SoVITS-WebUI is a voice conversion and text-to-speech webUI. In versions 20250228v3 and prior, there is a command injection vulnerability in webui.py open_asr function. asr_inp_dir (and a number of other variables) takes user input, which is passed to the open_asr function, which concatenates the user input into a command and runs it on the server, leading to arbitrary command execution. At time of publication, no known patched versions are available.	N/A	More Details
CVE-2025-49836	GPT-SoVITS-WebUI is a voice conversion and text-to-speech webUI. In versions 20250228v3 and prior, there is a command injection vulnerability in webui.py change_label function. path_list takes user input, which is passed to the change_label function, which concatenates the user input into a command and runs it on the server, leading to arbitrary command execution. At time of publication, no known patched versions are available.	N/A	More Details
CVE-2025-49837	GPT-SoVITS-WebUI is a voice conversion and text-to-speech webUI. In versions 20250228v3 and prior, there is an unsafe deserialization vulnerability in vr.py AudioPre. The model_choose variable takes user input (e.g. a path to a model) and passes it to the uvr function. In uvr, a new instance of AudioPre class is created with the model_path attribute containing the aforementioned user input (here called locally model_name). Note that in this step the .pth extension is added to the path. In the AudioPre class, the user input, here called model_path, is used to load the model on that path with torch.load, which can lead to unsafe deserialization. At time of publication, no known patched versions are available.	N/A	More Details
CVE-2025-49838	GPT-SoVITS-WebUI is a voice conversion and text-to-speech webUI. In versions 20250228v3 and prior, there is an unsafe deserialization vulnerability in vr.py AudioPreDeEcho. The model_choose variable takes user input (e.g. a path to a model) and passes it to the uvr function. In uvr, a new instance of AudioPreDeEcho class is created with the model_path attribute containing the aforementioned user input (here called locally model_name). Note that in this step the .pth extension is added to the path. In the AudioPreDeEcho class, the user input, here called model_path, is used to load the model on that path with torch.load, which can lead to unsafe deserialization. At time of publication, no known patched versions are available.	N/A	More Details
CVE-2025-49839	GPT-SoVITS-WebUI is a voice conversion and text-to-speech webUI. In versions 20250228v3 and prior, there is an unsafe deserialization vulnerability in bsroformer.py. The model_choose variable takes user input (e.g. a path to a model) and passes it to the uvr function. In uvr, a new instance of Roformer_Loader class is created with the model_path attribute containing the aformentioned user input (here called locally model_name). Note that in this step the .ckpt extension is added to the path. In the Roformer_Loader class, the user input, here called model_path, is used to load the model on that path with torch.load, which can lead to unsafe deserialization. At time of publication, no known patched versions are available.	N/A	More Details
CVE-2025-49840	GPT-SoVITS-WebUI is a voice conversion and text-to-speech webUI. In versions 20250228v3 and prior, there is an unsafe deserialization vulnerability in inference_webui.py. The GPT_dropdown variable takes user input and passes it to the change_gpt_weights function. In change_gpt_weights, the user input, here gpt_path is used to load a model with torch.load, leading to unsafe deserialization. At time of publication, no known patched versions are available.	N/A	More Details
CVE-2025-49841	GPT-SoVITS-WebUI is a voice conversion and text-to-speech webUI. In versions 20250228v3 and prior, there is an unsafe deserialization vulnerability in process_ckpt.py. The SoVITS_dropdown variable takes user input and passes it to the load_sovits_new function in process_ckpt.py. In load_sovits_new, the user input, here sovits_path is used to load a model with torch.load, leading to unsafe deserialization. At time of publication, no known patched versions are available.	N/A	More Details
CVE-2025-38242	In the Linux kernel, the following vulnerability has been resolved: mm: userfaultfd: fix race of userfaultfd_move and swap cache This commit fixes two kinds of races, they may have different results: Barry reported a BUG_ON in commit c50f8e6053b0, we may see the same BUG_ON if the filemap lookup returned NULL and folio is added to swap cache after that. If another kind of race is triggered (folio changed after lookup) we may see RSS counter is corrupted: [406.893936] BUG: Bad rss-counter state mm:ffff0000c5a9ddc0 type:MM_ANONPAGES val:-1 [406.894071] BUG: Bad rss-counter state mm:ffff0000c5a9ddc0 type:MM_SHMEMPAGES val:1 Because the folio is being accounted to the wrong VMA. I'm not sure if there will be any data corruption though, seems no. The issues above are critical already. On seeing a swap entry PTE, userfaultfd_move does a lockless swap cache lookup, and tries to move the found folio to the faulting vma. Currently, it relies on checking the PTE value to ensure that the moved folio still belongs to the src swap entry and that no new folio has been added to the swap cache, which turns out to be unreliable. While working and reviewing the swap table series with Barry, following existing races are observed and reproduced [1]: In the example below, move_pages_pte is moving src_pte to dst_pte, where src_pte is a swap entry PTE holding swap entry S1, and S1 is not in the swap cache: CPU1 CPU2 userfaultfd_move move_pages_pte() entry = pte_to_swp_entry(orig_src_pte); // Here it got entry = S1 ... < interrupted> ... <swapin src_pte, alloc and use folio A> // folio A is a new allocated folio // and get installed into src_pte <frees swap entry S1> // src_pte now points to folio A, S1 // has swap count == 0, it can be freed // by folio_swap_swap or swap // allocator's reclaim. <try to swap out another folio B> // folio B is a folio in another VMA. <put folio B to swap cache using S1 > // S1 is freed, folio B can use it // for swap out with no problem. ... folio = filemap_get_folio(S1) // Got folio B here !!! ... < interrupted again> ... <swapin folio B and free S1> // Now S1 is free to be used again. <swapout src_pte & folio A using S1> // Now src_pte is a swap entry PTE // holding S1 again. folio_trylock(folio) move_swap_pte double_pt_lock is_pte_pages_stable // Check passed because src_pte == S1 folio_move_anon_rmap(...) // Moved invalid folio B here !!! The race window is very short and requires multiple collisions of multiple rare events, so it's very unlikely to happen, but with a deliberately constructed reproducer and increased time window, it can be reproduced easily. This can be fixed by checking if the folio returned by filemap is the valid swap cache folio after acquiring the folio lock. Another similar race is possible: filemap_get_folio may return NULL, but folio (A) could be swapped in and then swapped out again using the same swap entry after the lookup. In such a case, folio (A) may remain in the swap cache, so it must be moved too: CPU1 CPU2 userfaultfd_move move_pages_pte() entry = pte_to_swp_entry(orig_src_pte); // Here it got entry = S1, and S1 is not in swap cache folio = filemap_get ---truncated---	N/A	More Details

<table>
<tr><td>CVE-2025-49830</td><td>Conjur provides secrets management and application identity for infrastructure. An authenticated attacker who is able to load policy can use the policy yaml parser to reference files on the Secrets Manager, Self-Hosted server. These references may be used as reconnaissance to better understand the folder structure of the Secrets Manager/Conjur server or to have the yaml parser include files on the server in the yaml that is processed as the policy loads. This issue affects Secrets Manager, Self-Hosted (formerly Conjur Enterprise) prior to versions 13.5.1 and 13.6.1 and Conjur OSS prior to version 1.22.1. Conjur OSS version 1.22.1 and Secrets Manager, Self-Hosted versions 13.5.1 and 13.6.1 fix the issue.</td><td>N/A</td><td>More Details</td></tr>
<tr><td>CVE-2025-38263</td><td>In the Linux kernel, the following vulnerability has been resolved: bcache: fix NULL pointer in cache_set_flush() 1. LINE#1794 - LINE#1887 is some codes about function of bch_cache_set_alloc(). 2. LINE#2078 - LINE#2142 is some codes about function of register_cache_set(). 3. register_cache_set() will call bch_cache_set_alloc() in LINE#2098. 1794 struct cache_set *bch_cache_set_alloc(struct cache_sb *sb) 1795 { ... 1860 if (!(c->devices = kcalloc(c->nr_uuids, sizeof(void *), GFP_KERNEL)) || 1861 mempool_init_slab_pool(&c->search, 32, bch_search_cache) || 1862 mempool_init_kmalloc_pool(&c->bio_meta, 2, 1863 sizeof(struct bbio) + sizeof(struct bio_vec) * 1864 bucket_pages(c)) || 1865 mempool_init_kmalloc_pool(&c->fill_iter, 1, iter_size) || 1866 bioset_init(&c->bio_split, 4, offsetof(struct bbio, bio), 1867 BIOSET_NEED_BVECS|BIOSET_NEED_RESCUER) || 1868 !(c->uuids = alloc_bucket_pages(GFP_KERNEL, c)) || 1869 !(c->moving_gc_wq = alloc_workqueue("bcache_gc", 1870 WQ_MEM_RECLAIM, 0)) || 1871 bch_journal_alloc(c) || 1872 bch_btree_cache_alloc(c) || 1873 bch_open_buckets_alloc(c) || 1874 bch_bset_sort_state_init(&c->sort, ilog2(c->btree_pages))) 1875 goto err; ^^^^^^^^ 1876 ... 1883 return c; 1884 err: 1885 bch_cache_set_unregister(c); ^^^^^^^^^^^^^^^^^^^^^^^^^^^ 1886 return NULL; 1887 } ... 2078 static const char *register_cache_set(struct cache *ca) 2079 { ... 2098 c = bch_cache_set_alloc(&ca->sb); 2099 if (!c) 2100 return err; ^^^^^^^^^^ ... 2128 ca->set = c; 2129 ca->set->cache[ca->sb.nr_this_dev] = ca; ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ ... 2138 return NULL; 2139 err: 2140 bch_cache_set_unregister(c); 2141 return err; 2142 } (1) If LINE#1860 - LINE#1874 is true, then do 'goto err'(LINE#1875) and call bch_cache_set_unregister()(LINE#1885). (2) As (1) return NULL(LINE#1886), LINE#2098 - LINE#2100 would return. (3) As (2) has returned, LINE#2128 - LINE#2129 would do *not* give the value to c->cache[], it means that c->cache[] is NULL. LINE#1624 - LINE#1665 is some codes about function of cache_set_flush(). As (1), in LINE#1885 call bch_cache_set_unregister() ---> bch_cache_set_stop() ---> closure_queue() -.-> cache_set_flush() (as below LINE#1624) 1624 static void cache_set_flush(struct closure *cl) 1625 { ... 1654 for_each_cache(ca, c, i) 1655 if (ca->alloc_thread) ^^ 1656 kthread_stop(ca->alloc_thread); ... 1665 } (4) In LINE#1655 ca is NULL(see (3)) in cache_set_flush() then the kernel crash occurred as below: [846.712887] bcache: register_cache() error drbd6: cannot allocate memory [846.713242] bcache: register_bcache() error : failed to register device [846.713336] bcache: cache_set_free() Cache set 2f84bdc1-498a-4f2f-98a7-01946bf54287 unregistered [846.713768] BUG: unable to handle kernel NULL pointer dereference at 00000000000009f8 [846.714790] PGD 0 P4D 0 [846.715129] Oops: 0000 [#1] SMP PTI [846.715472] CPU: 19 PID: 5057 Comm: kworker/19:16 Kdump: loaded Tainted: G OE --------- - - 4.18.0-147.5.1.el8_1.5es.3.x86_64 #1 [846.716082] Hardware name: ESPAN GI-25212/X11DPL-i, BIOS 2.1 06/15/2018 [846.716451] Workqueue: events cache_set_flush [bcache] [846.716808] RIP: 0010:cache_set_flush+0xc9/0x1b0 [bcache] [846.717155] Code: 00 4c 89 a5 b0 03 00 00 48 8b 85 68 f6 ff ff a8 08 0f 84 88 00 00 00 31 db 66 83 bd 3c f7 ff ff 00 48 8b 85 48 ff ff ff 74 28 <48> 8b b8 f8 09 00 0 ---truncated---</td><td>N/A</td><td>More Details</td></tr>
<tr><td>CVE-2025-49829</td><td>Conjur provides secrets management and application identity for infrastructure. Missing validations in Secrets Manager, Self-Hosted allows authenticated attackers to inject resources into the database and to bypass permission checks. This issue affects Secrets Manager, Self-Hosted (formerly Conjur Enterprise) prior to versions 13.5.1 and 13.6.1 and Conjur OSS prior to version 1.22.1. Conjur OSS version 1.22.1 and Secrets Manager, Self-Hosted versions 13.5.1 and 13.6.1 fix the issue.</td><td>N/A</td><td>More Details</td></tr>
<tr><td>CVE-2025-38262</td><td>In the Linux kernel, the following vulnerability has been resolved: tty: serial: uartlite: register uart driver in init When two instances of uart devices are probing, a concurrency race can occur. If one thread calls uart_register_driver function, which first allocates and assigns memory to 'uart_state' member of uart_driver structure, the other instance can bypass uart driver registration and call ulite_assign. This calls uart_add_one_port, which expects the uart driver to be fully initialized. This leads to a kernel panic due to a null pointer dereference: [8.143581] BUG: kernel NULL pointer dereference, address: 00000000000002b8 [8.156982] #PF: supervisor write access in kernel mode [8.156984] #PF: error_code(0x0002) - not-present page [8.156986] PGD 0 P4D 0 ... [8.180668] RIP: 0010:mutex_lock+0x19/0x30 [8.188624] Call Trace: [8.188629] ? __die_body.cold+0x1a/0x1f [8.195260] ? page_fault_oops+0x15c/0x290 [8.209183] ? __irq_resolve_mapping+0x47/0x80 [8.209187] ? exc_page_fault+0x64/0x140 [8.209190] ? asm_exc_page_fault+0x22/0x30 [8.209196] ? mutex_lock+0x19/0x30 [8.223116] uart_add_one_port+0x60/0x440 [8.223122] ? proc_tty_register_driver+0x43/0x50 [8.223126] ? tty_register_driver+0x1ca/0x1e0 [8.246250] ulite_probe+0x357/0x4b0 [uartlite] To prevent it, move uart driver registration in to init function. This will ensure that uart_driver is always registered when probe function is called.</td><td>N/A</td><td>More Details</td></tr>
<tr><td>CVE-2025-38261</td><td>In the Linux kernel, the following vulnerability has been resolved: riscv: save the SR_SUM status over switches When threads/tasks are switched we need to ensure the old execution's SR_SUM state is saved and the new thread has the old SR_SUM state restored. The issue was seen under heavy load especially with the syz-stress tool running, with crashes as follows in schedule_tail: Unable to handle kernel access to user memory without uaccess routines at virtual address 000000002749f0d0 Oops [#1] Modules linked in: CPU: 1 PID: 4875 Comm: syz-executor.0 Not tainted 5.12.0-rc2-syzkaller-00467-g0d7588ab9ef9 #0 Hardware name: riscv-virtio,qemu (DT) epc : schedule_tail+0x72/0xb2 kernel/sched/core.c:4264 ra : task_pid_vnr include/linux/sched.h:1421 [inline] ra : schedule_tail+0x70/0xb2 kernel/sched/core.c:4264 epc : ffffffe00008c8b0 ra : ffffffe00008c8ae sp : ffffffe025d17ec0 gp : ffffffe005d25378 tp : ffffffe00f0d0000 t0 : 0000000000000000 t1 : 0000000000000001 t2 : 00000000000f4240 s0 : ffffffe025d17ee0 s1 : 000000002749f0d0 a0 : 000000000000002a a1 : 0000000000000003 a2 : 1ffffffc0cfac500 a3 : ffffffe0000c80cc a4 : 5ae9db91c19bbe00 a5 : 0000000000000000 a6 : 0000000000f00000 a7 : ffffffe000082eba s2 : 0000000000040000 s3 : ffffffe00eef96c0 s4 : ffffffe022c77fe0 s5 : 0000000000004000 s6 : ffffffe067d74e00 s7 : ffffffe067d74850 s8 : ffffffe067d73e18 s9 : ffffffe067d74e00 s10: ffffffe00eef96e8 s11: 000000ae6cdf8368 t3 : 5ae9db91c19bbe00 t4 : ffffffc4043cafb2 t5 : ffffffc4043cafba t6 : 0000000000040000 status: 0000000000000120 badaddr: 000000002749f0d0 cause: 000000000000000f Call Trace: [<ffffffe00008c8b0>] schedule_tail+0x72/0xb2 kernel/sched/core.c:4264 [<ffffffe000005570>] ret_from_exception+0x0/0x14 Dumping ftrace buffer: (ftrace buffer empty) ---[end trace b5f8f9231dc87dda]--- The issue comes from the put_user() in schedule_tail (kernel/sched/core.c) doing the following: asmlinkage __visible void schedule_tail(struct task_struct *prev) { ... if (current->set_child_tid) put_user(task_pid_vnr(current), current->set_child_tid); ... } the put_user() macro causes the code sequence to come out as follows: 1: __enable_user_access() 2: reg = task_pid_vnr(current); 3: *current->set_child_tid = reg; 4: __disable_user_access() The problem is that we may have a sleeping function as argument which could clear SR_SUM causing the panic above. This was fixed by evaluating the argument of the put_user() macro outside the user-enabled section in commit 285a76bb2cf5 ("riscv: evaluate put_user() arg before enabling user access")" In order for riscv to take advantage of unsafe_get/put_XXX() macros and to avoid the same issue we had with put_user() and sleeping functions we must ensure code flow can go through switch_to() from within a region of code with SR_SUM enabled and come back with SR_SUM still enabled. This patch addresses the problem allowing future work to enable full use of unsafe_get/put_XXX() macros without needing to take a CSR bit flip cost on every access. Make switch_to() save and restore SR_SUM.</td><td>N/A</td><td>More Details</td></tr>
<tr><td></td><td>ZITADEL is an open source identity management system. Starting in version 2.53.0 and prior to versions 4.0.0-rc.2, 3.3.2, 2.71.13,</td><td></td><td></td></tr>
</table>

CVE-2025-53895	and 2.70.14, vulnerability in ZITADEL's session management API allows any authenticated user to update a session if they know its ID, due to a missing permission check. This flaw enables session hijacking, allowing an attacker to impersonate another user and access sensitive resources. Versions prior to `2.53.0` are not affected, as they required the session token for updates. Versions 4.0.0-rc.2, 3.3.2, 2.71.13, and 2.70.14 fix the issue.	N/A	More Details
CVE-2025-38260	In the Linux kernel, the following vulnerability has been resolved: btrfs: handle csum tree error with rescue=ibadroots correctly [BUG] There is syzbot based reproducer that can crash the kernel, with the following call trace: (With some debug output added) DEBUG: rescue=ibadroots parsed BTRFS: device fsid 14d642db-7b15-43e4-81e6-4b8fac6a25f8 devid 1 transid 8 /dev/loop0 (7:0) scanned by repro (1010) BTRFS info (device loop0): first mount of filesystem 14d642db-7b15-43e4-81e6-4b8fac6a25f8 BTRFS info (device loop0): using blake2b (blake2b-256-generic) checksum algorithm BTRFS info (device loop0): using free-space-tree BTRFS warning (device loop0): checksum verify failed on logical 5312512 mirror 1 wanted 0xb043382657aede36608fd3386d6b001692ff406164733d94e2d9a180412c6003 found 0x810ceb2bacb7f0f9eb2bf3b2b15c02af867cb35ad450898169f3b1f0bd818651 level 0 DEBUG: read tree root path failed for tree csum, ret=-5 BTRFS warning (device loop0): checksum verify failed on logical 5328896 mirror 1 wanted 0x51be4e8b303da58e6340226815b70e3a93592dac3f30dd510c7517454de8567a found 0x51be4e8b303da58e634022a315b70e3a93592dac3f30dd510c7517454de8567a level 0 BTRFS warning (device loop0): checksum verify failed on logical 5292032 mirror 1 wanted 0x1924ccd683be9efc2fa98582ef58760e3848e9043db8649ee382681e220cdee4 found 0x0cb6184f6e8799d9f8cb335dccd1d1832da1071d12290dab3b85b587ecacca6e level 0 process 'repro' launched './file2' with NULL argv: empty string added DEBUG: no csum root, idatacsums=0 ibadroots=134217728 Oops: general protection fault, probably for non-canonical address 0xdffffc0000000041: 0000 [#1] SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000208-0x000000000000020f] CPU: 5 UID: 0 PID: 1010 Comm: repro Tainted: G OE 6.15.0-custom+ #249 PREEMPT(full) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS unknown 02/02/2022 RIP: 0010:btrfs_lookup_csum+0x93/0x3d0 [btrfs] Call Trace: <TASK> btrfs_lookup_bio_sums+0x47a/0xdf0 [btrfs] btrfs_submit_bbio+0x43e/0x1a80 [btrfs] submit_one_bio+0xde/0x160 [btrfs] btrfs_readahead+0x498/0x6a0 [btrfs] read_pages+0x1c3/0xb20 page_cache_ra_order+0x4b5/0xc20 filemap_get_pages+0x2d3/0x19e0 filemap_read+0x314/0xde0 __kernel_read+0x35b/0x900 bprm_execve+0x62e/0x1140 do_execveat_common.isra.0+0x3fc/0x520 __x64_sys_execveat+0xdc/0x130 do_syscall_64+0x54/0x1d0 entry_SYSCALL_64_after_hwframe+0x76/0x7e ---[end trace 0000000000000000]--- [CAUSE] Firstly the fs has a corrupted csum tree root, thus to mount the fs we have to go "ro,rescue=ibadroots" mount option. Normally with that mount option, a bad csum tree root should set BTRFS_FS_STATE_NO_DATA_CSUMS flag, so that any future data read will ignore csum search. But in this particular case, we have the following call trace that caused NULL csum root, but not setting BTRFS_FS_STATE_NO_DATA_CSUMS: load_global_roots_objectid(): ret = btrfs_search_slot(); /* Succeeded */ btrfs_item_key_to_cpu() found = true; /* We found the root item for csum tree. */ root = read_tree_root_path(); if (IS_ERR(root)) { if (!btrfs_test_opt(fs_info, IGNOREBADROOTS)) /* * Since we have rescue=ibadroots mount option, * @ret is still 0. */ break; if (!found || ret) { /* @found is true, @ret is 0, error handling for csum * tree is skipped. */ } This means we completely skipped to set BTRFS_FS_STATE_NO_DATA_CSUMS if the csum tree is corrupted, which results unexpected later csum lookup. [FIX] If read_tree_root_path() failed, always populate @ret to the error number. As at the end of the function, we need @ret to determine if we need to do the extra error handling for csum tree.	N/A	More Details
CVE-2025-53826	File Browser provides a file managing interface within a specified directory and it can be used to upload, delete, preview, rename, and edit files. In version 2.39.0, File Browser’s authentication system issues long-lived JWT tokens that remain valid even after the user logs out. As of time of publication, no known patches exist.	N/A	More Details
CVE-2025-53893	File Browser provides a file managing interface within a specified directory and it can be used to upload, delete, preview, rename, and edit files. In version 2.38.0, a Denial of Service (DoS) vulnerability exists in the file processing logic when reading a file on endpoint `Filebrowser-Server-IP:PORT/files/{file-name}` . While the server correctly handles and stores uploaded files, it attempts to load the entire content into memory during read operations without size checks or resource limits. This allows an authenticated user to upload a large file and trigger uncontrolled memory consumption on read, potentially crashing the server and making it unresponsive. As of time of publication, no known patches are available.	N/A	More Details
CVE-2025-38259	In the Linux kernel, the following vulnerability has been resolved: ASoC: codecs: wcd9335: Fix missing free of regulator supplies Driver gets and enables all regulator supplies in probe path (wcd9335_parse_dt() and wcd9335_power_on_reset()), but does not cleanup in final error paths and in unbind (missing remove() callback). This leads to leaked memory and unbalanced regulator enable count during probe errors or unbind. Fix this by converting entire code into devm_regulator_bulk_get_enable() which also greatly simplifies the code.	N/A	More Details
CVE-2025-38258	In the Linux kernel, the following vulnerability has been resolved: mm/damon/sysfs-schemes: free old damon_sysfs_scheme_filter->memcg_path on write memcg_path_store() assigns a newly allocated memory buffer to filter->memcg_path, without deallocating the previously allocated and assigned memory buffer. As a result, users can leak kernel memory by continuously writing a data to memcg_path DAMOS sysfs file. Fix the leak by deallocating the previously set memory buffer.	N/A	More Details
CVE-2025-38257	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Prevent overflow in size calculation for memdup_user() Number of apqn target list entries contained in 'nr_apqns' variable is determined by userspace via an ioctl call so the result of the product in calculation of size passed to memdup_user() may overflow. In this case the actual size of the allocated area and the value describing it won't be in sync leading to various types of unpredictable behaviour later. Use a proper memdup_array_user() helper which returns an error if an overflow is detected. Note that it is different from when nr_apqns is initially zero - that case is considered valid and should be handled in subsequent pkey_handler implementations. Found by Linux Verification Center (linuxtesting.org).	N/A	More Details
CVE-2025-38256	In the Linux kernel, the following vulnerability has been resolved: io_uring/rsrc: fix folio unpinning syzbot complains about an unmapping failure: [108.070381][T14] kernel BUG at mm/gup.c:71! [108.070502][T14] Internal error: Oops - BUG: 00000000f2000800 [#1] SMP [108.123672][T14] Hardware name: QEMU KVM Virtual Machine, BIOS edk2-20250221-8.fc42 02/21/2025 [108.127458][T14] Workqueue: iou_exit io_ring_exit_work [108.174205][T14] Call trace: [108.175649][T14] sanity_check_pinned_pages+0x7cc/0x7d0 (P) [108.178138][T14] unpin_user_page+0x80/0x10c [108.180189][T14] io_release_ubuf+0x84/0xf8 [108.182196][T14] io_free_rsrc_node+0x250/0x57c [108.184345][T14] io_rsrc_data_free+0x148/0x298 [108.186493][T14] io_sqe_buffers_unregister+0x84/0xa0 [108.188991][T14] io_ring_ctx_free+0x48/0x480 [108.191057][T14] io_ring_exit_work+0x764/0x7d8 [108.193207][T14] process_one_work+0x7e8/0x155c [108.195431][T14] worker_thread+0x958/0xed8 [108.197561][T14] kthread+0x5fc/0x75c [108.199362][T14] ret_from_fork+0x10/0x20 We can pin a tail page of a folio, but then io_uring will try to unpin the head page of the folio. While it should be fine in terms of keeping the page actually alive, mm folks say it's wrong and triggers a debug warning. Use unpin_user_folio() instead of unpin_user_page*. [axboe: adapt to current tree, massage commit message]	N/A	More Details
CVE-2025-	The Scratch Channel is a news website that is under development as of time of this writing. The file `/api/users.js` doesn't properly sanitize text box inputs, leading to a potential vulnerability to cross-site scripting attacks. Commit	N/A	More

53903	90b39eb56b27b2bac29001abb1a3cac0964b8ddb addresses this issue.		Details
CVE-2025-38255	In the Linux kernel, the following vulnerability has been resolved: lib/group_cpus: fix NULL pointer dereference from group_cpus_evenly() While testing null_blk with configfs, echo 0 > poll_queues will trigger following panic: BUG: kernel NULL pointer dereference, address: 0000000000000010 Oops: Oops: 0000 [#1] SMP NOPTI CPU: 27 UID: 0 PID: 920 Comm: bash Not tainted 6.15.0-02023-gadbdb95c8696-dirty #1238 PREEMPT(undef) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.1-2.fc37 04/01/2014 RIP: 0010:__bitmap_or+0x48/0x70 Call Trace: <TASK> __group_cpus_evenly+0x822/0x8c0 group_cpus_evenly+0x2d9/0x490 blk_mq_map_queues+0x1e/0x110 null_map_queues+0xc9/0x170 [null_blk] blk_mq_update_queue_map+0xdb/0x160 blk_mq_update_nr_hw_queues+0x22b/0x560 nullb_update_nr_hw_queues+0x71/0xf0 [null_blk] nullb_device_poll_queues_store+0xa4/0x130 [null_blk] configfs_write_iter+0x109/0x1d0 vfs_write+0x26e/0x6f0 ksys_write+0x79/0x180 __x64_sys_write+0x1d/0x30 x64_sys_call+0x45c4/0x45f0 do_syscall_64+0xa5/0x240 entry_SYSCALL_64_after_hwframe+0x76/0x7e Root cause is that numgrps is set to 0, and ZERO_SIZE_PTR is returned from kcalloc(), and later ZERO_SIZE_PTR will be deferenced. Fix the problem by checking numgrps first in group_cpus_evenly(), and return NULL directly if numgrps is zero. [yukuai3@huawei.com: also fix the non-SMP version]	N/A	More Details
CVE-2025-38254	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add sanity checks for drm_edid_raw() When EDID is retrieved via drm_edid_raw(), it doesn't guarantee to return proper EDID bytes the caller wants: it may be either NULL (that leads to an Oops) or with too long bytes over the fixed size raw_edid array (that may lead to memory corruption). The latter was reported actually when connected with a bad adapter. Add sanity checks for drm_edid_raw() to address the above corner cases, and return EDID_BAD_INPUT accordingly. (cherry picked from commit 648d3f4d209725d51900d6a3ed46b7b600140cdf)	N/A	More Details
CVE-2025-38253	In the Linux kernel, the following vulnerability has been resolved: HID: wacom: fix crash in wacom_aes_battery_handler() Commit fd2a9b29dc9c ("HID: wacom: Remove AES power_supply after extended inactivity") introduced wacom_aes_battery_handler() which is scheduled as a delayed work (aes_battery_work). In wacom_remove(), aes_battery_work is not canceled. Consequently, if the device is removed while aes_battery_work is still pending, then hard crashes or "Oops: general protection fault..." are experienced when wacom_aes_battery_handler() is finally called. E.g., this happens with built-in USB devices after resume from hibernate when aes_battery_work was still pending at the time of hibernation. So, take care to cancel aes_battery_work in wacom_remove().	N/A	More Details
CVE-2025-38252	In the Linux kernel, the following vulnerability has been resolved: cxl/ras: Fix CPER handler device confusion By inspection, cxl_cper_handle_prot_err() is making a series of fragile assumptions that can lead to crashes: 1/ It assumes that endpoints identified in the record are a CXL-type-3 device, nothing guarantees that. 2/ It assumes that the device is bound to the cxl_pci driver, nothing guarantees that. 3/ Minor, it holds the device lock over the switch-port tracing for no reason as the trace is 100% generated from data in the record. Correct those by checking that the PCIe endpoint parents a cxl_memdev before assuming the format of the driver data, and move the lock to where it is required. Consequently this also makes the implementation ready for CXL accelerators that are not bound to cxl_pci.	N/A	More Details
CVE-2025-38251	In the Linux kernel, the following vulnerability has been resolved: atm: clip: prevent NULL deref in clip_push() Blamed commit missed that vcc_destroy_socket() calls clip_push() with a NULL skb. If clip_devs is NULL, clip_push() then crashes when reading skb->truesize.	N/A	More Details
CVE-2025-38250	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_core: Fix use-after-free in vhci_flush() syzbot reported use-after-free in vhci_flush() without repro. [0] From the splat, a thread close()d a vhci file descriptor while its device was being used by iotcl() on another thread. Once the last fd refcnt is released, vhci_release() calls hci_unregister_dev(), hci_free_dev(), and kfree() for struct vhci_data, which is set to hci_dev->dev->driver_data. The problem is that there is no synchronisation after unlinking hdev from hci_dev_list in hci_unregister_dev(). There might be another thread still accessing the hdev which was fetched before the unlink operation. We can use SRCU for such synchronisation. Let's run hci_dev_reset() under SRCU and wait for its completion in hci_unregister_dev(). Another option would be to restore hci_dev->destruct(), which was removed in commit 587ae086f6e4 ("Bluetooth: Remove unused hci-destruct cb"). However, this would not be a good solution, as we should not run hci_unregister_dev() while there are in-flight ioctl() requests, which could lead to another data-race KCSAN splat. Note that other drivers seem to have the same problem, for exmaple, virtbt_remove(). [0]: BUG: KASAN: slab-use-after-free in skb_queue_empty_lockless include/linux/skbuff.h:1891 [inline] BUG: KASAN: slab-use-after-free in skb_queue_purge_reason+0x99/0x360 net/core/skbuff.c:3937 Read of size 8 at addr ffff88807cb8d858 by task syz.1.219/6718 CPU: 1 UID: 0 PID: 6718 Comm: syz.1.219 Not tainted 6.16.0-rc1-syzkaller-00196-g08207f42d3ff #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/07/2025 Call Trace: <TASK> dump_stack_lvl+0x189/0x250 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:408 [inline] print_report+0xd2/0x2b0 mm/kasan/report.c:521 kasan_report+0x118/0x150 mm/kasan/report.c:634 skb_queue_empty_lockless include/linux/skbuff.h:1891 [inline] skb_queue_purge_reason+0x99/0x360 net/core/skbuff.c:3937 skb_queue_purge include/linux/skbuff.h:3368 [inline] vhci_flush+0x44/0x50 drivers/bluetooth/hci_vhci.c:69 hci_dev_do_reset net/bluetooth/hci_core.c:552 [inline] hci_dev_reset+0x420/0x5c0 net/bluetooth/hci_core.c:592 sock_do_ioctl+0xd9/0x300 net/socket.c:1190 sock_ioctl+0x576/0x790 net/socket.c:1311 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:907 [inline] __se_sys_ioctl+0xf9/0x170 fs/ioctl.c:893 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: 0033:0x7fcf5b98e929 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:00007fcf5c7b9038 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 00007fcf5bbb6160 RCX: 00007fcf5b98e929 RDX: 0000000000000000 RSI: 00000000400448cb RDI: 0000000000000009 RBP: 00007fcf5ba10b39 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007fcf5bbb6160 R15: 00007ffd6353d528 </TASK> Allocated by task 6535: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:68 poison_kmalloc_redzone mm/kasan/common.c:377 [inline] __kasan_kmalloc+0x93/0xb0 mm/kasan/common.c:394 kasan_kmalloc include/linux/kasan.h:260 [inline] __kmalloc_cache_noprof+0x230/0x3d0 mm/slub.c:4359 kmalloc_noprof include/linux/slab.h:905 [inline] kzalloc_noprof include/linux/slab.h:1039 [inline] vhci_open+0x57/0x360 drivers/bluetooth/hci_vhci.c:635 misc_open+0x2bc/0x330 drivers/char/misc.c:161 chrdev_open+0x4c9/0x5e0 fs/char_dev.c:414 do_dentry_open+0xdf0/0x1970 fs/open.c:964 vfs_open+0x3b/0x340 fs/open.c:1094 do_open fs/namei.c:3887 [inline] path_openat+0x2ee5/0x3830 fs/name ---truncated---	N/A	More Details
CVE-2025-38249	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Fix out-of-bounds read in snd_usb_get_audioformat_uac3() In snd_usb_get_audioformat_uac3(), the length value returned from snd_usb_ctl_msg() is used directly for memory allocation without validation. This length is controlled by the USB device. The allocated buffer is cast to a uac3_cluster_header_descriptor and its fields are accessed without verifying that the buffer is large enough. If the device returns a smaller than expected length, this leads to an out-of-bounds read. Add a length check to ensure the buffer is large enough for uac3_cluster_header_descriptor.	N/A	More Details

CVE-2025-38248	In the Linux kernel, the following vulnerability has been resolved: bridge: mcast: Fix use-after-free during router port configuration The bridge maintains a global list of ports behind which a multicast router resides. The list is consulted during forwarding to ensure multicast packets are forwarded to these ports even if the ports are not member in the matching MDB entry. When per-VLAN multicast snooping is enabled, the per-port multicast context is disabled on each port and the port is removed from the global router port list: # ip link add name br1 up type bridge vlan_filtering 1 mcast_snooping 1 # ip link add name dummy1 up master br1 type dummy # ip link set dev dummy1 type bridge_slave mcast_router 2 $ bridge -d mdb show | grep router router ports on br1: dummy1 # ip link set dev br1 type bridge mcast_vlan_snooping 1 $ bridge -d mdb show | grep router However, the port can be re-added to the global list even when per-VLAN multicast snooping is enabled: # ip link set dev dummy1 type bridge_slave mcast_router 0 # ip link set dev dummy1 type bridge_slave mcast_router 2 $ bridge -d mdb show | grep router router ports on br1: dummy1 Since commit 4b30ae9adb04 ("net: bridge: mcast: re-implement br_multicast_{enable, disable}_port functions"), when per-VLAN multicast snooping is enabled, multicast disablement on a port will disable the per-{port, VLAN} multicast contexts and not the per-port one. As a result, a port will remain in the global router port list even after it is deleted. This will lead to a use-after-free [1] when the list is traversed (when adding a new port to the list, for example): # ip link del dev dummy1 # ip link add name dummy2 up master br1 type dummy # ip link set dev dummy2 type bridge_slave mcast_router 2 Similarly, stale entries can also be found in the per-VLAN router port list. When per-VLAN multicast snooping is disabled, the per-{port, VLAN} contexts are disabled on each port and the port is removed from the per-VLAN router port list: # ip link add name br1 up type bridge vlan_filtering 1 mcast_snooping 1 mcast_vlan_snooping 1 # ip link add name dummy1 up master br1 type dummy # bridge vlan add vid 2 dev dummy1 # bridge vlan global set vid 2 dev br1 mcast_snooping 1 # bridge vlan set vid 2 dev dummy1 mcast_router 2 $ bridge vlan global show dev br1 vid 2 | grep router router ports: dummy1 # ip link set dev br1 type bridge mcast_vlan_snooping 0 $ bridge vlan global show dev br1 vid 2 | grep router However, the port can be re-added to the per-VLAN list even when per-VLAN multicast snooping is disabled: # bridge vlan set vid 2 dev dummy1 mcast_router 0 # bridge vlan set vid 2 dev dummy1 mcast_router 2 $ bridge vlan global show dev br1 vid 2 | grep router router ports: dummy1 When the VLAN is deleted from the port, the per-{port, VLAN} multicast context will not be disabled since multicast snooping is not enabled on the VLAN. As a result, the port will remain in the per-VLAN router port list even after it is no longer member in the VLAN. This will lead to a use-after-free [2] when the list is traversed (when adding a new port to the list, for example): # ip link add name dummy2 up master br1 type dummy # bridge vlan add vid 2 dev dummy2 # bridge vlan del vid 2 dev dummy1 # bridge vlan set vid 2 dev dummy2 mcast_router 2 Fix these issues by removing the port from the relevant (global or per-VLAN) router port list in br_multicast_port_ctx_deinit(). The function is invoked during port deletion with the per-port multicast context and during VLAN deletion with the per-{port, VLAN} multicast context. Note that deleting the multicast router timer is not enough as it only takes care of the temporary multicast router states (1 or 3) and not the permanent one (2). [1] BUG: KASAN: slab-out-of-bounds in br_multicast_add_router.part.0+0x3f1/0x560 Write of size 8 at addr ffff888004a67328 by task ip/384 [...] Call Trace: <TASK> dump_stack ---truncated---	N/A	More Details
CVE-2025-38247	In the Linux kernel, the following vulnerability has been resolved: userns and mnt_idmap leak in open_tree_attr(2) Once want_mount_setattr() has returned a positive, it does require finish_mount_kattr() to release ->mnt_userns. Failing do_mount_setattr() does not change that. As the result, we can end up leaking userns and possibly mnt_idmap as well.	N/A	More Details
CVE-2025-38246	In the Linux kernel, the following vulnerability has been resolved: bnxt: properly flush XDP redirect lists We encountered following crash when testing a XDP_REDIRECT feature in production: [56251.579676] list_add corruption. next->prev should be prev (ffff93120dd40f30), but was ffffb301ef3a6740. (next=ffff93120dd 40f30). [56251.601413] ------------[cut here]------------ [56251.611357] kernel BUG at lib/list_debug.c:29! [56251.621082] Oops: invalid opcode: 0000 [#1] PREEMPT SMP NOPTI [56251.632073] CPU: 111 UID: 0 PID: 0 Comm: swapper/111 Kdump: loaded Tainted: P O 6.12.33-cloudflare-2025.6. 3 #1 [56251.653155] Tainted: [P]=PROPRIETARY_MODULE, [O]=OOT_MODULE [56251.663877] Hardware name: MiTAC GC68B-B8032-G11P6-GPU/S8032GM-HE-CFR, BIOS V7.020.B10-sig 01/22/2025 [56251.682626] RIP: 0010:__list_add_valid_or_report+0x4b/0xa0 [56251.693203] Code: 0e 48 c7 c7 68 e7 d9 97 e8 42 16 fe ff 0f 0b 48 8b 52 08 48 39 c2 74 14 48 89 f1 48 c7 c7 90 e7 d9 97 48 89 c6 e8 25 16 fe ff <0f> 0b 4c 8b 02 49 39 f0 74 14 48 89 d1 48 c7 c7 e8 e7 d9 97 4c 89 [56251.725811] RSP: 0018:ffff93120dd40b80 EFLAGS: 00010246 [56251.736094] RAX: 0000000000000075 RBX: ffffb301e6bba9d8 RCX: 0000000000000000 [56251.748260] RDX: 0000000000000000 RSI: ffff9149afda0b80 RDI: ffff9149afda0b80 [56251.760349] RBP: ffff9131e49c8000 R08: 0000000000000000 R09: ffff93120dd40a18 [56251.772382] R10: ffff9159cf2ce1a8 R11: 0000000000000003 R12: ffff911a80850000 [56251.784364] R13: ffff93120fbc7000 R14: 0000000000000010 R15: ffff9139e7510e40 [56251.796278] FS: 0000000000000000(0000) GS:ffff9149afd80000(0000) knlGS:0000000000000000 [56251.809133] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [56251.819561] CR2: 00007f5e85e6f300 CR3: 00000038b85e2006 CR4: 0000000000770ef0 [56251.831365] PKRU: 55555554 [56251.838653] Call Trace: [56251.845560] <IRQ> [56251.851943] cpu_map_enqueue.cold+0x5/0xa [56251.860243] xdp_do_redirect+0x2d9/0x480 [56251.868388] bnxt_rx_xdp+0x1d8/0x4c0 [bnxt_en] [56251.877028] bnxt_rx_pkt+0x5f7/0x19b0 [bnxt_en] [56251.885665] ? cpu_max_write+0x1e/0x100 [56251.893510] ? srso_alias_return_thunk+0x5/0xfbef5 [56251.902276] __bnxt_poll_work+0x190/0x340 [bnxt_en] [56251.911058] bnxt_poll+0xab/0x1b0 [bnxt_en] [56251.919041] ? srso_alias_return_thunk+0x5/0xfbef5 [56251.927568] ? srso_alias_return_thunk+0x5/0xfbef5 [56251.935958] ? srso_alias_return_thunk+0x5/0xfbef5 [56251.944250] __napi_poll+0x2b/0x160 [56251.951155] bpf_trampoline_6442548651+0x79/0x123 [56251.959262] __napi_poll+0x5/0x160 [56251.966037] net_rx_action+0x3d2/0x880 [56251.973133] ? srso_alias_return_thunk+0x5/0xfbef5 [56251.981265] ? srso_alias_return_thunk+0x5/0xfbef5 [56251.989262] ? __hrtimer_run_queues+0x162/0x2a0 [56251.996967] ? srso_alias_return_thunk+0x5/0xfbef5 [56252.004875] ? srso_alias_return_thunk+0x5/0xfbef5 [56252.012673] ? bnxt_msix+0x62/0x70 [bnxt_en] [56252.019903] handle_softirqs+0xcf/0x270 [56252.026650] irq_exit_rcu+0x67/0x90 [56252.032933] common_interrupt+0x85/0xa0 [56252.039498] </IRQ> [56252.044246] <TASK> [56252.048935] asm_common_interrupt+0x26/0x40 [56252.055727] RIP: 0010:cpuidle_enter_state+0xb8/0x420 [56252.063305] Code: dc 01 00 00 e8 f9 79 3b ff e8 64 f7 ff ff 49 89 c5 0f 1f 44 00 00 31 ff e8 a5 32 3a ff 45 84 ff 0f 85 ae 01 00 00 fb 45 85 f6 <0f> 88 88 01 00 00 48 8b 04 24 49 63 ce 4c 89 ea 48 6b f1 68 48 29 [56252.088911] RSP: 0018:ffff93120c97fe98 EFLAGS: 00000202 [56252.096912] RAX: ffff9149afd80000 RBX: ffff9141d3a72800 RCX: 0000000000000000 [56252.106844] RDX: 00003329176c6b98 RSI: ffffffe36db3fdc7 RDI: 0000000000000000 [56252.116733] RBP: 0000000000000002 R08: 0000000000000002 R09: 000000000000004e [56252.126652] R10: ffff9149afdb30c4 R11: 071c71c71c71c71c R12: ffffffff985ff860 [56252.136637] R13: 00003329176c6b98 R14: 0000000000000002 R15: 0000000000000000 [56252.146667] ? cpuidle_enter_state+0xab/0x420 [56252.153909] cpuidle_enter+0x2d/0x40 [56252.160360] do_idle+0x176/0x1c0 [56252.166456 ---truncated---	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: atm: Release atm_dev_mutex after removing procfs in atm_dev_deregister(). syzbot reported a warning below during atm_dev_register(). [0] Before creating a new device and procfs/sysfs for it, atm_dev_register() looks up a duplicated device by __atm_dev_lookup(). These operations are done under atm_dev_mutex. However, when removing a device in atm_dev_deregister(), it releases the mutex just after removing the device from the list that __atm_dev_lookup() iterates over. So, there will be a small race window where the device does not exist on the device list but procfs/sysfs are still not removed, triggering the splat. Let's hold the mutex until procfs/sysfs are removed in atm_dev_deregister(). [0]: proc_dir_entry 'atm/atmtcp:0' already registered WARNING: CPU: 0 PID: 5919 at fs/proc/generic.c:377 proc_register+0x455/0x5f0 fs/proc/generic.c:377 Modules linked in: CPU: 0 UID: 0 PID: 5919 Comm: syz-executor284 Not tainted 6.16.0-rc2-syzkaller-00047-g52da431bf03b #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute		

CVE-2025-38245	Engine, BIOS Google 05/07/2025 RIP: 0010:proc_register+0x455/0x5f0 fs/proc/generic.c:377 Code: 48 89 f9 48 c1 e9 03 80 3c 01 00 0f 85 a2 01 00 00 48 8b 44 24 10 48 c7 c7 20 c0 c2 8b 48 8b b0 d8 00 00 00 e8 0c 02 1c ff 90 <0f> 0b 90 90 48 c7 c7 80 f2 82 8e e8 0b de 23 09 48 8b 4c 24 28 48 RSP: 0018:ffffc9000466fa30 EFLAGS: 00010282 RAX: 0000000000000000 RBX: 0000000000000000 RCX: ffffffff817ae248 RDX: ffff888026280000 RSI: ffffffff817ae255 RDI: 0000000000000001 RBP: ffff8880232bed48 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000001 R12: ffff888076ed2140 R13: dffffc0000000000 R14: ffff888078a61340 R15: ffffed100edda444 FS: 00007f38b3b0c6c0(0000) GS:ffff888124753000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f38b3bdf953 CR3: 0000000076d58000 CR4: 00000000003526f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> proc_create_data+0xbe/0x110 fs/proc/generic.c:585 atm_proc_dev_register+0x112/0x1e0 net/atm/proc.c:361 atm_dev_register+0x46d/0x890 net/atm/resources.c:113 atmtcp_create+0x77/0x210 drivers/atm/atmtcp.c:369 atmtcp_attach drivers/atm/atmtcp.c:403 [inline] atmtcp_ioctl+0x2f9/0xd60 drivers/atm/atmtcp.c:464 do_vcc_ioctl+0x12c/0x930 net/atm/ioctl.c:159 sock_do_ioctl+0x115/0x280 net/socket.c:1190 sock_ioctl+0x227/0x6b0 net/socket.c:1311 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:907 [inline] __se_sys_ioctl fs/ioctl.c:893 [inline] __x64_sys_ioctl+0x18b/0x210 fs/ioctl.c:893 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xcd/0x4c0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f38b3b74459 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 18 00 00 90 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 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f38b3b0c198 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 00007f38b3bfe318 RCX: 00007f38b3b74459 RDX: 0000000000000000 RSI: 0000000000006180 RDI: 0000000000000005 RBP: 00007f38b3bfe310 R08: 65732f636f72702f R09: 65732f636f72702f R10: 65732f636f72702f R11: 0000000000000246 R12: 00007f38b3bcb0ac R13: 00007f38b3b0c1a0 R14: 0000200000000200 R15: 00007f38b3bcb03b </TASK>	N/A	More Details
CVE-2025-38244	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential deadlock when reconnecting channels Fix cifs_signal_cifsd_for_reconnect() to take the correct lock order and prevent the following deadlock from happening == WARNING: possible circular locking dependency detected 6.16.0-rc3-build2+ #1301 Tainted: G S W -- cifsd/6055 is trying to acquire lock: ffff88810ad56038 (&tcp_ses->srv_lock){+.+.}-{3:3}, at: cifs_signal_cifsd_for_reconnect+0x134/0x200 but task is already holding lock: ffff888119c64330 (&ret_buf->chan_lock){+.+.}-{3:3}, at: cifs_signal_cifsd_for_reconnect+0xcf/0x200 which lock already depends on the new lock. the existing dependency chain (in reverse order) is: -> #2 (&ret_buf->chan_lock){+.+.}-{3:3}: validate_chain+0x1cf/0x270 __lock_acquire+0x60e/0x780 lock_acquire.part.0+0xb4/0x1f0 _raw_spin_lock+0x2f/0x40 cifs_setup_session+0x81/0x4b0 cifs_get_smb_ses+0x771/0x900 cifs_mount_get_session+0x7e/0x170 cifs_mount+0x92/0x2d0 cifs_smb3_do_mount+0x161/0x460 smb3_get_tree+0x55/0x90 vfs_get_tree+0x46/0x180 do_new_mount+0x1b0/0x2e0 path_mount+0x6ee/0x740 do_mount+0x98/0xe0 __do_sys_mount+0x148/0x180 do_syscall_64+0xa4/0x260 entry_SYSCALL_64_after_hwframe+0x76/0x7e -> #1 (&ret_buf->ses_lock){+.+.}-{3:3}: validate_chain+0x1cf/0x270 __lock_acquire+0x60e/0x780 lock_acquire.part.0+0xb4/0x1f0 _raw_spin_lock+0x2f/0x40 cifs_match_super+0x101/0x320 sget+0xab/0x270 cifs_smb3_do_mount+0x1e0/0x460 smb3_get_tree+0x55/0x90 vfs_get_tree+0x46/0x180 do_new_mount+0x1b0/0x2e0 path_mount+0x6ee/0x740 do_mount+0x98/0xe0 __do_sys_mount+0x148/0x180 do_syscall_64+0xa4/0x260 entry_SYSCALL_64_after_hwframe+0x76/0x7e -> #0 (&tcp_ses->srv_lock){+.+.}-{3:3}: check_noncircular+0x95/0xc0 check_prev_add+0x115/0x2f0 validate_chain+0x1cf/0x270 __lock_acquire+0x60e/0x780 lock_acquire.part.0+0xb4/0x1f0 _raw_spin_lock+0x2f/0x40 cifs_signal_cifsd_for_reconnect+0x134/0x200 __cifs_reconnect+0x8f/0x500 cifs_handle_standard+0x112/0x280 cifs_demultiplex_thread+0x64d/0xbc0 kthread+0x2f7/0x310 ret_from_fork+0x2a/0x230 ret_from_fork_asm+0x1a/0x30 other info that might help us debug this: Chain exists of: &tcp_ses->srv_lock --> &ret_buf->ses_lock --> &ret_buf->chan_lock Possible unsafe locking scenario: CPU0 CPU1 ---- ---- lock(&ret_buf->chan_lock); lock(&ret_buf->ses_lock); lock(&ret_buf->chan_lock); lock(&tcp_ses->srv_lock); *** DEADLOCK *** 3 locks held by cifsd/6055: #0: ffffffff857de398 (&cifs_tcp_ses_lock){+.+.}-{3:3}, at: cifs_signal_cifsd_for_reconnect+0x7b/0x200 #1: ffff888119c64060 (&ret_buf->ses_lock){+.+.}-{3:3}, at: cifs_signal_cifsd_for_reconnect+0x9c/0x200 #2: ffff888119c64330 (&ret_buf->chan_lock){+.+.}-{3:3}, at: cifs_signal_cifsd_for_reconnect+0xcf/0x200	N/A	More Details
CVE-2025-53640	Indico is an event management system that uses Flask-Multipass, a multi-backend authentication system for Flask. Starting in version 2.2 and prior to version 3.3.7, an endpoint used to display details of users listed in certain fields (such as ACLs) could be misused to dump basic user details (such as name, affiliation and email) in bulk. Version 3.3.7 fixes the issue. Owners of instances that allow everyone to create a user account, who wish to truly restrict access to these user details, should consider restricting user search to managers. As a workaround, it is possible to restrict access to the affected endpoints (e.g. in the webserver config), but doing so would break certain form fields which could no longer show the details of the users listed in those fields, so upgrading instead is highly recommended.	N/A	More Details
CVE-2025-49828	Conjur provides secrets management and application identity for infrastructure. Conjur OSS versions 1.19.5 through 1.21.1 and Secrets Manager, Self-Hosted (formerly known as Conjur Enterprise) 13.1 through 13.4.1 are vulnerable to remote code execution An authenticated attacker who can inject secrets or templates into the Secrets Manager, Self-Hosted database could take advantage of an exposed API endpoint to execute arbitrary Ruby code within the Secrets Manager process. This issue affects both Secrets Manager, Self-Hosted (formerly Conjur Enterprise) and Conjur OSS. Conjur OSS version 1.21.2 and Secrets Manager, Self-Hosted version 13.5 fix the issue.	N/A	More Details
CVE-2025-53643	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.12.14, the Python parser is vulnerable to a request smuggling vulnerability due to not parsing trailer sections of an HTTP request. If a pure Python version of aiohttp is installed (i.e. without the usual C extensions) or AIOHTTP_NO_EXTENSIONS is enabled, then an attacker may be able to execute a request smuggling attack to bypass certain firewalls or proxy protections. Version 3.12.14 contains a patch for this issue.	N/A	More Details
CVE-2025-38275	In the Linux kernel, the following vulnerability has been resolved: phy: qcom-qmp-usb: Fix an NULL vs IS_ERR() bug The qmp_usb_iomap() helper function currently returns the raw result of devm_ioremap() for non-exclusive mappings. Since devm_ioremap() may return a NULL pointer and the caller only checks error pointers with IS_ERR(), NULL could bypass the check and lead to an invalid dereference. Fix the issue by checking if devm_ioremap() returns NULL. When it does, qmp_usb_iomap() now returns an error pointer via IOMEM_ERR_PTR(-ENOMEM), ensuring safe and consistent error handling.	N/A	More Details
CVE-2025-53639	MeterSphere is an open source continuous testing platform. Prior to version 3.6.5-lts, the sortField parameter in certain API endpoints is not properly validated or sanitized. An attacker can supply crafted input to inject and execute arbitrary SQL statements through the sorting functionality. This could result in modification or deletion of database contents, with a potential full compromise of the application’s database integrity and availability. Version 3.6.5-lts fixes the issue.	N/A	More Details
CVE-2025-34096	A stack-based buffer overflow vulnerability exists in Easy File Sharing HTTP Server version 7.2. The flaw is triggered when a crafted POST request is sent to the /sendemail.ghp endpoint containing an overly long Email parameter. The application fails to properly validate the length of this field, resulting in a memory corruption condition. An unauthenticated remote attacker can exploit this to	N/A	More Details

	execute arbitrary code with the privileges of the server process.		
CVE-2024-7650	Improper Control of Generation of Code ('Code Injection') vulnerability in OpenText™ Directory Services allows Remote Code Inclusion. The vulnerability could allow access to the system via script injection.This issue affects Directory Services: 23.4.	N/A	More Details
CVE-2025-6211	A vulnerability in the DocugamiReader class of the run-llama/llama_index repository, up to version 0.12.28, involves the use of MD5 hashing to generate IDs for document chunks. This approach leads to hash collisions when structurally distinct chunks contain identical text, resulting in one chunk overwriting another. This can cause loss of semantically or legally important document content, breakage of parent-child chunk hierarchies, and inaccurate or hallucinated responses in AI outputs. The issue is resolved in version 0.3.1.	N/A	More Details
CVE-2025-7370	Rejected reason: Upon investigtion upstream maintainers discovered this was not a real issue. See the references for more details. See: https://gitlab.gnome.org/GNOME/libsoup/-/issues/430#note_2494090.	N/A	More Details
CVE-2025-53549	The Matrix Rust SDK is a collection of libraries that make it easier to build Matrix clients in Rust. An SQL injection vulnerability in the EventCache::find_event_with_relations method of matrix-sdk 0.11 and 0.12 allows malicious room members to execute arbitrary SQL commands in Matrix clients that directly pass relation types provided by those room members into this method, when used with the default sqlite-based store backend. Exploitation is unlikely, as no known clients currently use the API in this manner. This vulnerability is fixed in 0.13.	N/A	More Details
CVE-2025-53625	The DynamicPageList3 extension is a reporting tool for MediaWiki, listing category members and intersections with various formats and details. Several #dpl parameters can leak usernames that have been hidden using revision deletion, suppression, or the hideuser block flag. The vulnerability is fixed in 3.6.4.	N/A	More Details
CVE-2025-34093	An authenticated command injection vulnerability exists in the Polycom HDX Series command shell interface accessible over Telnet. The lan traceroute command in the devcmds console accepts unsanitized input, allowing attackers to execute arbitrary system commands. By injecting shell metacharacters through the traceroute interface, an attacker can achieve remote code execution under the context of the root user. This flaw affects systems where Telnet access is enabled and either unauthenticated access is allowed or credentials are known.	N/A	More Details
CVE-2025-34095	An OS command injection vulnerability exists in Mako Server versions 2.5 and 2.6, specifically within the tutorial interface provided by the examples/save.lsp endpoint. An unauthenticated attacker can send a crafted PUT request containing arbitrary Lua os.execute() code, which is then persisted on disk and triggered via a subsequent GET request to examples/manage.lsp. This allows remote command execution on the underlying operating system, impacting both Windows and Unix-based deployments.	N/A	More Details
CVE-2025-34097	An unrestricted file upload vulnerability exists in ProcessMaker versions prior to 3.5.4 due to improper handling of uploaded plugin archives. An attacker with administrative privileges can upload a malicious .tar plugin file containing arbitrary PHP code. Upon installation, the plugin’s install() method is invoked, resulting in execution of attacker-supplied PHP code on the server with the privileges of the web server user. This vulnerability can be chained with CVE-2022-38577 — a privilege escalation flaw in the user profile page — to achieve full remote code execution from a low-privileged account.	N/A	More Details
CVE-2025-38348	In the Linux kernel, the following vulnerability has been resolved: wifi: p54: prevent buffer-overflow in p54_rx_eeprom_readback() Robert Morris reported: |If a malicious USB device pretends to be an Intersil p54 wifi |interface and generates an eeprom_readback message with a large |eeprom->v1.len, p54_rx_eeprom_readback() will copy data from the |message beyond the end of priv->eeprom. | |static void p54_rx_eeprom_readback(struct p54_common *priv, | struct sk_buff *skb) |{ | struct p54_hdr *hdr = (struct p54_hdr *) skb->data; | struct p54_eeprom_lm86 *eeprom = (struct p54_eeprom_lm86 *) hdr->data; | | if (priv->fw_var >= 0x509) { | memcpy(priv->eeprom, eeprom->v2.data, | le16_to_cpu(eeprom->v2.len)); | } else { | memcpy(priv->eeprom, eeprom->v1.data, | le16_to_cpu(eeprom->v1.len)); | } | [...] The eeprom->v{1,2}.len is set by the driver in p54_download_eeprom(). The device is supposed to provide the same length back to the driver. But yes, it's possible (like shown in the report) to alter the value to something that causes a crash/panic due to overrun. This patch addresses the issue by adding the size to the common device context, so p54_rx_eeprom_readback no longer relies on possibly tampered values... That said, it also checks if the "firmware" altered the value and no longer copies them. The one, small saving grace is: Before the driver tries to read the eeprom, it needs to upload >a< firmware. the vendor firmware has a proprietary license and as a reason, it is not present on most distributions by default.	N/A	More Details
CVE-2025-34098	A path traversal vulnerability exists in Riverbed SteelHead VCX appliances (confirmed in VCX255U 9.6.0a) due to improper input validation in the log filtering functionality exposed via the management web interface. An authenticated attacker can exploit this flaw by submitting crafted filter expressions to the log_filter endpoint using the filterStr parameter. This input is processed by a backend parser that permits execution of file expansion syntax, allowing the attacker to retrieve arbitrary system files via the log viewing interface.	N/A	More Details
CVE-2025-34099	An unauthenticated command injection vulnerability exists in VICIdial versions 2.9 RC1 through 2.13 RC1, within the vicidial_sales_viewer.php component when password encryption is enabled (a non-default configuration). The application improperly passes the HTTP Basic Authentication password directly to a call to exec() without adequate sanitation. This allows remote attackers to inject and execute arbitrary operating system commands as the web server user.	N/A	More Details
CVE-2025-34100	An unrestricted file upload vulnerability exists in BuilderEngine 3.5.0 via the integration of the elFinder 2.0 file manager and its use of the jQuery File Upload plugin. The plugin fails to properly validate or restrict file types or locations during upload operations, allowing an attacker to upload a malicious .php file and subsequently execute arbitrary PHP code on the server under the context of the web server process. While the root vulnerability lies within the jQuery File Upload component, BuilderEngine’s improper integration and lack of access controls expose this functionality to unauthenticated users, resulting in full remote code execution.	N/A	More Details
CVE-2025-34101	An unauthenticated command injection vulnerability exists in Serviio Media Server versions 1.4 through 1.8 on Windows, in the /rest/action API endpoint exposed by the console component (default port 23423). The checkStreamUrl method accepts a VIDEO parameter that is passed unsanitized to a call to cmd.exe, enabling arbitrary command execution under the privileges of the web server. No authentication is required to exploit this issue, as the REST API is exposed by default and lacks access controls.	N/A	More Details
CVE-2025-34102	A remote code execution vulnerability exists in CryptoLog (PHP version, discontinued since 2009) due to a chained exploitation of SQL injection and command injection vulnerabilities. An unauthenticated attacker can gain shell access as the web server user by first exploiting a SQL injection flaw in login.php to bypass authentication, followed by command injection in logshares_ajax.php to execute arbitrary operating system commands. The login bypass is achieved by submitting crafted SQL via the user POST parameter. Once authenticated, the attacker can abuse the lsid POST parameter in the logshares_ajax.php endpoint to inject and	N/A	More Details

	execute a command using $(...) syntax, resulting in code execution under the web context. This exploitation path does not exist in the ASP.NET version of CryptoLog released since 2009.		
CVE-2025-53628	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.20.1, cpp-httplib does not have a limit for a unique line, permitting an attacker to explore this to allocate memory arbitrarily. This vulnerability is fixed in 0.20.1. NOTE: This vulnerability is related to CVE-2025-53629.	N/A	More Details
CVE-2025-53630	llama.cpp is an inference of several LLM models in C/C++. Integer Overflow in the gguf_init_from_file_impl function in ggml/src/gguf.cpp can lead to Heap Out-of-Bounds Read/Write. This vulnerability is fixed in commit 26a48ad699d50b6268900062661bd22f3e792579.	N/A	More Details
CVE-2025-7012	An issue in Cato Networks' CatoClient for Linux, before version 5.5, allows a local attacker to escalate privileges to root by exploiting improper symbolic link handling.	N/A	More Details
CVE-2025-38347	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to do sanity check on ino and xnid syzbot reported a f2fs bug as below: INFO: task syz-executor140:5308 blocked for more than 143 seconds. Not tainted 6.14.0-rc7-syzkaller-00069-g81e4f8d68c66 #0 "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. task:syz-executor140 state:D stack:24016 pid:5308 tgid:5308 ppid:5306 task_flags:0x400140 flags:0x00000006 Call Trace: <TASK> context_switch kernel/sched/core.c:5378 [inline] __schedule+0x190e/0x4c90 kernel/sched/core.c:6765 __schedule_loop kernel/sched/core.c:6842 [inline] schedule+0x14b/0x320 kernel/sched/core.c:6857 io_schedule+0x8d/0x110 kernel/sched/core.c:7690 folio_wait_bit_common+0x839/0xee0 mm/filemap.c:1317 __folio_lock mm/filemap.c:1664 [inline] folio_lock include/linux/pagemap.h:1163 [inline] __filemap_get_folio+0x147/0xb40 mm/filemap.c:1917 pagecache_get_page+0x2c/0x130 mm/folio-compat.c:87 find_get_page_flags include/linux/pagemap.h:842 [inline] f2fs_grab_cache_page+0x2b/0x320 fs/f2fs/f2fs.h:2776 __get_node_page+0x131/0x11b0 fs/f2fs/node.c:1463 read_xattr_block+0xfb/0x190 fs/f2fs/xattr.c:306 lookup_all_xattrs fs/f2fs/xattr.c:355 [inline] f2fs_getxattr+0x676/0xf70 fs/f2fs/xattr.c:533 __f2fs_get_acl+0x52/0x870 fs/f2fs/acl.c:179 f2fs_acl_create fs/f2fs/acl.c:375 [inline] f2fs_init_acl+0xd7/0x9b0 fs/f2fs/acl.c:418 f2fs_init_inode_metadata+0xa0f/0x1050 fs/f2fs/dir.c:539 f2fs_add_inline_entry+0x448/0x860 fs/f2fs/inline.c:666 f2fs_add_dentry+0xba/0x1e0 fs/f2fs/dir.c:765 f2fs_do_add_link+0x28c/0x3a0 fs/f2fs/dir.c:808 f2fs_add_link fs/f2fs/f2fs.h:3616 [inline] f2fs_mknod+0x2e8/0x5b0 fs/f2fs/namei.c:766 vfs_mknod+0x36d/0x3b0 fs/namei.c:4191 unix_bind_bsd net/unix/af_unix.c:1286 [inline] unix_bind+0x563/0xe30 net/unix/af_unix.c:1379 __sys_bind_socket net/socket.c:1817 [inline] __sys_bind+0x1e4/0x290 net/socket.c:1848 __do_sys_bind net/socket.c:1853 [inline] __se_sys_bind net/socket.c:1851 [inline] __x64_sys_bind+0x7a/0x90 net/socket.c:1851 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 Let's dump and check metadata of corrupted inode, it shows its xattr_nid is the same to its i_ino. dump.f2fs -i 3 chaseyu.img.raw i_xattr_nid [0x 3 : 3] So that, during mknod in the corrupted directory, it tries to get and lock inode page twice, result in deadlock. - f2fs_mknod - f2fs_add_inline_entry - f2fs_get_inode_page --- lock dir's inode page - f2fs_init_acl - f2fs_acl_create(dir,..) - __f2fs_get_acl - f2fs_getxattr - lookup_all_xattrs - __get_node_page --- try to lock dir's inode page In order to fix this, let's add sanity check on ino and xnid.	N/A	More Details
CVE-2025-53633	Chall-Manager is a platform-agnostic system able to start Challenges on Demand of a player. When decoding a scenario (i.e. a zip archive), the size of the decoded content is not checked, potentially leading to zip bombs decompression. Exploitation does not require authentication nor authorization, so anyone can exploit it. It should nonetheless not be exploitable as it is highly recommended to bury Chall-Manager deep within the infrastructure due to its large capabilities, so no users could reach the system. Patch has been implemented by commit 14042aa and shipped in v0.1.4.	N/A	More Details
CVE-2025-38337	In the Linux kernel, the following vulnerability has been resolved: jbd2: fix data-race and null-ptr-deref in jbd2_journal_dirty_metadata() Since handle->h_transaction may be a NULL pointer, so we should change it to call is_handle_aborted(handle) first before dereferencing it. And the following data-race was reported in my fuzzer: === BUG: KCSAN: data-race in jbd2_journal_dirty_metadata / jbd2_journal_dirty_metadata write to 0xffff888011024104 of 4 bytes by task 10881 on cpu 1: jbd2_journal_dirty_metadata+0x2a5/0x770 fs/jbd2/transaction.c:1556 __ext4_handle_dirty_metadata+0xe7/0x4b0 fs/ext4/ext4_jbd2.c:358 ext4_do_update_inode fs/ext4/inode.c:5220 [inline] ext4_mark_iloc_dirty+0x32c/0xd50 fs/ext4/inode.c:5869 __ext4_mark_inode_dirty+0xe1/0x450 fs/ext4/inode.c:6074 ext4_dirty_inode+0x98/0xc0 fs/ext4/inode.c:6103 .... read to 0xffff888011024104 of 4 bytes by task 10880 on cpu 0: jbd2_journal_dirty_metadata+0xf2/0x770 fs/jbd2/transaction.c:1512 __ext4_handle_dirty_metadata+0xe7/0x4b0 fs/ext4/ext4_jbd2.c:358 ext4_do_update_inode fs/ext4/inode.c:5220 [inline] ext4_mark_iloc_dirty+0x32c/0xd50 fs/ext4/inode.c:5869 __ext4_mark_inode_dirty+0xe1/0x450 fs/ext4/inode.c:6074 ext4_dirty_inode+0x98/0xc0 fs/ext4/inode.c:6103 .... value changed: 0x00000000 -> 0x00000001 === This issue is caused by missing data-race annotation for jh->b_modified. Therefore, the missing annotation needs to be added.	N/A	More Details
CVE-2025-38330	In the Linux kernel, the following vulnerability has been resolved: firmware: cs_dsp: Fix OOB memory read access in KUnit test (ctl cache) KASAN reported out of bounds access - cs_dsp_ctl_cache_init_multiple_offsets(). The code uses mock_coeff_template.length_bytes (4 bytes) for register value allocations. But later, this length is set to 8 bytes which causes test code failures. As fix, just remove the lenght override, keeping the original value 4 for all operations.	N/A	More Details
CVE-2025-38331	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: cortina: Use TOE/TSO on all TCP It is desireable to push the hardware accelerator to also process non-segmented TCP frames: we pass the skb->len to the "TOE/TSO" offloader and it will handle them. Without this quirk the driver becomes unstable and lock up and and crash. I do not know exactly why, but it is probably due to the TOE (TCP offload engine) feature that is coupled with the segmentation feature - it is not possible to turn one part off and not the other, either both TOE and TSO are active, or neither of them. Not having the TOE part active seems detrimental, as if that hardware feature is not really supposed to be turned off. The datasheet says: "Based on packet parsing and TCP connection/NAT table lookup results, the NetEngine puts the packets belonging to the same TCP connection to the same queue for the software to process. The NetEngine puts incoming packets to the buffer or series of buffers for a jumbo packet. With this hardware acceleration, IP/TCP header parsing, checksum validation and connection lookup are offloaded from the software processing." After numerous tests with the hardware locking up after something between minutes and hours depending on load using iperf3 I have concluded this is necessary to stabilize the hardware.	N/A	More Details
CVE-2025-38332	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Use memcpy() for BIOS version The strlcat() with FORTIFY support is triggering a panic because it thinks the target buffer will overflow although the correct target buffer size is passed in. Anyway, instead of memset() with 0 followed by a strlcat(), just use memcpy() and ensure that the resulting buffer is NULL terminated. BIOSVersion is only used for the lpfc_printf_log() which expects a properly terminated string.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to bail out in get_new_segment() ------------[cut here]--------		

CVE-2025-38333	---- WARNING: CPU: 3 PID: 579 at fs/f2fs/segment.c:2832 new_curseg+0x5e8/0x6dc pc : new_curseg+0x5e8/0x6dc Call trace: new_curseg+0x5e8/0x6dc f2fs_allocate_data_block+0xa54/0xe28 do_write_page+0x6c/0x194 f2fs_do_write_node_page+0x38/0x78 __write_node_page+0x248/0x6d4 f2fs_sync_node_pages+0x524/0x72c f2fs_write_checkpoint+0x4bc/0x9b0 __checkpoint_and_complete_reqs+0x80/0x244 issue_checkpoint_thread+0x8c/0xec kthread+0x114/0x1bc ret_from_fork+0x10/0x20 get_new_segment() detects inconsistent status in between free_segmap and free_secmap, let's record such error into super block, and bail out get_new_segment() instead of continue using the segment.	N/A	More Details
CVE-2025-38334	In the Linux kernel, the following vulnerability has been resolved: x86/sgx: Prevent attempts to reclaim poisoned pages TL;DR: SGX page reclaim touches the page to copy its contents to secondary storage. SGX instructions do not gracefully handle machine checks. Despite this, the existing SGX code will try to reclaim pages that it _knows_ are poisoned. Avoid even trying to reclaim poisoned pages. The longer story: Pages used by an enclave only get epc_page->poison set in arch_memory_failure() but they currently stay on sgx_active_page_list until sgx_encl_release(), with the SGX_EPC_PAGE_RECLAIMER_TRACKED flag untouched. epc_page->poison is not checked in the reclaimer logic meaning that, if other conditions are met, an attempt will be made to reclaim an EPC page that was poisoned. This is bad because 1. we don't want that page to end up added to another enclave and 2. it is likely to cause one core to shut down and the kernel to panic. Specifically, reclaiming uses microcode operations including "EWB" which accesses the EPC page contents to encrypt and write them out to non-SGX memory. Those operations cannot handle MCEs in their accesses other than by putting the executing core into a special shutdown state (affecting both threads with HT.) The kernel will subsequently panic on the remaining cores seeing the core didn't enter MCE handler(s) in time. Call sgx_unmark_page_reclaimable() to remove the affected EPC page from sgx_active_page_list on memory error to stop it being considered for reclaiming. Testing epc_page->poison in sgx_reclaim_pages() would also work but I assume it's better to add code in the less likely paths. The affected EPC page is not added to &node->sgx_poison_page_list until later in sgx_encl_release()->sgx_free_epc_page() when it is EREMOVEd. Membership on other lists doesn't change to avoid changing any of the lists' semantics except for sgx_active_page_list. There's a "TBD" comment in arch_memory_failure() about pre-emptive actions, the goal here is not to address everything that it may imply. This also doesn't completely close the time window when a memory error notification will be fatal (for a not previously poisoned EPC page) -- the MCE can happen after sgx_reclaim_pages() has selected its candidates or even *inside* a microcode operation (actually easy to trigger due to the amount of time spent in them.) The spinlock in sgx_unmark_page_reclaimable() is safe because memory_failure() runs in process context and no spinlocks are held, explicitly noted in a mm/memory-failure.c comment.	N/A	More Details
CVE-2025-38335	In the Linux kernel, the following vulnerability has been resolved: Input: gpio-keys - fix a sleep while atomic with PREEMPT_RT When enabling PREEMPT_RT, the gpio_keys_irq_timer() callback runs in hard irq context, but the input_event() takes a spin_lock, which isn't allowed there as it is converted to a rt_spin_lock(). [4054.289999] BUG: sleeping function called from invalid context at kernel/locking/spinlock_rt.c:48 [4054.290028] in_atomic(): 1, irqs_disabled(): 1, non_block: 0, pid: 0, name: swapper/0 ... [4054.290195] __might_resched+0x13c/0x1f4 [4054.290209] rt_spin_lock+0x54/0x11c [4054.290219] input_event+0x48/0x80 [4054.290230] gpio_keys_irq_timer+0x4c/0x78 [4054.290243] __hrtimer_run_queues+0x1a4/0x438 [4054.290257] hrtimer_interrupt+0xe4/0x240 [4054.290269] arch_timer_handler_phys+0x2c/0x44 [4054.290283] handle_percpu_devid_irq+0x8c/0x14c [4054.290297] handle_irq_desc+0x40/0x58 [4054.290307] generic_handle_domain_irq+0x1c/0x28 [4054.290316] gic_handle_irq+0x44/0xcc Considering the gpio_keys_irq_isr() can run in any context, e.g. it can be threaded, it seems there's no point in requesting the timer isr to run in hard irq context. Relax the hrtimer not to use the hard context.	N/A	More Details
CVE-2025-38336	In the Linux kernel, the following vulnerability has been resolved: ata: pata_via: Force PIO for ATAPI devices on VT6415/VT6330 The controller has a hardware bug that can hard hang the system when doing ATAPI DMAs without any trace of what happened. Depending on the device attached, it can also prevent the system from booting. In this case, the system hangs when reading the ATIP from optical media with cdrecord -vvv -atip on an _NEC DVD_RW ND-4571A 1-01 and an Optiarc DVD RW AD-7200A 1.06 attached to an ASRock 990FX Extreme 4, running at UDMA/33. The issue can be reproduced by running the same command with a cygwin build of cdrecord on WinXP, although it requires more attempts to cause it. The hang in that case is also resolved by forcing PIO. It doesn't appear that VIA has produced any drivers for that OS, thus no known workaround exists. HDDs attached to the controller do not suffer from any DMA issues.	N/A	More Details
CVE-2025-38338	In the Linux kernel, the following vulnerability has been resolved: fs/nfs/read: fix double-unlock bug in nfs_return_empty_folio() Sometimes, when a file was read while it was being truncated by another NFS client, the kernel could deadlock because folio_unlock() was called twice, and the second call would XOR back the `PG_locked` flag. Most of the time (depending on the timing of the truncation), nobody notices the problem because folio_unlock() gets called three times, which flips `PG_locked` back off: 1. vfs_read, nfs_read_folio, ... nfs_read_add_folio, nfs_return_empty_folio 2. vfs_read, nfs_read_folio, ... netfs_read_collection, netfs_unlock_abandoned_read_pages 3. vfs_read, ... nfs_do_read_folio, nfs_read_add_folio, nfs_return_empty_folio The problem is that nfs_read_add_folio() is not supposed to unlock the folio if fscache is enabled, and a nfs_netfs_folio_unlock() check is missing in nfs_return_empty_folio(). Rarely this leads to a warning in netfs_read_collection(): ------------[cut here]------------ R=0000031c: folio 10 is not locked WARNING: CPU: 0 PID: 29 at fs/netfs/read_collect.c:133 netfs_read_collection+0x7c0/0xf00 [...] Workqueue: events_unbound netfs_read_collection_worker RIP: 0010:netfs_read_collection+0x7c0/0xf00 [...] Call Trace: <TASK> netfs_read_collection_worker+0x67/0x80 process_one_work+0x12e/0x2c0 worker_thread+0x295/0x3a0 Most of the time, however, processes just get stuck forever in folio_wait_bit_common(), waiting for `PG_locked` to disappear, which never happens because nobody is really holding the folio lock.	N/A	More Details
CVE-2025-38346	In the Linux kernel, the following vulnerability has been resolved: ftrace: Fix UAF when lookup kallsym after ftrace disabled The following issue happens with a buggy module: BUG: unable to handle page fault for address: ffffffffc05d0218 PGD 1bd66f067 P4D 1bd66f067 PUD 1bd671067 PMD 101808067 PTE 0 Oops: Oops: 0000 [#1] SMP KASAN PTI Tainted: [O]=OOT_MODULE, [E]=UNSIGNED_MODULE Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS RIP: 0010:sized_strscpy+0x81/0x2f0 RSP: 0018:ffff88812d76fa08 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffffffffc0601010 RCX: dffffc0000000000 RDX: 0000000000000038 RSI: dffffc0000000000 RDI: ffff88812608da2d RBP: 8080808080808080 R08: ffff88812608da2d R09: ffff88812608da68 R10: ffff88812608d82d R11: ffff88812608d810 R12: 0000000000000038 R13: ffff88812608da2d R14: ffffffffc05d0218 R15: fefefefefefefeff FS: 00007fef552de740(0000) GS:ffff8884251c7000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffffffc05d0218 CR3: 00000001146f0000 CR4: 00000000000006f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ftrace_mod_get_kallsym+0x1ac/0x590 update_iter_mod+0x239/0x5b0 s_next+0x5b/0xa0 seq_read_iter+0x8c9/0x1070 seq_read+0x249/0x3b0 proc_reg_read+0x1b0/0x280 vfs_read+0x17f/0x920 ksys_read+0xf3/0x1c0 do_syscall_64+0x5f/0x2e0 entry_SYSCALL_64_after_hwframe+0x76/0x7e The above issue may happen as follows: (1) Add kprobe tracepoint; (2) insmod test.ko; (3) Module triggers ftrace disabled; (4) rmmod test.ko; (5) cat /proc/kallsyms; --> Will trigger UAF as test.ko already removed; ftrace_mod_get_kallsym() ... strscpy(module_name, mod_map->mod->name, MODULE_NAME_LEN); ... The problem is when a module triggers an issue with ftrace and sets ftrace_disable. The ftrace_disable is set when an anomaly is discovered and to prevent any more damage, ftrace stops all text modification. The issue that happened was that the ftrace_disable stops more than just the text modification. When a module is loaded, its init functions can also be traced. Because kallsyms deletes	N/A	More Details

	the init functions after a module has loaded, ftrace saves them when the module is loaded and function tracing is enabled. This allows the output of the function trace to show the init function names instead of just their raw memory addresses. When a module is removed, ftrace_release_mod() is called, and if ftrace_disable is set, it just returns without doing anything more. The problem here is that it leaves the mod_list still around and if kallsyms is called, it will call into this code and access the module memory that has already been freed as it will return: strscpy(module_name, mod_map->mod->name, MODULE_NAME_LEN); Where the "mod" no longer exists and triggers a UAF bug.		
CVE-2025-38339	In the Linux kernel, the following vulnerability has been resolved: powerpc/bpf: fix JIT code size calculation of bpf trampoline arch_bpf_trampoline_size() provides JIT size of the BPF trampoline before the buffer for JIT'ing it is allocated. The total number of instructions emitted for BPF trampoline JIT code depends on where the final image is located. So, the size arrived at with the dummy pass in arch_bpf_trampoline_size() can vary from the actual size needed in arch_prepare_bpf_trampoline(). When the instructions accounted in arch_bpf_trampoline_size() is less than the number of instructions emitted during the actual JIT compile of the trampoline, the below warning is produced: WARNING: CPU: 8 PID: 204190 at arch/powerpc/net/bpf_jit_comp.c:981 __arch_prepare_bpf_trampoline.isra.0+0xd2c/0xdcc which is: /* Make sure the trampoline generation logic doesn't overflow */ if (image && WARN_ON_ONCE(&image[ctx->idx] > (u32 *)rw_image_end - BPF_INSN_SAFETY)) { So, during the dummy pass, instead of providing some arbitrary image location, account for maximum possible instructions if and when there is a dependency with image location for JIT'ing.	N/A	More Details
CVE-2025-38340	In the Linux kernel, the following vulnerability has been resolved: firmware: cs_dsp: Fix OOB memory read access in KUnit test KASAN reported out of bounds access - cs_dsp_mock_bin_add_name_or_info(), because the source string length was rounded up to the allocation size.	N/A	More Details
CVE-2025-38341	In the Linux kernel, the following vulnerability has been resolved: eth: fbnic: avoid double free when failing to DMA-map FW msg The semantics are that caller of fbnic_mbx_map_msg() retains the ownership of the message on error. All existing callers dutifully free the page.	N/A	More Details
CVE-2025-38342	In the Linux kernel, the following vulnerability has been resolved: software node: Correct a OOB check in software_node_get_reference_args() software_node_get_reference_args() wants to get @index-th element, so the property value requires at least '(index + 1) * sizeof(*ref)' bytes but that can not be guaranteed by current OOB check, and may cause OOB for malformed property. Fix by using as OOB check '((index + 1) * sizeof(*ref) > prop->length)'.	N/A	More Details
CVE-2025-38343	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7996: drop fragments with multicast or broadcast RA IEEE 802.11 fragmentation can only be applied to unicast frames. Therefore, drop fragments with multicast or broadcast RA. This patch addresses vulnerabilities such as CVE-2020-26145.	N/A	More Details
CVE-2025-38344	In the Linux kernel, the following vulnerability has been resolved: ACPICA: fix acpi parse and parseext cache leaks ACPICA commit 8829e70e1360c81e7a5a901b5d4f48330e021ea5 I'm Seunghun Han, and I work for National Security Research Institute of South Korea. I have been doing a research on ACPI and found an ACPI cache leak in ACPI early abort cases. Boot log of ACPI cache leak is as follows: [0.352414] ACPI: Added _OSI(Module Device) [0.353182] ACPI: Added _OSI(Processor Device) [0.353182] ACPI: Added _OSI(3.0 _SCP Extensions) [0.353182] ACPI: Added _OSI(Processor Aggregator Device) [0.356028] ACPI: Unable to start the ACPI Interpreter [0.356799] ACPI Error: Could not remove SCI handler (20170303/evmisc-281) [0.360215] kmem_cache_destroy Acpi-State: Slab cache still has objects [0.360648] CPU: 0 PID: 1 Comm: swapper/0 Tainted: G W 4.12.0-rc4-next-20170608+ #10 [0.361273] Hardware name: innotek gmb_h virtual_box/virtual_box, BIOS virtual_box 12/01/2006 [0.361873] Call Trace: [0.362243] ? dump_stack+0x5c/0x81 [0.362591] ? kmem_cache_destroy+0x1aa/0x1c0 [0.362944] ? acpi_sleep_proc_init+0x27/0x27 [0.363296] ? acpi_os_delete_cache+0xa/0x10 [0.363646] ? acpi_ut_delete_caches+0x6d/0x7b [0.364000] ? acpi_terminate+0xa/0x14 [0.364000] ? acpi_init+0x2af/0x34f [0.364000] ? __class_create+0x4c/0x80 [0.364000] ? video_setup+0x7f/0x7f [0.364000] ? acpi_sleep_proc_init+0x27/0x27 [0.364000] ? do_one_initcall+0x4e/0x1a0 [0.364000] ? kernel_init_freeable+0x189/0x20a [0.364000] ? rest_init+0xc0/0xc0 [0.364000] ? kernel_init+0xa/0x100 [0.364000] ? ret_from_fork+0x25/0x30 I analyzed this memory leak in detail. I found that “Acpi-State” cache and “Acpi-Parse” cache were merged because the size of cache objects was same slab cache size. I finally found “Acpi-Parse” cache and “Acpi-parse_ext” cache were leaked using SLAB_NEVER_MERGE flag in kmem_cache_create() function. Real ACPI cache leak point is as follows: [0.360101] ACPI: Added _OSI(Module Device) [0.360101] ACPI: Added _OSI(Processor Device) [0.360101] ACPI: Added _OSI(3.0 _SCP Extensions) [0.361043] ACPI: Added _OSI(Processor Aggregator Device) [0.364016] ACPI: Unable to start the ACPI Interpreter [0.365061] ACPI Error: Could not remove SCI handler (20170303/evmisc-281) [0.368174] kmem_cache_destroy Acpi-Parse: Slab cache still has objects [0.369332] CPU: 1 PID: 1 Comm: swapper/0 Tainted: G W 4.12.0-rc4-next-20170608+ #8 [0.371256] Hardware name: innotek gmb_h virtual_box/virtual_box, BIOS virtual_box 12/01/2006 [0.372000] Call Trace: [0.372000] ? dump_stack+0x5c/0x81 [0.372000] ? kmem_cache_destroy+0x1aa/0x1c0 [0.372000] ? acpi_sleep_proc_init+0x27/0x27 [0.372000] ? acpi_os_delete_cache+0xa/0x10 [0.372000] ? acpi_ut_delete_caches+0x56/0x7b [0.372000] ? acpi_terminate+0xa/0x14 [0.372000] ? acpi_init+0x2af/0x34f [0.372000] ? __class_create+0x4c/0x80 [0.372000] ? video_setup+0x7f/0x7f [0.372000] ? acpi_sleep_proc_init+0x27/0x27 [0.372000] ? do_one_initcall+0x4e/0x1a0 [0.372000] ? kernel_init_freeable+0x189/0x20a [0.372000] ? rest_init+0xc0/0xc0 [0.372000] ? kernel_init+0xa/0x100 [0.372000] ? ret_from_fork+0x25/0x30 [0.388039] kmem_cache_destroy Acpi-parse_ext: Slab cache still has objects [0.389063] CPU: 1 PID: 1 Comm: swapper/0 Tainted: G W 4.12.0-rc4-next-20170608+ #8 [0.390557] Hardware name: innotek gmb_h virtual_box/virtual_box, BIOS virtual_box 12/01/2006 [0.392000] Call Trace: [0.392000] ? dump_stack+0x5c/0x81 [0.392000] ? kmem_cache_destroy+0x1aa/0x1c0 [0.392000] ? acpi_sleep_proc_init+0x27/0x27 [0.392000] ? acpi_os_delete_cache+0xa/0x10 [0.392000] ? acpi_ut_delete_caches+0x6d/0x7b [0.392000] ? acpi_terminate+0xa/0x14 [0.392000] ? acpi_init+0x2af/0x3 ---truncated---	N/A	More Details
CVE-2025-38345	In the Linux kernel, the following vulnerability has been resolved: ACPICA: fix acpi operand cache leak in dswstate.c ACPICA commit 987a3b5cf7175916e2a4b6ea5b8e70f830dfe732 I found an ACPI cache leak in ACPI early termination and boot continuing case. When early termination occurs due to malicious ACPI table, Linux kernel terminates ACPI function and continues to boot process. While kernel terminates ACPI function, kmem_cache_destroy() reports Acpi-Operand cache leak. Boot log of ACPI operand cache leak is as follows: >[0.585957] ACPI: Added _OSI(Module Device) >[0.587218] ACPI: Added _OSI(Processor Device) >[0.588530] ACPI: Added _OSI(3.0 _SCP Extensions) >[0.589790] ACPI: Added _OSI(Processor Aggregator Device) >[0.591534] ACPI Error: Illegal I/O port address/length above 64K: C806E00000004002/0x2 (20170303/hwvalid-155) >[0.594351] ACPI Exception: AE_LIMIT, Unable to initialize fixed events (20170303/evevent-88) >[0.597858] ACPI: Unable to start the ACPI Interpreter >[0.599162] ACPI Error: Could not remove SCI handler (20170303/evmisc-281) >[0.601836] kmem_cache_destroy Acpi-Operand: Slab cache still has objects >[0.603556] CPU: 0 PID: 1 Comm: swapper/0 Not tainted 4.12.0-rc5 #26 >[0.605159] Hardware name: innotek gmb_h virtual_box/virtual_box, BIOS virtual_box 12/01/2006 >[0.609177] Call Trace: >[0.610063] ? dump_stack+0x5c/0x81 >[0.611118] ? kmem_cache_destroy+0x1aa/0x1c0 >[0.612632] ? acpi_sleep_proc_init+0x27/0x27 >[0.613906] ? acpi_os_delete_cache+0xa/0x10 >[0.617986] ? acpi_ut_delete_caches+0x3f/0x7b >[0.619293] ? acpi_terminate+0xa/0x14 >[0.620394] ? acpi_init+0x2af/0x34f >[0.621616] ? __class_create+0x4c/0x80 >[0.623412] ? video_setup+0x7f/0x7f >[0.624585] ?	N/A	More Details

	acpi_sleep_proc_init+0x27/0x27 >[0.625861] ? do_one_initcall+0x4e/0x1a0 >[0.627513] ? kernel_init_freeable+0x19e/0x21f >[0.628972] ? rest_init+0x80/0x80 >[0.630043] ? kernel_init+0xa/0x100 >[0.631084] ? ret_from_fork+0x25/0x30 >[0.633343] vgaarb: loaded >[0.635036] EDAC MC: Ver: 3.0.0 >[0.638601] PCI: Probing PCI hardware >[0.639833] PCI host bridge to bus 0000:00 >[0.641031] pci_bus 0000:00: root bus resource [io 0x0000-0xffff] > ... Continue to boot and log is omitted ... I analyzed this memory leak in detail and found acpi_ds_obj_stack_pop_and_ delete() function miscalculated the top of the stack. acpi_ds_obj_stack_push() function uses walk_state->operand_index for start position of the top, but acpi_ds_obj_stack_pop_and_delete() function considers index 0 for it. Therefore, this causes acpi operand memory leak. This cache leak causes a security threat because an old kernel (<= 4.9) shows memory locations of kernel functions in stack dump. Some malicious users could use this information to neutralize kernel ASLR. I made a patch to fix ACPI operand cache leak.		
CVE-2025-53632	Chall-Manager is a platform-agnostic system able to start Challenges on Demand of a player. When decoding a scenario (i.e. a zip archive), the path of the file to write is not checked, potentially leading to zip slips. Exploitation does not require authentication nor authorization, so anyone can exploit it. It should nonetheless not be exploitable as it is highly recommended to bury Chall-Manager deep within the infrastructure due to its large capabilities, so no users could reach the system. Patch has been implemented by commit 47d188f and shipped in v0.1.4.	N/A	More Details
CVE-2025-53634	Chall-Manager is a platform-agnostic system able to start Challenges on Demand of a player. The HTTP Gateway processes headers, but with no timeout set. With a slow loris attack, an attacker could cause Denial of Service (DoS). Exploitation does not require authentication nor authorization, so anyone can exploit it. It should nonetheless not be exploitable as it is highly recommended to bury Chall-Manager deep within the infrastructure due to its large capabilities, so no users could reach the system. Patch has been implemented by commit 1385bd8 and shipped in v0.1.4.	N/A	More Details
CVE-2025-53623	The Job Iteration API is an an extension for ActiveJob that make jobs interruptible and resumable Versions prior to 1.11.0 have an arbitrary code execution vulnerability in the `CsvEnumerator` class. This vulnerability can be exploited by an attacker to execute arbitrary commands on the system where the application is running, potentially leading to unauthorized access, data leakage, or complete system compromise. The issue is fixed in versions `1.11.0` and above. Users can mitigate the risk by avoiding the use of untrusted input in the `CsvEnumerator` class and ensuring that any file paths are properly sanitized and validated before being passed to the class methods. Users should avoid using the `count_of_rows_in_file` method with untrusted CSV filenames.	N/A	More Details
CVE-2025-50121	A CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that could cause unauthenticated remote code execution when a malicious folder is created over the web interface HTTP when enabled. HTTP is disabled by default.	N/A	More Details
CVE-2025-7503	An OEM IP camera manufactured by Shenzhen Liandian Communication Technology LTD exposes a Telnet service (port 23) with undocumented, default credentials. The Telnet service is enabled by default and is not disclosed or configurable via the device’s web interface or user manual. An attacker with network access can authenticate using default credentials and gain root-level shell access to the device. The affected firmware version is AppFHE1_V1.0.6.0 (Kernel: KerFHE1_PTZ_WIFI_V3.1.1, Hardware: HwFHE1_WF6_PTZ_WIFI_20201218). No official fix or firmware update is available, and the vendor could not be contacted. This vulnerability allows for remote code execution and privilege escalation.	N/A	More Details
CVE-2025-30025	The communication protocol used between the server process and the service control had a flaw that could lead to a local privilege escalation.	N/A	More Details
CVE-2025-30026	The AXIS Camera Station Server had a flaw that allowed to bypass authentication that is normally required.	N/A	More Details
CVE-2025-5028	Installation file of ESET security products on Windows allow an attacker to misuse to delete an arbitrary file without having the permissions to do so.	N/A	More Details
CVE-2025-5992	When passing values outside of the expected range to QColorTransferGenericFunction it can cause a denial of service, for example, this can happen when passing a specifically crafted ICC profile to QColorSpace::fromICCProfile.This issue affects Qt from 6.6.0 through 6.8.3, from 6.9.0 through 6.9.1. This is fixed in 6.8.4 and 6.9.2.	N/A	More Details
CVE-2025-6438	A CWE-611: Improper Restriction of XML External Entity Reference vulnerability exists that could cause manipulation of SOAP API calls and XML external entities injection resulting in unauthorized file access when the server is accessed via the network using an application account.	N/A	More Details
CVE-2025-3933	A Regular Expression Denial of Service (ReDoS) vulnerability was discovered in the Hugging Face Transformers library, specifically within the DonutProcessor class's `token2json()` method. This vulnerability affects versions 4.50.3 and earlier, and is fixed in version 4.52.1. The issue arises from the regex pattern `<s_(.*?)>` which can be exploited to cause excessive CPU consumption through crafted input strings due to catastrophic backtracking. This vulnerability can lead to service disruption, resource exhaustion, and potential API service vulnerabilities, impacting document processing tasks using the Donut model.	N/A	More Details
CVE-2025-43856	immich is a high performance self-hosted photo and video management solution. Prior to 1.132.0, immich is vulnerable to account hijacking through oauth2, because the state parameter is not being checked. The oauth2 state parameter is similar to a csrf token, so when the user starts the login flow this unpredictable token is generated and somehow saved in the browser session and passed to the identity provider, which will return the state parameter when redirecting the user back to immich. Before the user is logged in that parameter needs to be verified to make sure the login was actively initiated by the user in this browser session. On it's own, this wouldn't be too bad, but when immich uses the /user-settings page as a redirect_uri, it will automatically link the accounts if the user was already logged in. This means that if someone has an immich instance with a public oauth provider (like google), an attacker can - for example - embed a hidden iframe in a webpage or even just send the victim a forged oauth login url with a code that logs the victim into the attackers oauth account and redirects back to immich and links the accounts. After this, the attacker can log into the victims account using their own oauth credentials. This vulnerability is fixed in 1.132.0.	N/A	More Details
CVE-2025-53851	Rejected reason: Not used	N/A	More Details
CVE-	Meshtastic is an open source mesh networking solution. Prior to 2.5.1, traceroute responses from the remote node are not rate limited. Given that there are SNR measurements attributed to each received transmission, this is a guaranteed way to get a remote		

2024-47065	station to reliably and continuously respond. You could easily get 100 samples in a short amount of time (estimated 2 minutes), whereas passively doing the same could take hours or days. There are secondary effects that non-ratelimited traceroute does also allow a 2:1 reflected DoS of the network as well, but these concerns are less than the problem with positional confidentiality (other DoS routes exist). This vulnerability is fixed in 2.5.1.	N/A	More Details
CVE-2025-50122	A CWE-331: Insufficient Entropy vulnerability exists that could cause root password discovery when the password generation algorithm is reverse engineered with access to installation or upgrade artifacts.	N/A	More Details
CVE-2025-50123	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists that could cause remote command execution by a privileged account when the server is accessed via a console and through exploitation of the hostname input.	N/A	More Details
CVE-2025-50124	A CWE-269: Improper Privilege Management vulnerability exists that could cause privilege escalation when the server is accessed by a privileged account via a console and through exploitation of a setup script.	N/A	More Details
CVE-2025-50125	A CWE-918: Server-Side Request Forgery (SSRF) vulnerability exists that could cause unauthenticated remote code execution when the server is accessed via the network with knowledge of hidden URLs and manipulation of host request header.	N/A	More Details
CVE-2025-6788	A CWE-668: Exposure of Resource to Wrong Sphere vulnerability exists that exposes TGML diagram resources to the wrong control sphere, providing other authenticated users with potentially inappropriate access to TGML diagrams.	N/A	More Details
CVE-2025-34077	An authentication bypass vulnerability exists in the WordPress Pie Register plugin ≤ 3.7.1.4 that allows unauthenticated attackers to impersonate arbitrary users by submitting a crafted POST request to the login endpoint. By setting social_site=true and manipulating the user_id_social_site parameter, an attacker can generate a valid WordPress session cookie for any user ID, including administrators. Once authenticated, the attacker may exploit plugin upload functionality to install a malicious plugin containing arbitrary PHP code, resulting in remote code execution on the underlying server.	N/A	More Details
CVE-2025-53852	Rejected reason: Not used	N/A	More Details
CVE-2025-53850	Rejected reason: Not used	N/A	More Details
CVE-2025-7021	Fullscreen API Spoofing and UI Redressing in the handling of Fullscreen API and UI rendering in OpenAI Operator SaaS on Web allows a remote attacker to capture sensitive user input (e.g., login credentials, email addresses) via displaying a deceptive fullscreen interface with overlaid fake browser controls and a distracting element (like a cookie consent screen) to obscure fullscreen notifications, tricking the user into interacting with the malicious site.	N/A	More Details
CVE-2025-53878	Rejected reason: Not used	N/A	More Details
CVE-2025-4662	Brocade SANnav before SANnav 2.4.0a logs plaintext passphrases in the Brocade SANnav host server audit logs while executing OpenSSL command using a passphrase from the command line or while providing the passphrase through a temporary file. These audit logs are the local server VM’s audit logs and are not controlled by SANnav. These logs are only visible to the server admin of the host server and are not visible to the SANnav admin or any SANnav user.	N/A	More Details
CVE-2025-6390	Brocade SANnav before SANnav 2.4.0a logs passwords and pbe keys in the Brocade SANnav server audit logs after installation and under specific conditions. These audit logs are the local server VM’s audit logs and are not controlled by SANnav. These logs are only visible to the server admin of the host server and are not visible to the SANnav admin or any SANnav user.	N/A	More Details
CVE-2025-6392	Brocade SANnav before Brocade SANnav 2.4.0a could log database passwords in clear text in audit logs when the daily data dump collector invokes docker exec commands. These audit logs are the local server VM’s audit logs and are not controlled by SANnav. These logs are only visible to the server admin of the host server and are not visible to the SANnav admin or any SANnav user.	N/A	More Details
CVE-2024-38648	A hardcoded secret in Ivanti DSM before 2024.2 allows an authenticated attacker on an adjacent network to decrypt sensitive data including user credentials.	N/A	More Details
CVE-2023-39339	A vulnerability exists on all versions of Ivanti Policy Secure below 22.6R1 where an authenticated administrator can perform an arbitrary file read via a maliciously crafted web request.	N/A	More Details
CVE-2023-39338	Enables an authenticated user (enrolled device) to access a service protected by Sentry even if they are not authorized according to the sentry policy to access that service. It does not enable the user to authenticate to or use the service, it just provides the tunnel access.	N/A	More Details
CVE-2025-53879	Rejected reason: Not used	N/A	More Details
CVE-2025-53877	Rejected reason: Not used	N/A	More Details
CVE-2025-53849	Rejected reason: Not used	N/A	More Details

CVE-2025-53876	Rejected reason: Not used	N/A	More Details
CVE-2025-53875	Rejected reason: Not used	N/A	More Details
CVE-2025-53874	Rejected reason: Not used	N/A	More Details
CVE-2025-53873	Rejected reason: Not used	N/A	More Details
CVE-2025-53872	Rejected reason: Not used	N/A	More Details
CVE-2025-53871	Rejected reason: Not used	N/A	More Details
CVE-2025-53848	Rejected reason: Not used	N/A	More Details
CVE-2025-38329	In the Linux kernel, the following vulnerability has been resolved: firmware: cs_dsp: Fix OOB memory read access in KUnit test (wmfw info) KASAN reported out of bounds access - cs_dsp_mock_wmfw_add_info(), because the source string length was rounded up to the allocation size.	N/A	More Details
CVE-2025-38328	In the Linux kernel, the following vulnerability has been resolved: jffs2: check jffs2_prealloc_raw_node_refs() result in few other places Fuzzing hit another invalid pointer dereference due to the lack of checking whether jffs2_prealloc_raw_node_refs() completed successfully. Subsequent logic implies that the node refs have been allocated. Handle that. The code is ready for propagating the error upwards. KASAN: null-ptr-deref in range [0x0000000000000008-0x000000000000000f] CPU: 1 PID: 5835 Comm: syz-executor145 Not tainted 5.10.234-syzkaller #0 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.12.0-1 04/01/2014 RIP: 0010:jffs2_link_node_ref+0xac/0x690 fs/jffs2/nodelist.c:600 Call Trace: jffs2_mark_erased_block fs/jffs2/erase.c:460 [inline] jffs2_erase_pending_blocks+0x688/0x1860 fs/jffs2/erase.c:118 jffs2_garbage_collect_pass+0x638/0x1a00 fs/jffs2/gc.c:253 jffs2_reserve_space+0x3f4/0xad0 fs/jffs2/nodemgmt.c:167 jffs2_write_inode_range+0x246/0xb50 fs/jffs2/write.c:362 jffs2_write_end+0x712/0x1110 fs/jffs2/file.c:302 generic_perform_write+0x2c2/0x500 mm/filemap.c:3347 __generic_file_write_iter+0x252/0x610 mm/filemap.c:3465 generic_file_write_iter+0xdb/0x230 mm/filemap.c:3497 call_write_iter include/linux/fs.h:2039 [inline] do_iter_readv_writev+0x46d/0x750 fs/read_write.c:740 do_iter_write+0x18c/0x710 fs/read_write.c:866 vfs_writev+0x1db/0x6a0 fs/read_write.c:939 do_pwritev fs/read_write.c:1036 [inline] __do_sys_pwritev fs/read_write.c:1083 [inline] __se_sys_pwritev fs/read_write.c:1078 [inline] __x64_sys_pwritev+0x235/0x310 fs/read_write.c:1078 do_syscall_64+0x30/0x40 arch/x86/entry/common.c:46 entry_SYSCALL_64_after_hwframe+0x67/0xd1 Found by Linux Verification Center (linuxtesting.org) with Syzkaller.	N/A	More Details
CVE-2025-38327	In the Linux kernel, the following vulnerability has been resolved: fgraph: Do not enable function_graph tracer when setting funcgraph-args When setting the funcgraph-args option when function graph tracer is net enabled, it incorrectly enables it. Worse, it unregisters itself when it was never registered. Then when it gets enabled again, it will register itself a second time causing a WARNing. ~# echo 1 > /sys/kernel/tracing/options/funcgraph-args ~# head -20 /sys/kernel/tracing/trace # tracer: nop # # entries-in-buffer/entries-written: 813/26317372 #P:8 # # _-----=> irqs-off/BH-disabled # / _----=> need-resched # | / _---=> hardirq/softirq # || / _--=> preempt-depth # ||| / _-=> migrate-disable # |||| / delay # TASK-PID CPU# ||||| TIMESTAMP FUNCTION # | | | ||||| | | <idle>-0 [007] d..4. 358.966010: 7) 1.692 us | fetch_next_timer_interrupt(basej=4294981640, basem=357956000000, base_local=0xffff88823c3ae040, base_global=0xffff88823c3af300, tevt=0xffff888100e47cb8); <idle>-0 [007] d..4. 358.966012: 7) | tmigr_cpu_deactivate(nextexp=357988000000) { <idle>-0 [007] d..4. 358.966013: 7) | _raw_spin_lock(lock=0xffff88823c3b2320) { <idle>-0 [007] d..4. 358.966014: 7) 0.981 us | preempt_count_add(val=1); <idle>-0 [007] d..5. 358.966017: 7) 1.058 us | do_raw_spin_lock(lock=0xffff88823c3b2320); <idle>-0 [007] d..4. 358.966019: 7) 5.824 us | } <idle>-0 [007] d..5. 358.966021: 7) | tmigr_inactive_up(group=0xffff888100cb9000, child=0x0, data=0xffff888100e47bc0) { <idle>-0 [007] d..5. 358.966022: 7) | tmigr_update_events(group=0xffff888100cb9000, child=0x0, data=0xffff888100e47bc0) { Notice the "tracer: nop" at the top there. The current tracer is the "nop" tracer, but the content is obviously the function graph tracer. Enabling function graph tracing will cause it to register again and trigger a warning in the accounting: ~# echo function_graph > /sys/kernel/tracing/current_tracer -bash: echo: write error: Device or resource busy With the dmesg of: ------------[cut here]------------ WARNING: CPU: 7 PID: 1095 at kernel/trace/ftrace.c:3509 ftrace_startup_subops+0xc1e/0x1000 Modules linked in: kvm_intel kvm irqbypass CPU: 7 UID: 0 PID: 1095 Comm: bash Not tainted 6.16.0-rc2-test-00006-gea03de4105d3 #24 PREEMPT Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 RIP: 0010:ftrace_startup_subops+0xc1e/0x1000 Code: 48 b8 22 01 00 00 00 00 ad de 49 89 84 24 88 01 00 00 8b 44 24 08 89 04 24 e9 c3 f7 ff ff c7 04 24 ed ff ff ff e9 b7 f7 ff ff <0f> 0b c7 04 24 f0 ff ff ff e9 a9 f7 ff ff c7 04 24 f4 ff ff ff e9 RSP: 0018:ffff888133cff948 EFLAGS: 00010202 RAX: 0000000000000001 RBX: 1ffff1102679ff31 RCX: 0000000000000000 RDX: 1ffffffff0b27a60 RSI: ffffffff8593d2f0 RDI: ffffffff85941140 RBP: 00000000000c2041 R08: ffffffffffffffff R09: ffffed1020240221 R10: ffff88810120110f R11: ffffed1020240214 R12: ffffffff8593d2f0 R13: ffffffff8593d300 R14: ffffffff85941140 R15: ffffffff85631100 FS: 00007f7ec6f28740(0000) GS:ffff8882b5251000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f7ec6f181c0 CR3: 000000012f1d0005 CR4: 0000000000172ef0 Call Trace: <TASK> ? __pfx_ftrace_startup_subops+0x10/0x10 ? find_held_lock+0x2b/0x80 ? ftrace_stub_direct_tramp+0x10/0x10 ? ftrace_stub_direct_tramp+0x10/0x10 ? trace_preempt_on+0xd0/0x110 ? __pfx_trace_graph_entry_args+0x10/ ---truncated---	N/A	More Details
CVE-2025-38282	In the Linux kernel, the following vulnerability has been resolved: kernfs: Relax constraint in draining guard The active reference lifecycle provides the break/unbreak mechanism but the active reference is not truly active after unbreak -- callers don't use it afterwards but it's important for proper pairing of kn->active counting. Assuming this mechanism is in place, the WARN check in kernfs_should_drain_open_files() is too sensitive -- it may transiently catch those (rightful) callers between kernfs_unbreak_active_protection() and kernfs_put_active() as found out by Chen Ridong: kernfs_remove_by_name_ns kernfs_get_active // active=1 __kernfs_remove // active=0x80000002 kernfs_drain ... wait_event //waiting (active == 0x80000001)	N/A	More Details

	kernfs_break_active_protection // active = 0x80000001 // continue kernfs_unbreak_active_protection // active = 0x80000002 ... kernfs_should_drain_open_files // warning occurs kernfs_put_active To avoid the false positives (mind panic_on_warn) remove the check altogether. (This is meant as quick fix, I think active reference break/unbreak may be simplified with larger rework.)		
CVE-2025-38276	In the Linux kernel, the following vulnerability has been resolved: fs/dax: Fix "don't skip locked entries when scanning entries" Commit 6be3e21d25ca ("fs/dax: don't skip locked entries when scanning entries") introduced a new function, wait_entry_unlocked_exclusive(), which waits for the current entry to become unlocked without advancing the XArray iterator state. Waiting for the entry to become unlocked requires dropping the XArray lock. This requires calling xas_pause() prior to dropping the lock which leaves the xas in a suitable state for the next iteration. However this has the side-effect of advancing the xas state to the next index. Normally this isn't an issue because xas_for_each() contains code to detect this state and thus avoid advancing the index a second time on the next loop iteration. However both callers of and wait_entry_unlocked_exclusive() itself subsequently use the xas state to reload the entry. As xas_pause() updated the state to the next index this will cause the current entry which is being waited on to be skipped. This caused the following warning to fire intermittently when running xftest generic/068 on an XFS filesystem with FS DAX enabled: [35.067397] ------------[cut here]------------ [35.068229] WARNING: CPU: 21 PID: 1640 at mm/truncate.c:89 truncate_folio_batch_exceptionals+0xd8/0x1e0 [35.069717] Modules linked in: nd_pmem dax_pmem nd_btt nd_e820 libnvdimm [35.071006] CPU: 21 UID: 0 PID: 1640 Comm: fstest Not tainted 6.15.0-rc7+ #77 PREEMPT(voluntary) [35.072613] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/204 [35.074845] RIP: 0010:truncate_folio_batch_exceptionals+0xd8/0x1e0 [35.075962] Code: a1 00 00 00 f6 47 0d 20 0f 84 97 00 00 00 4c 63 e8 41 39 c4 7f 0b eb 61 49 83 c5 01 45 39 ec 7e 58 42 f68 [35.079522] RSP: 0018:ffffb04e426c7850 EFLAGS: 00010202 [35.080359] RAX: 0000000000000000 RBX: ffff9d21e3481908 RCX: ffffb04e426c77f4 [35.081477] RDX: ffffb04e426c79e8 RSI: ffffb04e426c79e0 RDI: ffff9d21e34816e8 [35.082590] RBP: ffffb04e426c79e0 R08: 0000000000000001 R09: 0000000000000003 [35.083733] R10: 0000000000000000 R11: 822b53c0f7a49868 R12: 000000000000001f [35.084850] R13: 0000000000000000 R14: ffffb04e426c78e8 R15: fffffffffffffffe [35.085953] FS: 00007f9134c87740(0000) GS:ffff9d22abba0000(0000) knlGS:0000000000000000 [35.087346] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [35.088244] CR2: 00007f9134c86000 CR3: 000000040afff000 CR4: 00000000000006f0 [35.089354] Call Trace: [35.089749] <TASK> [35.090168] truncate_inode_pages_range+0xfc/0x4d0 [35.091078] truncate_pagecache+0x47/0x60 [35.091735] xfs_setattr_size+0xc7/0x3e0 [35.092648] xfs_vn_setattr+0x1ea/0x270 [35.093437] notify_change+0x1f4/0x510 [35.094219] ? do_truncate+0x97/0xe0 [35.094879] do_truncate+0x97/0xe0 [35.095640] path_openat+0xabd/0xca0 [35.096278] do_filp_open+0xd7/0x190 [35.096860] do_sys_openat2+0x8a/0xe0 [35.097459] __x64_sys_openat+0x6d/0xa0 [35.098076] do_syscall_64+0xbb/0x1d0 [35.098647] entry_SYSCALL_64_after_hwframe+0x77/0x7f [35.099444] RIP: 0033:0x7f9134d81fc1 [35.100033] Code: 75 57 89 f0 25 00 00 41 00 3d 00 00 41 00 74 49 80 3d 2a 26 0e 00 00 74 6d 89 da 48 89 ee bf 9c ff ff ff5 [35.102993] RSP: 002b:00007ffcd41e0d10 EFLAGS: 00000202 ORIG_RAX: 0000000000000101 [35.104263] RAX: ffffffffffffffda RBX: 0000000000000242 RCX: 00007f9134d81fc1 [35.105452] RDX: 0000000000000242 RSI: 00007ffcd41e1200 RDI: 00000000ffffff9c [35.106663] RBP: 00007ffcd41e1200 R08: 0000000000000000 R09: 0000000000000064 [35.107923] R10: 00000000000001a4 R11: 0000000000000202 R12: 0000000000000066 [35.109112] R13: 0000000000100000 R14: 0000000000100000 R15: 0000000000000400 [35.110357] </TASK> [35.110769] irq event stamp: 8415587 [35.111486] hardirqs last enabled at (8415599): [<ffffffff8d74b562>] __up_console_se ---truncated---	N/A	[More Details]()
CVE-2025-7618	A stored Cross-Site Scripting (XSS) vulnerability vulnerability was found in the File Explorer and Text Editor of ADM. An attacker could exploit this vulnerability to inject malicious scripts into the applications, which may then access cookies or other sensitive information retained by the browser and used with the affected applications. Affected products and versions include: from ADM 4.1.0 to ADM 4.3.3.RH61 as well as ADM 5.0.0.RIN1 and earlier, and Text Editor 1.0.0.r112 and earlier.	N/A	[More Details]()
CVE-2025-38277	In the Linux kernel, the following vulnerability has been resolved: mtd: nand: ecc-mxic: Fix use of uninitialized variable ret If ctx->steps is zero, the loop processing ECC steps is skipped, and the variable ret remains uninitialized. It is later checked and returned, which leads to undefined behavior and may cause unpredictable results in user space or kernel crashes. This scenario can be triggered in edge cases such as misconfigured geometry, ECC engine misuse, or if ctx->steps is not validated after initialization. Initialize ret to zero before the loop to ensure correct and safe behavior regardless of the ctx->steps value. Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	[More Details]()
CVE-2025-38278	In the Linux kernel, the following vulnerability has been resolved: octeontx2-pf: QOS: Refactor TC_HTB_LEAF_DEL_LAST callback This patch addresses below issues, 1. Active traffic on the leaf node must be stopped before its send queue is reassigned to the parent. This patch resolves the issue by marking the node as 'Inner'. 2. During a system reboot, the interface receives TC_HTB_LEAF_DEL and TC_HTB_LEAF_DEL_LAST callbacks to delete its HTB queues. In the case of TC_HTB_LEAF_DEL_LAST, although the same send queue is reassigned to the parent, the current logic still attempts to update the real number of queues, leadning to below warnings New queues can't be registered after device unregistration. WARNING: CPU: 0 PID: 6475 at net/core/net-sysfs.c:1714 netdev_queue_update_kobjects+0x1e4/0x200	N/A	[More Details]()
CVE-2025-38279	In the Linux kernel, the following vulnerability has been resolved: bpf: Do not include stack ptr register in precision backtracking bookkeeping Yi Lai reported an issue ([1]) where the following warning appears in kernel dmesg: [60.643604] verifier backtracking bug [60.643635] WARNING: CPU: 10 PID: 2315 at kernel/bpf/verifier.c:4302 __mark_chain_precision+0x3a6c/0x3e10 [60.648428] Modules linked in: bpf_testmod(OE) [60.650471] CPU: 10 UID: 0 PID: 2315 Comm: test_progs Tainted: G OE 6.15.0-rc4-gef11287f8289-dirty #327 PREEMPT(full) [60.654385] Tainted: [O]=OOT_MODULE, [E]=UNSIGNED_MODULE [60.656682] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-prebuilt.qemu.org 04/01/2014 [60.660475] RIP: 0010:__mark_chain_precision+0x3a6c/0x3e10 [60.662814] Code: 5a 30 84 89 ea e8 c4 d9 01 00 80 3d 3e 7d d8 04 00 0f 85 60 fa ff ff c6 05 31 7d d8 04 01 48 c7 c7 00 58 30 84 e8 c4 06 a5 ff <0f> 0b e9 46 fa ff ff 48 ... [60.668720] RSP: 0018:ffff888116cc7298 EFLAGS: 00010246 [60.671075] RAX: 54d70e82dfd31900 RBX: ffff888115b65e20 RCX: 0000000000000000 [60.673659] RDX: 0000000000000001 RSI: 0000000000000004 RDI: 00000000ffffffff [60.676241] RBP: 0000000000000400 R08: ffff8881f6f23bd3 R09: 1ffff1103ede477a [60.678787] R10: dffffc0000000000 R11: ffffed103ede477b R12: ffff888115b60ae8 [60.681420] R13: 1ffff11022b6cbc4 R14: 00000000fffffff2 R15: 0000000000000001 [60.684030] FS: 00007fc2aedd80c0(0000) GS:ffff88826fa8a000(0000) knlGS:0000000000000000 [60.686837] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [60.689027] CR2: 000056325369e000 CR3: 000000011088b002 CR4: 0000000000370ef0 [60.691623] Call Trace: [60.692821] <TASK> [60.693960] ? __pfx_verbose+0x10/0x10 [60.695656] ? __pfx_disasm_kfunc_name+0x10/0x10 [60.697495] check_cond_jmp_op+0x16f7/0x39b0 [60.699237] do_check+0x58fa/0xab10 ... Further analysis shows the warning is at line 4302 as below: 4294 /* static subprog call instruction, which 4295 * means that we are exiting current subprog, 4296 * so only r1-r5 could be still requested as 4297 * precise, r0 and r6-r10 or any stack slot in 4298 * the current frame should be zero by now 4299 */ 4300 if (bt_reg_mask(bt) & ~BPF_REGMASK_ARGS) { 4301 verbose(env, "BUG regs %x\n", bt_reg_mask(bt)); 4302 WARN_ONCE(1, "verifier backtracking bug"); 4303 return -EFAULT; 4304 } With the below test (also in the next patch): __used __naked static void __bpf_jmp_r10(void) { asm volatile ("r2 = 2314885393468386424 ll;" "goto +0;" "if r2 <= r10 goto +3;" "if r1 >= -1835016 goto +0;" "if r2 <= 8 goto +0;" "if r3 <= 0 goto +0;" "exit;" ::: __clobber_all); } SEC("?raw_tp") __naked void bpf_jmp_r10(void) { asm volatile ("r3 = 0 ll;" "call __bpf_jmp_r10;" "r0 = 0;" "exit;" ::: __clobber_all); } The following is the verifier failure log: 0: (18) r3 = 0x0 ; R3_w=0 2: (85) call pc+2 caller: R10=fp0 callee: frame1: R1=ctx() R3_w=0 R10=fp0 5: frame1: R1=ctx() R3_w=0 R10=fp0 ; asm	N/A	[More Details]()

	volatile (" \ @ verifier_precision.c:184 5: (18) r2 = 0x20202000256c6c78 ; frame1: R2_w=0x20202000256c6c78 7: (05) goto pc+0 8: (bd) if r2 <= r10 goto pc+3 ; frame1: R2_w=0x20202000256c6c78 R10=fp0 9: (35) if r1 >= 0xffe3fff8 goto pc+0 ; frame1: R1=ctx() 10: (b5) if r2 <= 0x8 goto pc+0 mark_precise: frame1: last_idx 10 first_idx 0 subseq_idx -1 mark_precise: frame1: regs=r2 stack= before 9: (35) if r1 >= 0xffe3fff8 goto pc+0 mark_precise: frame1: regs=r2 stack= before 8: (bd) if r2 <= r10 goto pc+3 mark_preci ---truncated---		
CVE-2025-38280	In the Linux kernel, the following vulnerability has been resolved: bpf: Avoid __bpf_prog_ret0_warn when jit fails syzkaller reported an issue: WARNING: CPU: 3 PID: 217 at kernel/bpf/core.c:2357 __bpf_prog_ret0_warn+0xa/0x20 kernel/bpf/core.c:2357 Modules linked in: CPU: 3 UID: 0 PID: 217 Comm: kworker/u32:6 Not tainted 6.15.0-rc4-syzkaller-00040-g8bac8898fe39 RIP: 0010:__bpf_prog_ret0_warn+0xa/0x20 kernel/bpf/core.c:2357 Call Trace: <TASK> bpf_dispatcher_nop_func include/linux/bpf.h:1316 [inline] __bpf_prog_run include/linux/filter.h:718 [inline] bpf_prog_run include/linux/filter.h:725 [inline] cls_bpf_classify+0x74a/0x1110 net/sched/cls_bpf.c:105 ... When creating bpf program, 'fp->jit_requested' depends on bpf_jit_enable. This issue is triggered because of CONFIG_BPF_JIT_ALWAYS_ON is not set and bpf_jit_enable is set to 1, causing the arch to attempt JIT the prog, but jit failed due to FAULT_INJECTION. As a result, incorrectly treats the program as valid, when the program runs it calls `__bpf_prog_ret0_warn` and triggers the WARN_ON_ONCE(1).	N/A	More Details
CVE-2025-38281	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7996: Add NULL check in mt7996_thermal_init devm_kasprintf() can return a NULL pointer on failure,but this returned value in mt7996_thermal_init() is not checked. Add NULL check in mt7996_thermal_init(), to handle kernel NULL pointer dereference error.	N/A	More Details
CVE-2025-38283	In the Linux kernel, the following vulnerability has been resolved: hisi_acc_vfio_pci: bugfix live migration function without VF device driver If the VF device driver is not loaded in the Guest OS and we attempt to perform device data migration, the address of the migrated data will be NULL. The live migration recovery operation on the destination side will access a null address value, which will cause access errors. Therefore, live migration of VMs without added VF device drivers does not require device data migration. In addition, when the queue address data obtained by the destination is empty, device queue recovery processing will not be performed.	N/A	More Details
CVE-2025-38273	In the Linux kernel, the following vulnerability has been resolved: net: tipc: fix refcount warning in tipc_aead_encrypt syzbot reported a refcount warning [1] caused by calling get_net() on a network namespace that is being destroyed (refcount=0). This happens when a TIPC discovery timer fires during network namespace cleanup. The recently added get_net() call in commit e279024617134 ("net/tipc: fix slab-use-after-free Read in tipc_aead_encrypt_done") attempts to hold a reference to the network namespace. However, if the namespace is already being destroyed, its refcount might be zero, leading to the use-after-free warning. Replace get_net() with maybe_get_net(), which safely checks if the refcount is non-zero before incrementing it. If the namespace is being destroyed, return -ENODEV early, after releasing the bearer reference. [1]: https://lore.kernel.org/all/68342b55.a70a0220.253bc2.0091.GAE@google.com/T/#m12019cf9ae77e1954f666914640efa36d52704a2	N/A	More Details
CVE-2025-38284	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: pci: configure manual DAC mode via PCI config API only To support 36-bit DMA, configure chip proprietary bit via PCI config API or chip DBI interface. However, the PCI device mmap isn't set yet and the DBI is also inaccessible via mmap, so only if the bit can be accessible via PCI config API, chip can support 36-bit DMA. Otherwise, fallback to 32-bit DMA. With NULL mmap address, kernel throws trace: BUG: unable to handle page fault for address: 0000000000001090 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 0 P4D 0 Oops: Oops: 0002 [#1] PREEMPT SMP PTI CPU: 1 UID: 0 PID: 71 Comm: irq/26-pciehp Tainted: G OE 6.14.2-061402-generic #202504101348 Tainted: [O]=OOT_MODULE, [E]=UNSIGNED_MODULE RIP: 0010:rtw89_pci_ops_write16+0x12/0x30 [rtw89_pci] RSP: 0018:ffffb0ffc0acf9d8 EFLAGS: 00010206 RAX: ffffffffc158f9c0 RBX: ffff94865e702020 RCX: 0000000000000000 RDX: 0000000000000718 RSI: 0000000000001090 RDI: ffff94865e702020 RBP: ffffb0ffc0acf9d8 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: 0000000000000015 R13: 0000000000000719 R14: ffffb0ffc0acfa1f R15: ffffffffc1813060 FS: 0000000000000000(0000) GS:ffff9486f3480000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000001090 CR3: 0000000090440001 CR4: 00000000000626f0 Call Trace: <TASK> rtw89_pci_read_config_byte+0x6d/0x120 [rtw89_pci] rtw89_pci_cfg_dac+0x5b/0xb0 [rtw89_pci] rtw89_pci_probe+0xa96/0xbd0 [rtw89_pci] ? __pfx___device_attach_driver+0x10/0x10 ? __pfx___device_attach_driver+0x10/0x10 local_pci_probe+0x47/0xa0 pci_call_probe+0x5d/0x190 pci_device_probe+0xa7/0x160 really_probe+0xf9/0x370 ? pm_runtime_barrier+0x55/0xa0 __driver_probe_device+0x8c/0x140 driver_probe_device+0x24/0xd0 __device_attach_driver+0xcd/0x170 bus_for_each_drv+0x99/0x100 __device_attach+0xb4/0x1d0 device_attach+0x10/0x20 pci_bus_add_device+0x59/0x90 pci_bus_add_devices+0x31/0x80 pciehp_configure_device+0xaa/0x170 pciehp_enable_slot+0xd6/0x240 pciehp_handle_presence_or_link_change+0xf1/0x180 pciehp_ist+0x162/0x1c0 irq_thread_fn+0x24/0x70 irq_thread+0xef/0x1c0 ? __pfx_irq_thread_fn+0x10/0x10 ? __pfx_irq_thread_dtor+0x10/0x10 ? __pfx_irq_thread+0x10/0x10 kthread+0xfc/0x230 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x47/0x70 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK>	N/A	More Details
CVE-2025-38285	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix WARN() in get_bpf_raw_tp_regs syzkaller reported an issue: WARNING: CPU: 3 PID: 5971 at kernel/trace/bpf_trace.c:1861 get_bpf_raw_tp_regs+0xa4/0x100 kernel/trace/bpf_trace.c:1861 Modules linked in: CPU: 3 UID: 0 PID: 5971 Comm: syz-executor205 Not tainted 6.15.0-rc5-syzkaller-00038-g707df3375124 #0 PREEMPT(full) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2~bpo12+1 04/01/2014 RIP: 0010:get_bpf_raw_tp_regs+0xa4/0x100 kernel/trace/bpf_trace.c:1861 RSP: 0018:ffffc90003636fa8 EFLAGS: 00010293 RAX: 0000000000000000 RBX: 0000000000000003 RCX: ffffffff81c6bc4c RDX: ffff888032efc880 RSI: ffffffff81c6bc83 RDI: 0000000000000005 RBP: ffff88806a730860 R08: 0000000000000005 R09: 0000000000000003 R10: 0000000000000004 R11: 0000000000000000 R12: 0000000000000004 R13: 0000000000000001 R14: ffffc90003637008 R15: 0000000000000900 FS: 0000000000000000(0000) GS:ffff8880d6cdf000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f7baee09130 CR3: 0000000029f5a000 CR4: 0000000000352ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ____bpf_get_stack_raw_tp kernel/trace/bpf_trace.c:1934 [inline] bpf_get_stack_raw_tp+0x24/0x160 kernel/trace/bpf_trace.c:1931 bpf_prog_ec3b2eefa702d8d3+0x43/0x47 bpf_dispatcher_nop_func include/linux/bpf.h:1316 [inline] __bpf_prog_run include/linux/filter.h:718 [inline] bpf_prog_run include/linux/filter.h:725 [inline] __bpf_trace_run kernel/trace/bpf_trace.c:2363 [inline] bpf_trace_run3+0x23f/0x5a0 kernel/trace/bpf_trace.c:2405 __bpf_trace_mmap_lock_acquire_returned+0xfc/0x140 include/trace/events/mmap_lock.h:47 __traceiter_mmap_lock_acquire_returned+0x79/0xc0 include/trace/events/mmap_lock.h:47 __do_trace_mmap_lock_acquire_returned include/trace/events/mmap_lock.h:47 [inline] trace_mmap_lock_acquire_returned include/trace/events/mmap_lock.h:47 [inline] __mmap_lock_do_trace_acquire_returned+0x138/0x1f0 mm/mmap_lock.c:35 __mmap_lock_trace_acquire_returned include/linux/mmap_lock.h:36 [inline] mmap_read_trylock include/linux/mmap_lock.h:204 [inline] stack_map_get_build_id_offset+0x535/0x6f0 kernel/bpf/stackmap.c:157 __bpf_get_stack+0x307/0xa10 kernel/bpf/stackmap.c:483 ____bpf_get_stack kernel/bpf/stackmap.c:499 [inline] bpf_get_stack+0x32/0x40 kernel/bpf/stackmap.c:496 ____bpf_get_stack_raw_tp kernel/trace/bpf_trace.c:1941 [inline] bpf_get_stack_raw_tp+0x124/0x160 kernel/trace/bpf_trace.c:1931	N/A	More Details

	bpf_prog_ec3b2eefa702d8d3+0x43/0x47 Tracepoint like trace_mmap_lock_acquire_returned may cause nested call as the corner case show above, which will be resolved with more general method in the future. As a result, WARN_ON_ONCE will be triggered. As Alexei suggested, remove the WARN_ON_ONCE first.		
CVE-2025-38286	In the Linux kernel, the following vulnerability has been resolved: pinctrl: at91: Fix possible out-of-boundary access at91_gpio_probe() doesn't check that given OF alias is not available or something went wrong when trying to get it. This might have consequences when accessing gpio_chips array with that value as an index. Note, that BUG() can be compiled out and hence won't actually perform the required checks.	N/A	More Details
CVE-2025-38287	In the Linux kernel, the following vulnerability has been resolved: IB/cm: Drop lockdep assert and WARN when freeing old msg The send completion handler can run after cm_id has advanced to another message. The cm_id lock is not needed in this case, but a recent change re-used cm_free_priv_msg(), which asserts that the lock is held and WARNs if the cm_id's currently outstanding msg is different than the one being freed.	N/A	More Details
CVE-2025-38288	In the Linux kernel, the following vulnerability has been resolved: scsi: smartpqi: Fix smp_processor_id() call trace for preemptible kernels Correct kernel call trace when calling smp_processor_id() when called in preemptible kernels by using raw_smp_processor_id(). smp_processor_id() checks to see if preemption is disabled and if not, issue an error message followed by a call to dump_stack(). Brief example of call trace: kernel: check_preemption_disabled: 436 callbacks suppressed kernel: BUG: using smp_processor_id() in preemptible [00000000] code: kworker/u1025:0/2354 kernel: caller is pqi_scsi_queue_command+0x183/0x310 [smartpqi] kernel: CPU: 129 PID: 2354 Comm: kworker/u1025:0 kernel: ... kernel: Workqueue: writeback wb_workfn (flush-253:0) kernel: Call Trace: kernel: <TASK> kernel: dump_stack_lvl+0x34/0x48 kernel: check_preemption_disabled+0xdd/0xe0 kernel: pqi_scsi_queue_command+0x183/0x310 [smartpqi] kernel: ...	N/A	More Details
CVE-2024-26293	The Avid Nexis Agent uses a vulnerable gSOAP version. An undocumented vulnerability impacting gSOAP v2.8 makes the application vulnerable to an Unauthenticated Path Traversal vulnerability. This issue affects Avid NEXIS E-series: before 2025.5.1; Avid NEXIS F-series: before 2025.5.1; Avid NEXIS PRO+: before 2025.5.1; System Director Appliance (SDA+): before 2025.5.1.	N/A	More Details
CVE-2025-38289	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Avoid potential ndlp use-after-free in dev_loss_tmo_callbk Smatch detected a potential use-after-free of an ndlp oject in dev_loss_tmo_callbk during driver unload or fatal error handling. Fix by reordering code to avoid potential use-after-free if initial nodelist reference has been previously removed.	N/A	More Details
CVE-2025-38274	In the Linux kernel, the following vulnerability has been resolved: fpga: fix potential null pointer deref in fpga_mgr_test_img_load_sgt() fpga_mgr_test_img_load_sgt() allocates memory for sgt using kunit_kzalloc() however it does not check if the allocation failed. It then passes sgt to sg_alloc_table(), which passes it to __sg_alloc_table(). This function calls memset() on sgt in an attempt to zero it out. If the allocation fails then sgt will be NULL and the memset will trigger a NULL pointer dereference. Fix this by checking the allocation with KUNIT_ASSERT_NOT_ERR_OR_NULL().	N/A	More Details
CVE-2025-38272	In the Linux kernel, the following vulnerability has been resolved: net: dsa: b53: do not enable EEE on bcm63xx BCM63xx internal switches do not support EEE, but provide multiple RGMII ports where external PHYs may be connected. If one of these PHYs are EEE capable, we may try to enable EEE for the MACs, which then hangs the system on access of the (non-existent) EEE registers. Fix this by checking if the switch actually supports EEE before attempting to configure it.	N/A	More Details
CVE-2025-38326	In the Linux kernel, the following vulnerability has been resolved: aoe: clean device rq_list in aoedev_downdev() An aoe device's rq_list contains accepted block requests that are waiting to be transmitted to the aoe target. This queue was added as part of the conversion to blk_mq. However, the queue was not cleaned out when an aoe device is downed which caused blk_mq_freeze_queue() to sleep indefinitely waiting for those requests to complete, causing a hang. This fix cleans out the queue before calling blk_mq_freeze_queue().	N/A	More Details
CVE-2025-53751	Rejected reason: Not used	N/A	More Details
CVE-2025-0141	An incorrect privilege assignment vulnerability in the Palo Alto Networks GlobalProtect™ App on enables a locally authenticated non administrative user to escalate their privileges to root on macOS and Linux or NT AUTHORITY\SYSTEM on Windows. The GlobalProtect app on iOS, Android, Chrome OS and GlobalProtect UWP app are not affected.	N/A	More Details
CVE-2025-0646	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-53746	Rejected reason: Not used	N/A	More Details
CVE-2025-53747	Rejected reason: Not used	N/A	More Details
CVE-2025-53748	Rejected reason: Not used	N/A	More Details
CVE-2025-53749	Rejected reason: Not used	N/A	More Details
CVE-2025-53750	Rejected reason: Not used	N/A	More Details
CVE-2025-53752	Rejected reason: Not used	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net: prevent a NULL deref in rtnl_create_link() At the time		

CVE-2025-38271	rtnl_create_link() is running, dev->netdev_ops is NULL, we must not use netdev_lock_ops() or risk a NULL deref if CONFIG_NET_SHAPER is defined. Use netif_set_group() instead of dev_set_group(). RIP: 0010:netdev_need_ops_lock include/net/netdev_lock.h:33 [inline] RIP: 0010:netdev_lock_ops include/net/netdev_lock.h:41 [inline] RIP: 0010:dev_set_group+0xc0/0x230 net/core/dev_api.c:82 Call Trace: <TASK> rtnl_create_link+0x748/0xd10 net/core/rtnetlink.c:3674 rtnl_newlink_create+0x25c/0xb00 net/core/rtnetlink.c:3813 __rtnl_newlink net/core/rtnetlink.c:3940 [inline] rtnl_newlink+0x16d6/0x1c70 net/core/rtnetlink.c:4055 rtnetlink_rcv_msg+0x7cf/0xb70 net/core/rtnetlink.c:6944 netlink_rcv_skb+0x208/0x470 net/netlink/af_netlink.c:2534 netlink_unicast_kernel net/netlink/af_netlink.c:1313 [inline] netlink_unicast+0x75b/0x8d0 net/netlink/af_netlink.c:1339 netlink_sendmsg+0x805/0xb30 net/netlink/af_netlink.c:1883 sock_sendmsg_nosec net/socket.c:712 [inline]	N/A	More Details
CVE-2025-53753	Rejected reason: Not used	N/A	More Details
CVE-2025-38265	In the Linux kernel, the following vulnerability has been resolved: serial: jsm: fix NPE during jsm_uart_port_init No device was set which caused serial_base_ctrl_add to crash. BUG: kernel NULL pointer dereference, address: 0000000000000050 Oops: Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 16 UID: 0 PID: 368 Comm: (udev-worker) Not tainted 6.12.25-amd64 #1 Debian 6.12.25-1 RIP: 0010:serial_base_ctrl_add+0x96/0x120 Call Trace: <TASK> serial_core_register_port+0x1a0/0x580 ? __setup_irq+0x39c/0x660 ? __kmalloc_cache_noprof+0x111/0x310 jsm_uart_port_init+0xe8/0x180 [jsm] jsm_probe_one+0x1f4/0x410 [jsm] local_pci_probe+0x42/0x90 pci_device_probe+0x22f/0x270 really_probe+0xdb/0x340 ? pm_runtime_barrier+0x54/0x90 ? __pfx___driver_attach+0x10/0x10 __driver_probe_device+0x78/0x110 driver_probe_device+0x1f/0xa0 __driver_attach+0xba/0x1c0 bus_for_each_dev+0x8c/0xe0 bus_add_driver+0x112/0x1f0 driver_register+0x72/0xd0 jsm_init_module+0x36/0xff0 [jsm] ? __pfx_jsm_init_module+0x10/0x10 [jsm] do_one_initcall+0x58/0x310 do_init_module+0x60/0x230 Tested with Digi Neo PCIe 8 port card.	N/A	More Details
CVE-2025-38266	In the Linux kernel, the following vulnerability has been resolved: pinctrl: mediatek: eint: Fix invalid pointer dereference for v1 platforms Commit 3ef9f710efcb ("pinctrl: mediatek: Add EINT support for multiple addresses") introduced an access to the 'soc' field of struct mtk_pinctrl in mtk_eint_do_init() and for that an include of pinctrl-mtk-common-v2.h. However, pinctrl drivers relying on the v1 common driver include pinctrl-mtk-common.h instead, which provides another definition of struct mtk_pinctrl that does not contain an 'soc' field. Since mtk_eint_do_init() can be called both by v1 and v2 drivers, it will now try to dereference an invalid pointer when called on v1 platforms. This has been observed on Genio 350 EVK (MT8365), which crashes very early in boot (the kernel trace can only be seen with earlycon). In order to fix this, since 'struct mtk_pinctrl' was only needed to get a 'struct mtk_eint_pin', make 'struct mtk_eint_pin' a parameter of mtk_eint_do_init() so that callers need to supply it, removing mtk_eint_do_init()'s dependency on any particular 'struct mtk_pinctrl'.	N/A	More Details
CVE-2025-38267	In the Linux kernel, the following vulnerability has been resolved: ring-buffer: Do not trigger WARN_ON() due to a commit_overrun When reading a memory mapped buffer the reader page is just swapped out with the last page written in the write buffer. If the reader page is the same as the commit buffer (the buffer that is currently being written to) it was assumed that it should never have missed events. If it does, it triggers a WARN_ON_ONCE(). But there just happens to be one scenario where this can legitimately happen. That is on a commit_overrun. A commit overrun is when an interrupt preempts an event being written to the buffer and then the interrupt adds so many new events that it fills and wraps the buffer back to the commit. Any new events would then be dropped and be reported as "missed_events". In this case, the next page to read is the commit buffer and after the swap of the reader page, the reader page will be the commit buffer, but this time there will be missed events and this triggers the following warning: ------------[cut here]------------ WARNING: CPU: 2 PID: 1127 at kernel/trace/ring_buffer.c:7357 ring_buffer_map_get_reader+0x49a/0x780 Modules linked in: kvm_intel kvm irqbypass CPU: 2 UID: 0 PID: 1127 Comm: trace-cmd Not tainted 6.15.0-rc7-test-00004-g478bc2824b45-dirty #564 PREEMPT Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 RIP: 0010:ring_buffer_map_get_reader+0x49a/0x780 Code: 00 00 00 48 89 fe 48 c1 ee 03 80 3c 2e 00 0f 85 ec 01 00 00 4d 3b a6 a8 00 00 00 0f 85 8a fd ff ff 48 85 c0 0f 84 55 fe ff ff <0f> 0b e9 4e fe ff ff be 08 00 00 00 4c 89 54 24 58 48 89 54 24 50 RSP: 0018:ffff888121787dc0 EFLAGS: 00010002 RAX: 00000000000006a2 RBX: ffff888100062800 RCX: ffffffff8190cb49 RDX: ffff888126934c00 RSI: 1ffff11020200a15 RDI: ffff8881010050a8 RBP: dffffc0000000000 R08: 0000000000000000 R09: ffffed1024d26982 R10: ffff888126934c17 R11: ffff8881010050a8 R12: ffff888126934c00 R13: ffff8881010050b8 R14: ffff888101005000 R15: ffff888126930008 FS: 00007f95c8cd7540(0000) GS:ffff8882b576e000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f95c8de4dc0 CR3: 0000000128452002 CR4: 0000000000172ef0 Call Trace: <TASK> ? __pfx_ring_buffer_map_get_reader+0x10/0x10 tracing_buffers_ioctl+0x283/0x370 __x64_sys_ioctl+0x134/0x190 do_syscall_64+0x79/0x1c0 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7f95c8de48db Code: 00 48 89 44 24 18 31 c0 48 8d 44 24 60 c7 04 24 10 00 00 00 48 89 44 24 08 48 8d 44 24 20 48 89 44 24 10 b8 10 00 00 00 0f 05 <89> c2 3d 00 f0 ff ff 77 1c 48 8b 44 24 18 64 48 2b 04 25 28 00 00 RSP: 002b:00007ffe037ba110 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 00007ffe037bb2b0 RCX: 00007f95c8de48db RDX: 0000000000000000 RSI: 0000000000005220 RDI: 0000000000000006 RBP: 00007ffe037ba180 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007ffe037bb6f8 R14: 00007f95c9065000 R15: 00005575c7492c90 </TASK> irq event stamp: 5080 hardirqs last enabled at (5079): [<ffffffff83e0adb0>] _raw_spin_unlock_irqrestore+0x50/0x70 hardirqs last disabled at (5080): [<ffffffff83e0aa83>] _raw_spin_lock_irqsave+0x63/0x70 softirqs last enabled at (4182): [<ffffffff81516122>] handle_softirqs+0x552/0x710 softirqs last disabled at (4159): [<ffffffff815163f7>] __irq_exit_rcu+0x107/0x210 ---[end trace 0000000000000000]--- The above was triggered by running on a kernel with both lockdep and KASAN as well as kmemleak enabled and executing the following command: # perf record -o perf-test.dat -a -- trace-cmd record --nosplice -e all -p function hackbench 50 With perf interjecting a lot of interrupts and trace-cmd enabling all events as well as function tracing, with lockdep, KASAN and kmemleak enabled, it could cause an interrupt preempting an event being written to add enough event ---truncated---	N/A	More Details
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: usb: typec: tcpm: move tcpm_queue_vdm_unlocked to asynchronous work A state check was previously added to tcpm_queue_vdm_unlocked to prevent a deadlock where the DisplayPort Alt Mode driver would be executing work and attempting to grab the tcpm_lock while the TCPM was holding the lock and attempting to unregister the altmode, blocking on the altmode driver's cancel_work_sync call. Because the state check isn't protected, there is a small window where the Alt Mode driver could determine that the TCPM is in a ready state and attempt to grab the lock while the TCPM grabs the lock and changes the TCPM state to one that causes the deadlock. The callstack is provided below: [110121.667392][C7] Call trace: [110121.667396][C7] __switch_to+0x174/0x338 [110121.667406][C7] __schedule+0x608/0x9f0 [110121.667414][C7] schedule+0x7c/0xe8 [110121.667423][C7] kernfs_drain+0xb0/0x114 [110121.667431][C7] __kernfs_remove+0x16c/0x20c [110121.667436][C7] kernfs_remove_by_name_ns+0x74/0xe8 [110121.667442][C7] sysfs_remove_group+0x84/0xe8 [110121.667450][C7] sysfs_remove_groups+0x34/0x58 [110121.667458][C7] device_remove_groups+0x10/0x20 [110121.667464][C7] device_release_driver_internal+0x164/0x2e4 [110121.667475][C7] device_release_driver+0x18/0x28 [110121.667484][C7] bus_remove_device+0xec/0x118 [110121.667491][C7] device_del+0x1e8/0x4ac [110121.667498][C7] device_unregister+0x18/0x38 [110121.667504][C7]	N/A	More

38268	typec_unregister_altmode+0x30/0x44 [110121.667515][C7] tcpm_reset_port+0xac/0x370 [110121.667523][C7] tcpm_snk_detach+0x84/0xb8 [110121.667529][C7] run_state_machine+0x4c0/0x1b68 [110121.667536][C7] tcpm_state_machine_work+0x94/0xe4 [110121.667544][C7] kthread_worker_fn+0x10c/0x244 [110121.667552][C7] kthread+0x104/0x1d4 [110121.667557][C7] ret_from_fork+0x10/0x20 [110121.667689][C7] Workqueue: events dp_altmode_work [110121.667697][C7] Call trace: [110121.667701][C7] __switch_to+0x174/0x338 [110121.667710][C7] __schedule+0x608/0x9f0 [110121.667717][C7] schedule+0x7c/0xe8 [110121.667725][C7] schedule_preempt_disabled+0x24/0x40 [110121.667733][C7] __mutex_lock+0x408/0xdac [110121.667741][C7] __mutex_lock_slowpath+0x14/0x24 [110121.667748][C7] mutex_lock+0x40/0xec [110121.667757][C7] tcpm_altmode_enter+0x78/0xb4 [110121.667764][C7] typec_altmode_enter+0xdc/0x10c [110121.667769][C7] dp_altmode_work+0x68/0x164 [110121.667775][C7] process_one_work+0x1e4/0x43c [110121.667783][C7] worker_thread+0x25c/0x430 [110121.667789][C7] kthread+0x104/0x1d4 [110121.667794][C7] ret_from_fork+0x10/0x20 Change tcpm_queue_vdm_unlocked to queue for tcpm_queue_vdm_work, which can perform the state check while holding the TCPM lock while the Alt Mode lock is no longer held. This requires a new struct to hold the vdm data, altmode_vdm_event.		Details
CVE-2025-38269	In the Linux kernel, the following vulnerability has been resolved: btrfs: exit after state insertion failure at btrfs_convert_extent_bit() If insert_state() state failed it returns an error pointer and we call extent_io_tree_panic() which will trigger a BUG() call. However if CONFIG_BUG is disabled, which is an uncommon and exotic scenario, then we fallthrough and call cache_state() which will dereference the error pointer, resulting in an invalid memory access. So jump to the 'out' label after calling extent_io_tree_panic(), it also makes the code more clear besides dealing with the exotic scenario where CONFIG_BUG is disabled.	N/A	More Details
CVE-2025-38270	In the Linux kernel, the following vulnerability has been resolved: net: drv: netdevsim: don't napi_complete() from netpoll netdevsim supports netpoll. Make sure we don't call napi_complete() from it, since it may not be scheduled. Breno reports hitting a warning in napi_complete_done(): WARNING: CPU: 14 PID: 104 at net/core/dev.c:6592 napi_complete_done+0x2cc/0x560 __napi_poll+0x2d8/0x3a0 handle_softirqs+0x1fe/0x710 This is presumably after netpoll stole the SCHED bit prematurely.	N/A	More Details
CVE-2025-38290	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix node corruption in ar->arvifs list In current WLAN recovery code flow, ath12k_core_halt() only reinitializes the "arvifs" list head. This will cause the list node immediately following the list head to become an invalid list node. Because the prev of that node still points to the list head "arvifs", but the next of the list head "arvifs" no longer points to that list node. When a WLAN recovery occurs during the execution of a vif removal, and it happens before the spin_lock_bh(&ar->data_lock) in ath12k_mac_vdev_delete(), list_del() will detect the previously mentioned situation, thereby triggering a kernel panic. The fix is to remove and reinitialize all vif list nodes from the list head "arvifs" during WLAN halt. The reinitialization is to make the list nodes valid, ensuring that the list_del() in ath12k_mac_vdev_delete() can execute normally. Call trace: __list_del_entry_valid_or_report+0xd4/0x100 (P) ath12k_mac_remove_link_interface.isra.0+0xf8/0x2e4 [ath12k] ath12k_scan_vdev_clean_work+0x40/0x164 [ath12k] cfg80211_wiphy_work+0xfc/0x100 process_one_work+0x164/0x2d0 worker_thread+0x254/0x380 kthread+0xfc/0x100 ret_from_fork+0x10/0x20 The change is mostly copied from the ath11k patch: https://lore.kernel.org/all/20250320053145.3445187-1-quic_stonez@quicinc.com/ Tested-on: QCN9274 hw2.0 PCI WLAN.WBE.1.4.1-00199-QCAHKSWPL_SILICONZ-1	N/A	More Details
CVE-2025-38291	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: Prevent sending WMI commands to firmware during firmware crash Currently, we encounter the following kernel call trace when a firmware crash occurs. This happens because the host sends WMI commands to the firmware while it is in recovery, causing the commands to fail and resulting in the kernel call trace. Set the ATH12K_FLAG_CRASH_FLUSH and ATH12K_FLAG_RECOVERY flags when the host driver receives the firmware crash notification from MHI. This prevents sending WMI commands to the firmware during recovery. Call Trace: <TASK> dump_stack_lvl+0x75/0xc0 register_lock_class+0x6be/0x7a0 ? __lock_acquire+0x644/0x19a0 __lock_acquire+0x95/0x19a0 lock_acquire+0x265/0x310 ? ath12k_ce_send+0xa2/0x210 [ath12k] ? find_held_lock+0x34/0xa0 ? ath12k_ce_send+0x56/0x210 [ath12k] _raw_spin_lock_bh+0x33/0x70 ? ath12k_ce_send+0xa2/0x210 [ath12k] ath12k_ce_send+0xa2/0x210 [ath12k] ath12k_htc_send+0x178/0x390 [ath12k] ath12k_wmi_cmd_send_nowait+0x76/0xa0 [ath12k] ath12k_wmi_cmd_send+0x62/0x190 [ath12k] ath12k_wmi_pdev_bss_chan_info_request+0x62/0xc0 [ath1 ath12k_mac_op_get_survey+0x2be/0x310 [ath12k] ieee80211_dump_survey+0x99/0x240 [mac80211] nl80211_dump_survey+0xe7/0x470 [cfg80211] ? kmalloc_reserve+0x59/0xf0 genl_dumpit+0x24/0x70 netlink_dump+0x177/0x360 __netlink_dump_start+0x206/0x280 genl_family_rcv_msg_dumpit.isra.22+0x8a/0xe0 ? genl_family_rcv_msg_attrs_parse.isra.23+0xe0/0xe0 ? genl_op_lock.part.12+0x10/0x10 ? genl_dumpit+0x70/0x70 genl_rcv_msg+0x1d0/0x290 ? nl80211_del_station+0x330/0x330 [cfg80211] ? genl_get_cmd_both+0x50/0x50 netlink_rcv_skb+0x4f/0x100 genl_rcv+0x1f/0x30 netlink_unicast+0x1b6/0x260 netlink_sendmsg+0x31a/0x450 __sock_sendmsg+0xa8/0xb0 ____sys_sendmsg+0x1e4/0x260 ___sys_sendmsg+0x89/0xe0 ? local_clock_noinstr+0xb/0xc0 ? rcu_is_watching+0xd/0x40 ? kfree+0x1de/0x370 ? __sys_sendmsg+0x7a/0xc0 Tested-on: QCN9274 hw2.0 PCI WLAN.WBE.1.4.1-00199-QCAHKSWPL_SILICONZ-1	N/A	More Details
CVE-2025-38292	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix invalid access to memory In ath12k_dp_rx_msdu_coalesce(), rxcb is fetched from skb and boolean is_continuation is part of rxcb. Currently, after freeing the skb, the rxcb->is_continuation accessed again which is wrong since the memory is already freed. This might lead use-after-free error. Hence, fix by locally defining bool is_continuation from rxcb, so that after freeing skb, is_continuation can be used. Compile tested only.	N/A	More Details
CVE-2025-38317	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: Fix buffer overflow in debugfs If the user tries to write more than 32 bytes then it results in memory corruption. Fortunately, this is debugfs so it's limited to root users.	N/A	More Details
CVE-2025-38310	In the Linux kernel, the following vulnerability has been resolved: seg6: Fix validation of nexthop addresses The kernel currently validates that the length of the provided nexthop address does not exceed the specified length. This can lead to the kernel reading uninitialized memory if user space provided a shorter length than the specified one. Fix by validating that the provided length exactly matches the specified one.	N/A	More Details
CVE-2025-38311	In the Linux kernel, the following vulnerability has been resolved: iavf: get rid of the crit lock Get rid of the crit lock. That frees us from the error prone logic of try_locks. Thanks to netdev_lock() by Jakub it is now easy, and in most cases we were protected by it already - replace crit lock by netdev lock when it was not the case. Lockdep reports that we should cancel the work under crit_lock [splat1], and that was the scheme we have mostly followed since [1] by Slawomir. But when that is done we still got into deadlocks [splat2]. So instead we should look at the bigger problem, namely "weird locking/scheduling" of the iavf. The first step to fix that is to remove the crit lock. I will followup with a -next series that simplifies scheduling/tasks. Cancel the work without netdev lock (weird unlock+lock scheme), to fix the [splat2] (which would be totally ugly if we would kept the crit lock). Extend protected part of iavf_watchdog_task() to include scheduling more work. Note that the removed comment in iavf_reset_task() was misplaced, it belonged to inside of the removed if condition, so it's gone now. [splat1] - w/o this patch - The deadlock during VF removal: WARNING: possible circular locking dependency detected sh/3825 is trying to acquire lock: ((work_completion)(&(&adapter-	N/A	More Details

	>watchdog_task)->work)){+.+.}-{0:0}, at: start_flush_work+0x1a1/0x470 but task is already holding lock: (&adapter->crit_lock){+.+.}-{4:4}, at: iavf_remove+0xd1/0x690 [iavf] which lock already depends on the new lock. [splat2] - when cancelling work under crit lock, w/o this series, see [2] for the band aid attempt WARNING: possible circular locking dependency detected sh/3550 is trying to acquire lock: ((wq_completion)iavf){+.+.}-{0:0}, at: touch_wq_lockdep_map+0x26/0x90 but task is already holding lock: (&dev->lock){+.+.}-{4:4}, at: iavf_remove+0xa6/0x6e0 [iavf] which lock already depends on the new lock. [1] fc2e6b3b132a ("iavf: Rework mutexes for better synchronisation") [2] https://github.com/pkitszel/linux/commit/52dddbfc2bb60294083f5711a158a		
CVE-2025-38312	In the Linux kernel, the following vulnerability has been resolved: fbdev: core: fbcvt: avoid division by 0 in fb_cvt_hperiod() In fb_find_mode_cvt(), iff mode->refresh somehow happens to be 0x80000000, cvt.f_refresh will become 0 when multiplying it by 2 due to overflow. It's then passed to fb_cvt_hperiod(), where it's used as a divider -- division by 0 will result in kernel oops. Add a sanity check for cvt.f_refresh to avoid such overflow... Found by Linux Verification Center (linuxtesting.org) with the Svace static analysis tool.	N/A	More Details
CVE-2025-38313	In the Linux kernel, the following vulnerability has been resolved: bus: fsl-mc: fix double-free on mc_dev The blamed commit tried to simplify how the deallocations are done but, in the process, introduced a double-free on the mc_dev variable. In case the MC device is a DPRC, a new mc_bus is allocated and the mc_dev variable is just a reference to one of its fields. In this circumstance, on the error path only the mc_bus should be freed. This commit introduces back the following checkpatch warning which is a false-positive. WARNING: kfree(NULL) is safe and this check is probably not required + if (mc_bus) + kfree(mc_bus);	N/A	More Details
CVE-2025-38314	In the Linux kernel, the following vulnerability has been resolved: virtio-pci: Fix result size returned for the admin command completion The result size returned by virtio_pci_admin_dev_parts_get() is 8 bytes larger than the actual result data size. This occurs because the result_sg_size field of the command is filled with the result length from virtqueue_get_buf(), which includes both the data size and an additional 8 bytes of status. This oversized result size causes two issues: 1. The state transferred to the destination includes 8 bytes of extra data at the end. 2. The allocated buffer in the kernel may be smaller than the returned size, leading to failures when reading beyond the allocated size. The commit fixes this by subtracting the status size from the result of virtqueue_get_buf(). This fix has been tested through live migrations with virtio-net, virtio-net-transitional, and virtio-blk devices.	N/A	More Details
CVE-2025-38315	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btintel: Check dsbr size from EFI variable Since the size of struct btintel_dsbr is already known, we can just start there instead of querying the EFI variable size. If the final result doesn't match what we expect also fail. This fixes a stack buffer overflow when the EFI variable is larger than struct btintel_dsbr.	N/A	More Details
CVE-2025-38316	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7996: avoid NULL pointer dereference in mt7996_set_monitor() The function mt7996_set_monitor() dereferences phy before the NULL sanity check. Fix this to avoid NULL pointer dereference by moving the dereference after the check.	N/A	More Details
CVE-2025-38318	In the Linux kernel, the following vulnerability has been resolved: perf: arm-ni: Fix missing platform_set_drvdata() Add missing platform_set_drvdata in arm_ni_probe(), otherwise calling platform_get_drvdata() in remove returns NULL.	N/A	More Details
CVE-2025-38293	In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: fix node corruption in ar->arvifs list In current WLAN recovery code flow, ath11k_core_halt() only reinitializes the "arvifs" list head. This will cause the list node immediately following the list head to become an invalid list node. Because the prev of that node still points to the list head "arvifs", but the next of the list head "arvifs" no longer points to that list node. When a WLAN recovery occurs during the execution of a vif removal, and it happens before the spin_lock_bh(&ar->data_lock) in ath11k_mac_op_remove_interface(), list_del() will detect the previously mentioned situation, thereby triggering a kernel panic. The fix is to remove and reinitialize all vif list nodes from the list head "arvifs" during WLAN halt. The reinitialization is to make the list nodes valid, ensuring that the list_del() in ath11k_mac_op_remove_interface() can execute normally. Call trace: __list_del_entry_valid_or_report+0xb8/0xd0 ath11k_mac_op_remove_interface+0xb0/0x27c [ath11k] drv_remove_interface+0x48/0x194 [mac80211] ieee80211_do_stop+0x6e0/0x844 [mac80211] ieee80211_stop+0x44/0x17c [mac80211] __dev_close_many+0xac/0x150 __dev_change_flags+0x194/0x234 dev_change_flags+0x24/0x6c devinet_ioctl+0x3a0/0x670 inet_ioctl+0x200/0x248 sock_do_ioctl+0x60/0x118 sock_ioctl+0x274/0x35c __arm64_sys_ioctl+0xac/0xf0 invoke_syscall+0x48/0x114 ... Tested-on: QCA6698AQ hw2.1 PCI WLAN.HSP.1.1-04591-QCAHSPSWPL_V1_V2_SILICONZ_IOE-1	N/A	More Details
CVE-2025-38319	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pp: Fix potential NULL pointer dereference in atomctrl_initialize_mc_reg_table The function atomctrl_initialize_mc_reg_table() and atomctrl_initialize_mc_reg_table_v2_2() does not check the return value of smu_atom_get_data_table(). If smu_atom_get_data_table() fails to retrieve vram_info, it returns NULL which is later dereferenced.	N/A	More Details
CVE-2025-38320	In the Linux kernel, the following vulnerability has been resolved: arm64/ptrace: Fix stack-out-of-bounds read in regs_get_kernel_stack_nth() KASAN reports a stack-out-of-bounds read in regs_get_kernel_stack_nth(). Call Trace: [97.283505] BUG: KASAN: stack-out-of-bounds in regs_get_kernel_stack_nth+0xa8/0xc8 [97.284677] Read of size 8 at addr ffff800089277c10 by task 1.sh/2550 [97.285732] [97.286067] CPU: 7 PID: 2550 Comm: 1.sh Not tainted 6.6.0+ #11 [97.287032] Hardware name: linux,dummy-virt (DT) [97.287815] Call trace: [97.288279] dump_backtrace+0xa0/0x128 [97.288946] show_stack+0x20/0x38 [97.289551] dump_stack_lvl+0x78/0xc8 [97.290203] print_address_description.constprop.0+0x84/0x3c8 [97.291159] print_report+0xb0/0x280 [97.291792] kasan_report+0x84/0xd0 [97.292421] __asan_load8+0x9c/0xc0 [97.293042] regs_get_kernel_stack_nth+0xa8/0xc8 [97.293835] process_fetch_insn+0x770/0xa30 [97.294562] kprobe_trace_func+0x254/0x3b0 [97.295271] kprobe_dispatcher+0x98/0xe0 [97.295955] kprobe_breakpoint_handler+0x1b0/0x210 [97.296774] call_break_hook+0xc4/0x100 [97.297451] brk_handler+0x24/0x78 [97.298073] do_debug_exception+0xac/0x178 [97.298785] el1_dbg+0x70/0x90 [97.299344] el1h_64_sync_handler+0xcc/0xe8 [97.300066] el1h_64_sync+0x78/0x80 [97.300699] kernel_clone+0x0/0x500 [97.301331] __arm64_sys_clone+0x70/0x90 [97.302084] invoke_syscall+0x68/0x198 [97.302746] el0_svc_common.constprop.0+0x11c/0x150 [97.303569] do_el0_svc+0x38/0x50 [97.304164] el0_svc+0x44/0x1d8 [97.304749] el0t_64_sync_handler+0x100/0x130 [97.305500] el0t_64_sync+0x188/0x190 [97.306151] [97.306475] The buggy address belongs to stack of task 1.sh/2550 [97.307461] and is located at offset 0 in frame: [97.308257] __se_sys_clone+0x0/0x138 [97.308910] [97.309241] This frame has 1 object: [97.309873] [48, 184) 'args' [97.309876] [97.310749] The buggy address belongs to the virtual mapping at [97.310749] [ffff800089270000, ffff800089279000) created by: [97.310749] dup_task_struct+0xc0/0x2e8 [97.313347] [97.313674] The buggy address belongs to the physical page: [97.314604] page: refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x14f69a [97.315885] flags: 0x15ffffe00000000(node=1|zone=2|lastcpupid=0xfffff) [97.316957] raw: 015ffffe00000000 0000000000000000 dead000000000122 0000000000000000 [97.318207] raw: 0000000000000000 0000000000000000 00000001ffffffff 0000000000000000 [97.319445] page dumped because: kasan: bad access detected [97.320371] [97.320694] Memory state around the buggy address: [97.321511] ffff800089277b00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [97.322681] ffff800089277b80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [97.323846] >ffff800089277c00: 00 00 f1 f1 f1 f1 f1 f1 00 00 00 00 00 00 00 00 [97.325023] ^ [97.325683] ffff800089277c80: 00 00 00 00 00 00 00 00 f3 f3 f3 f3 f3 f3 f3 [	N/A	More Details

	97.326856] ffff800089277d00: f3 f3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 This issue seems to be related to the behavior of some gcc compilers and was also fixed on the s390 architecture before: commit d93a855c31b7 ("s390/ptrace: Avoid KASAN false positives in regs_get_kernel_stack_nth()") As described in that commit, regs_get_kernel_stack_nth() has confirmed that `addr` is on the stack, so reading the value at `*addr` should be allowed. Use READ_ONCE_NOCHECK() helper to silence the KASAN check for this case. [will: Use '*addr' as the argument to READ_ONCE_NOCHECK()]		
CVE-2025-38321	In the Linux kernel, the following vulnerability has been resolved: smb: Log an error when close_all_cached_dirs fails Under low-memory conditions, close_all_cached_dirs() can't move the dentries to a separate list to dput() them once the locks are dropped. This will result in a "Dentry still in use" error, so add an error message that makes it clear this is what happened: [495.281119] CIFS: VFS: \\otters.example.com\share Out of memory while dropping dentries [495.281595] ------------[cut here]------------ [495.281887] BUG: Dentry ffff888115531138{i=78,n=/} still in use (2) [unmount of cifs cifs] [495.282391] WARNING: CPU: 1 PID: 2329 at fs/dcache.c:1536 umount_check+0xc8/0xf0 Also, bail out of looping through all tcons as soon as a single allocation fails, since we're already in trouble, and kmalloc() attempts for subseqeuent tcons are likely to fail just like the first one did.	N/A	More Details
CVE-2025-38322	In the Linux kernel, the following vulnerability has been resolved: perf/x86/intel: Fix crash in icl_update_topdown_event() The perf_fuzzer found a hard-lockup crash on a RaptorLake machine: Oops: general protection fault, maybe for address 0xffff89aeceab400: 0000 CPU: 23 UID: 0 PID: 0 Comm: swapper/23 Tainted: [W]=WARN Hardware name: Dell Inc. Precision 9660/0VJ762 RIP: 0010:native_read_pmc+0x7/0x40 Code: cc e8 8d a9 01 00 48 89 03 5b cd cc cc cc cc 0f 1f ... RSP: 000:fffb03100273de8 EFLAGS: 00010046 .... Call Trace: <TASK> icl_update_topdown_event+0x165/0x190 ? ktime_get+0x38/0xd0 intel_pmu_read_event+0xf9/0x210 __perf_event_read+0xf9/0x210 CPUs 16-23 are E-core CPUs that don't support the perf metrics feature. The icl_update_topdown_event() should not be invoked on these CPUs. It's a regression of commit: f9bdf1f95339 ("perf/x86/intel: Avoid disable PMU if !cpuc->enabled in sample read") The bug introduced by that commit is that the is_topdown_event() function is mistakenly used to replace the is_topdown_count() call to check if the topdown functions for the perf metrics feature should be invoked. Fix it.	N/A	More Details
CVE-2025-38323	In the Linux kernel, the following vulnerability has been resolved: net: atm: add lec_mutex syzbot found its way in net/atm/lec.c, and found an error path in lecd_attach() could leave a dangling pointer in dev_lec[]. Add a mutex to protect dev_lecp[] uses from lecd_attach(), lec_vcc_attach() and lec_mcast_attach(). Following patch will use this mutex for /proc/net/atm/lec. BUG: KASAN: slab-use-after-free in lecd_attach net/atm/lec.c:751 [inline] BUG: KASAN: slab-use-after-free in lane_ioctl+0x2224/0x23e0 net/atm/lec.c:1008 Read of size 8 at addr ffff88807c7b8e68 by task syz.1.17/6142 CPU: 1 UID: 0 PID: 6142 Comm: syz.1.17 Not tainted 6.16.0-rc1-syzkaller-00239-g08215f5486ec #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/07/2025 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x116/0x1f0 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:408 [inline] print_report+0xcd/0x680 mm/kasan/report.c:521 kasan_report+0xe0/0x110 mm/kasan/report.c:634 lecd_attach net/atm/lec.c:751 [inline] lane_ioctl+0x2224/0x23e0 net/atm/lec.c:1008 do_vcc_ioctl+0x12c/0x930 net/atm/ioctl.c:159 sock_do_ioctl+0x118/0x280 net/socket.c:1190 sock_ioctl+0x227/0x6b0 net/socket.c:1311 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:907 [inline] __se_sys_ioctl fs/ioctl.c:893 [inline] __x64_sys_ioctl+0x18e/0x210 fs/ioctl.c:893 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xcd/0x4c0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> Allocated by task 6132: kasan_save_stack+0x33/0x60 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:4328 [inline] __kvmalloc_node_noprof+0x27b/0x620 mm/slub.c:5015 alloc_netdev_mqs+0xd2/0x1570 net/core/dev.c:11711 lecd_attach net/atm/lec.c:737 [inline] lane_ioctl+0x17db/0x23e0 net/atm/lec.c:1008 do_vcc_ioctl+0x12c/0x930 net/atm/ioctl.c:159 sock_do_ioctl+0x118/0x280 net/socket.c:1190 sock_ioctl+0x227/0x6b0 net/socket.c:1311 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:907 [inline] __se_sys_ioctl fs/ioctl.c:893 [inline] __x64_sys_ioctl+0x18e/0x210 fs/ioctl.c:893 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xcd/0x4c0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 6132: kasan_save_stack+0x33/0x60 mm/kasan/common.c:47 kasan_save_track+0x14/0x30 mm/kasan/common.c:68 kasan_save_free_info+0x3b/0x60 mm/kasan/generic.c:576 poison_slab_object mm/kasan/common.c:247 [inline] __kasan_slab_free+0x51/0x70 mm/kasan/common.c:264 kasan_slab_free include/linux/kasan.h:233 [inline] slab_free_hook mm/slub.c:2381 [inline] slab_free mm/slub.c:4643 [inline] kfree+0x2b4/0x4d0 mm/slub.c:4842 free_netdev+0x6c5/0x910 net/core/dev.c:11892 lecd_attach net/atm/lec.c:744 [inline] lane_ioctl+0x1ce8/0x23e0 net/atm/lec.c:1008 do_vcc_ioctl+0x12c/0x930 net/atm/ioctl.c:159 sock_do_ioctl+0x118/0x280 net/socket.c:1190 sock_ioctl+0x227/0x6b0 net/socket.c:1311 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:907 [inline] __se_sys_ioctl fs/ioctl.c:893 [inline] __x64_sys_ioctl+0x18e/0x210 fs/ioctl.c:893	N/A	More Details
CVE-2025-38324	In the Linux kernel, the following vulnerability has been resolved: mpls: Use rcu_dereference_rtnl() in mpls_route_input_rcu(). As syzbot reported [0], mpls_route_input_rcu() can be called from mpls_getroute(), where is under RTNL. net->mpls.platform_label is only updated under RTNL. Let's use rcu_dereference_rtnl() in mpls_route_input_rcu() to silence the splat. [0]: WARNING: suspicious RCU usage 6.15.0-rc7-syzkaller-00082-g5cdb2c77c4c3 #0 Not tainted ----------------------------- net/mpls/af_mpls.c:84 suspicious rcu_dereference_check() usage! other info that might help us debug this: rcu_scheduler_active = 2, debug_locks = 1 1 lock held by syz.2.4451/17730: #0: ffffffff9012a3e8 (rtnl_mutex){+.+.}-{4:4}, at: rtnl_lock net/core/rtnetlink.c:80 [inline] #0: ffffffff9012a3e8 (rtnl_mutex){+.+.}-{4:4}, at: rtnetlink_rcv_msg+0x371/0xe90 net/core/rtnetlink.c:6961 stack backtrace: CPU: 1 UID: 0 PID: 17730 Comm: syz.2.4451 Not tainted 6.15.0-rc7-syzkaller-00082-g5cdb2c77c4c3 #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/07/2025 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x16c/0x1f0 lib/dump_stack.c:120 lockdep_rcu_suspicious+0x166/0x260 kernel/locking/lockdep.c:6865 mpls_route_input_rcu+0x1d4/0x200 net/mpls/af_mpls.c:84 mpls_getroute+0x621/0x1ea0 net/mpls/af_mpls.c:2381 rtnetlink_rcv_msg+0x3c9/0xe90 net/core/rtnetlink.c:6964 netlink_rcv_skb+0x16d/0x440 net/netlink/af_netlink.c:2534 netlink_unicast_kernel net/netlink/af_netlink.c:1313 [inline] netlink_unicast+0x53a/0x7f0 net/netlink/af_netlink.c:1339 netlink_sendmsg+0x8d1/0xdd0 net/netlink/af_netlink.c:1883 sock_sendmsg_nosec net/socket.c:712 [inline] __sock_sendmsg net/socket.c:727 [inline] ____sys_sendmsg+0xa98/0xc70 net/socket.c:2566 ___sys_sendmsg+0x134/0x1d0 net/socket.c:2620 __sys_sendmmsg+0x200/0x420 net/socket.c:2709 __do_sys_sendmmsg net/socket.c:2736 [inline] __se_sys_sendmmsg net/socket.c:2733 [inline] __x64_sys_sendmmsg+0x9c/0x100 net/socket.c:2733 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xcd/0x230 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f0a2818e969 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:00007f0a28f52038 EFLAGS: 00000246 ORIG_RAX: 0000000000000133 RAX: ffffffffffffffda RBX: 00007f0a283b5fa0 RCX: 00007f0a2818e969 RDX: 0000000000000003 RSI: 0000200000000080 RDI: 0000000000000003 RBP: 00007f0a28210ab1 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007f0a283b5fa0 R15: 00007ffce5e9f268 </TASK>	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: ksmbd: add free_transport ops in ksmbd connection free_transport		More

2025-38325	function for tcp connection can be called from smbdirect. It will cause kernel oops. This patch add free_transport ops in ksmbd connection, and add each free_transports for tcp and smbdirect.	N/A	Details
CVE-2025-38309	In the Linux kernel, the following vulnerability has been resolved: drm/xe/vm: move xe_svm_init() earlier In xe_vm_close_and_put() we need to be able to call xe_svm_fini(), however during vm creation we can call this on the error path, before having actually initialised the svm state, leading to various splats followed by a fatal NPD. (cherry picked from commit 4f296d77cf49fcb5f90b4674123ad7f3a0676165)	N/A	More Details
CVE-2025-38308	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: avs: Fix possible null-ptr-deref when initing hw Search result of avs_dai_find_path_template() shall be verified before being used. As 'template' is already known when avs_hw_constraints_init() is fired, drop the search entirely.	N/A	More Details
CVE-2025-38307	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: avs: Verify content returned by parse_int_array() The first element of the returned array stores its length. If it is 0, any manipulation beyond the element at index 0 ends with null-ptr-deref.	N/A	More Details
CVE-2025-38306	In the Linux kernel, the following vulnerability has been resolved: fs/fhandle.c: fix a race in call of has_locked_children() may_decode_fh() is calling has_locked_children() while holding no locks. That's an oopsable race... The rest of the callers are safe since they are holding namespace_sem and are guaranteed a positive refcount on the mount in question. Rename the current has_locked_children() to __has_locked_children(), make it static and switch the fs/namespace.c users to it. Make has_locked_children() a wrapper for __has_locked_children(), calling the latter under read_seqlock_excl(&mount_lock).	N/A	More Details
CVE-2024-26292	An authenticated Arbitrary File Deletion vulnerability enables an attacker to delete critical files. This issue affects Avid NEXIS E-series: before 2025.5.1; Avid NEXIS F-series: before 2025.5.1; Avid NEXIS PRO+: before 2025.5.1; System Director Appliance (SDA+): before 2025.5.1.	N/A	More Details
CVE-2024-26291	An Unauthenticated Arbitrary File Read vulnerability affects the Agent when installed on a system. The parameter filename does not validate the path thus allowing users to read arbitrary files. As the application runs with the highest privileges (root/NT_AUTHORITY SYSTEM) by default attackers are able to obtain sensitive information. This issue affects Avid NEXIS E-series: before 2025.5.1; Avid NEXIS F-series: before 2025.5.1; Avid NEXIS PRO+: before 2025.5.1; System Director Appliance (SDA+): before 2025.5.1.	N/A	More Details
CVE-2025-38294	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix NULL access in assign channel context handler Currently, when ath12k_mac_assign_vif_to_vdev() fails, the radio handle (ar) gets accessed from the link VIF handle (arvif) for debug logging, This is incorrect. In the fail scenario, radio handle is NULL. Fix the NULL access, avoid radio handle access by moving to the hardware debug logging helper function (ath12k_hw_warn). Tested-on: QCN9274 hw2.0 PCI WLAN.WBE.1.3.1-00173-QCAHKSWPL_SILICONZ-1 Tested-on: WCN7850 hw2.0 PCI WLAN.HMT.1.0.c5-00481-QCAHMTSWPL_V1.0_V2.0_SILICONZ-3	N/A	More Details
CVE-2025-38295	In the Linux kernel, the following vulnerability has been resolved: perf/amlogic: Replace smp_processor_id() with raw_smp_processor_id() in meson_ddr_pmu_create() The Amlogic DDR PMU driver meson_ddr_pmu_create() function incorrectly uses smp_processor_id(), which assumes disabled preemption. This leads to kernel warnings during module loading because meson_ddr_pmu_create() can be called in a preemptible context. Following kernel warning and stack trace: [31.745138] [T2289] BUG: using smp_processor_id() in preemptible [00000000] code: (udev-worker)/2289 [31.745154] [T2289] caller is debug_smp_processor_id+0x28/0x38 [31.745172] [T2289] CPU: 4 UID: 0 PID: 2289 Comm: (udev-worker) Tainted: GW 6.14.0-0-MANJARO-ARM #1 59519addcbca6ba8de735e151fd7b9e97aac7ff0 [31.745181] [T2289] Tainted: [W]=WARN [31.745183] [T2289] Hardware name: Hardkernel ODROID-N2Plus (DT) [31.745188] [T2289] Call trace: [31.745191] [T2289] show_stack+0x28/0x40 (C) [31.745199] [T2289] dump_stack_lvl+0x4c/0x198 [31.745205] [T2289] dump_stack+0x20/0x50 [31.745209] [T2289] check_preemption_disabled+0xec/0xf0 [31.745213] [T2289] debug_smp_processor_id+0x28/0x38 [31.745216] [T2289] meson_ddr_pmu_create+0x200/0x560 [meson_ddr_pmu_g12 8095101c49676ad138d9961e3eddaee10acca7bd] [31.745237] [T2289] g12_ddr_pmu_probe+0x20/0x38 [meson_ddr_pmu_g12 8095101c49676ad138d9961e3eddaee10acca7bd] [31.745246] [T2289] platform_probe+0x98/0xe0 [31.745254] [T2289] really_probe+0x144/0x3f8 [31.745258] [T2289] __driver_probe_device+0xb8/0x180 [31.745261] [T2289] driver_probe_device+0x54/0x268 [31.745264] [T2289] __driver_attach+0x11c/0x288 [31.745267] [T2289] bus_for_each_dev+0xfc/0x160 [31.745274] [T2289] driver_attach+0x34/0x50 [31.745277] [T2289] bus_add_driver+0x160/0x2b0 [31.745281] [T2289] driver_register+0x78/0x120 [31.745285] [T2289] __platform_driver_register+0x30/0x48 [31.745288] [T2289] init_module+0x30/0xfe0 [meson_ddr_pmu_g12 8095101c49676ad138d9961e3eddaee10acca7bd] [31.745298] [T2289] do_one_initcall+0x11c/0x438 [31.745303] [T2289] do_init_module+0x68/0x228 [31.745311] [T2289] load_module+0x118c/0x13a8 [31.745315] [T2289] __arm64_sys_finit_module+0x274/0x390 [31.745320] [T2289] invoke_syscall+0x74/0x108 [31.745326] [T2289] el0_svc_common+0x90/0xf8 [31.745330] [T2289] do_el0_svc+0x2c/0x48 [31.745333] [T2289] el0_svc+0x60/0x150 [31.745337] [T2289] el0t_64_sync_handler+0x80/0x118 [31.745341] [T2289] el0t_64_sync+0x1b8/0x1c0 Changes replaces smp_processor_id() with raw_smp_processor_id() to ensure safe CPU ID retrieval in preemptible contexts.	N/A	More Details
CVE-2025-38296	In the Linux kernel, the following vulnerability has been resolved: ACPI: platform_profile: Avoid initializing on non-ACPI platforms The platform profile driver is loaded even on platforms that do not have ACPI enabled. The initialization of the sysfs entries was recently moved from platform_profile_register() to the module init call, and those entries need acpi_kobj to be initialized which is not the case when ACPI is disabled. This results in the following warning: WARNING: CPU: 5 PID: 1 at fs/sysfs/group.c:131 internal_create_group+0xa22/0xdd8 Modules linked in: CPU: 5 UID: 0 PID: 1 Comm: swapper/0 Tainted: G W 6.15.0-rc7-dirty #6 PREEMPT Tainted: [W]=WARN Hardware name: riscv-virtio,qemu (DT) epc : internal_create_group+0xa22/0xdd8 ra : internal_create_group+0xa22/0xdd8 Call Trace: internal_create_group+0xa22/0xdd8 sysfs_create_group+0x22/0x2e platform_profile_init+0x74/0xb2 do_one_initcall+0x198/0xa9e kernel_init_freeable+0x6d8/0x780 kernel_init+0x28/0x24c ret_from_fork+0xe/0x18 Fix this by checking if ACPI is enabled before trying to create sysfs entries. [rjw: Subject and changelog edits]	N/A	More Details
CVE-2025-38297	In the Linux kernel, the following vulnerability has been resolved: PM: EM: Fix potential division-by-zero error in em_compute_costs() When the device is of a non-CPU type, table[i].performance won't be initialized in the previous em_init_performance(), resulting in division by zero when calculating costs in em_compute_costs(). Since the 'cost' algorithm is only used for EAS energy efficiency calculations and is currently not utilized by other device drivers, we should add the _is_cpu_device(dev) check to prevent this division-by-zero issue.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: EDAC/skx_common: Fix general protection fault After loading i10nm_edac (which automatically loads skx_edac_common), if unload only i10nm_edac, then reload it and perform error injection testing, a general protection fault may occur: mce: [Hardware Error]: Machine check events logged Oops: general protection fault ...		

CVE-2025-38298	... Workqueue: events mce_gen_pool_process RIP: 0010:string+0x53/0xe0 ... Call Trace: <TASK> ? die_addr+0x37/0x90 ? exc_general_protection+0x1e7/0x3f0 ? asm_exc_general_protection+0x26/0x30 ? string+0x53/0xe0 vsnprintf+0x23e/0x4c0 snprintf+0x4d/0x70 skx_adxl_decode+0x16a/0x330 [skx_edac_common] skx_mce_check_error.part.0+0xf8/0x220 [skx_edac_common] skx_mce_check_error+0x17/0x20 [skx_edac_common] ... The issue arose was because the variable 'adxl_component_count' (inside skx_edac_common), which counts the ADXL components, was not reset. During the reloading of i10nm_edac, the count was incremented by the actual number of ADXL components again, resulting in a count that was double the real number of ADXL components. This led to an out-of-bounds reference to the ADXL component array, causing the general protection fault above. Fix this issue by resetting the 'adxl_component_count' in adxl_put(), which is called during the unloading of {skx,i10nm}_edac.	N/A	More Details
CVE-2025-38299	In the Linux kernel, the following vulnerability has been resolved: ASoC: mediatek: mt8195: Set ETDM1/2 IN/OUT to COMP_DUMMY() ETDM2_IN_BE and ETDM1_OUT_BE are defined as COMP_EMPTY(), in the case the codec dai_name will be null. Avoid a crash if the device tree is not assigning a codec to these links. [1.179936] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 [1.181065] Mem abort info: [1.181420] ESR = 0x0000000096000004 [1.181892] EC = 0x25: DABT (current EL), IL = 32 bits [1.182576] SET = 0, FnV = 0 [1.182964] EA = 0, S1PTW = 0 [1.183367] FSC = 0x04: level 0 translation fault [1.183983] Data abort info: [1.184406] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [1.185097] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [1.185766] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [1.186439] [0000000000000000] user address but active_mm is swapper [1.187239] Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP [1.188029] Modules linked in: [1.188420] CPU: 7 UID: 0 PID: 70 Comm: kworker/u32:1 Not tainted 6.14.0-rc4-next-20250226+ #85 [1.189515] Hardware name: Radxa NIO 12L (DT) [1.190065] Workqueue: events_unbound deferred_probe_work_func [1.190808] pstate: 40400009 (nZcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [1.191683] pc : __pi_strcmp+0x24/0x140 [1.192170] lr : mt8195_mt6359_soc_card_probe+0x224/0x7b0 [1.192854] sp : ffff800083473970 [1.193271] x29: ffff800083473a10 x28: 0000000000001008 x27: 0000000000000002 [1.194168] x26: ffff800082408960 x25: ffff800082417db0 x24: ffff800082417d88 [1.195065] x23: 000000000000001e x22: ffff800082dbf480 x21: ffff800082dc07b8 [1.195961] x20: 0000000000000000 x19: 0000000000000013 x18: 00000000ffffffff [1.196858] x17: 000000040044ffff x16: 005000f2b5503510 x15: 0000000000000006 [1.197755] x14: ffff800082407af0 x13: 6e6f69737265766e x12: 692d6b636f6c6374 [1.198651] x11: 0000000000000002 x10: ffff80008240b920 x9 : 0000000000000018 [1.199547] x8 : 0101010101010101 x7 : 0000000000000000 x6 : 0000000000000000 [1.200443] x5 : 0000000000000000 x4 : 8080808080000000 x3 : 303933383978616d [1.201339] x2 : 0000000000000000 x1 : ffff80008240b920 x0 : 0000000000000000 [1.202236] Call trace: [1.202545] __pi_strcmp+0x24/0x140 (P) [1.203029] mtk_soundcard_common_probe+0x3bc/0x5b8 [1.203644] platform_probe+0x70/0xe8 [1.204106] really_probe+0xc8/0x3a0 [1.204556] __driver_probe_device+0x84/0x160 [1.205104] driver_probe_device+0x44/0x130 [1.205630] __device_attach_driver+0xc4/0x170 [1.206189] bus_for_each_drv+0x8c/0xf8 [1.206672] __device_attach+0xa8/0x1c8 [1.207155] device_initial_probe+0x1c/0x30 [1.207681] bus_probe_device+0xb0/0xc0 [1.208165] deferred_probe_work_func+0xa4/0x100 [1.208747] process_one_work+0x158/0x3e0 [1.209254] worker_thread+0x2c4/0x3e8 [1.209727] kthread+0x134/0x1f0 [1.210136] ret_from_fork+0x10/0x20 [1.210589] Code: 54000401 b50002c6 d503201f f86a6803 (f8408402) [1.211355] ---[end trace 0000000000000000]---	N/A	More Details
CVE-2025-38300	In the Linux kernel, the following vulnerability has been resolved: crypto: sun8i-ce-cipher - fix error handling in sun8i_ce_cipher_prepare() Fix two DMA cleanup issues on the error path in sun8i_ce_cipher_prepare(): 1] If dma_map_sg() fails for areq->dst, the device driver would try to free DMA memory it has not allocated in the first place. To fix this, on the "theend_sgs" error path, call dma unmap only if the corresponding dma map was successful. 2] If the dma_map_single() call for the IV fails, the device driver would try to free an invalid DMA memory address on the "theend_iv" path: ------------[cut here]------------ DMA-API: sun8i-ce 1904000.crypto: device driver tries to free an invalid DMA memory address WARNING: CPU: 2 PID: 69 at kernel/dma/debug.c:968 check_unmap+0x123c/0x1b90 Modules linked in: skcipher_example(O+) CPU: 2 UID: 0 PID: 69 Comm: 1904000.crypto- Tainted: G O 6.15.0-rc3+ #24 PREEMPT Tainted: [O]=OOT_MODULE Hardware name: OrangePi Zero2 (DT) pc : check_unmap+0x123c/0x1b90 lr : check_unmap+0x123c/0x1b90 ... Call trace: check_unmap+0x123c/0x1b90 (P) debug_dma_unmap_page+0xac/0xc0 dma_unmap_page_attrs+0x1f4/0x5fc sun8i_ce_cipher_do_one+0x1bd4/0x1f40 crypto_pump_work+0x334/0x6e0 kthread_worker_fn+0x21c/0x438 kthread+0x374/0x664 ret_from_fork+0x10/0x20 ---[end trace 0000000000000000]--- To fix this, check for !dma_mapping_error() before calling dma_unmap_single() on the "theend_iv" path.	N/A	More Details
CVE-2025-38301	In the Linux kernel, the following vulnerability has been resolved: nvmem: zynqmp_nvmem: unbreak driver after cleanup Commit 29be47fcd6a0 ("nvmem: zynqmp_nvmem: zynqmp_nvmem_probe cleanup") changed the driver to expect the device pointer to be passed as the "context", but in nvmem the context parameter comes from nvmem_config.priv which is never set - Leading to null pointer exceptions when the device is accessed.	N/A	More Details
CVE-2025-7380	A stored Cross-Site Scripting (XSS) vulnerability exists in the Access Control of ADM, the issue allows an attacker to inject malicious scripts into the folder name field while creating a new shared folder. These scripts are not properly sanitized and will be executed when the folder name is subsequently displayed in the user interface. This allows attackers to execute arbitrary JavaScript in the context of another user's session, potentially accessing session cookies or other sensitive data. Affected products and versions include: from ADM 4.1.0 to ADM 4.3.3.RH61 as well as ADM 5.0.0.RIN1 and earlier.	N/A	More Details
CVE-2025-38302	In the Linux kernel, the following vulnerability has been resolved: block: don't use submit_bio_noacct_nocheck in blk_zone_wplug_bio_work Bios queued up in the zone write plug have already gone through all all preparation in the submit_bio path, including the freeze protection. Submitting them through submit_bio_noacct_nocheck duplicates the work and can can cause deadlocks when freezing a queue with pending bio write plugs. Go straight to ->submit_bio or blk_mq_submit_bio to bypass the superfluous extra freeze protection and checks.	N/A	More Details
CVE-2025-38303	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: eir: Fix possible crashes on eir_create_adv_data eir_create_adv_data may attempt to add EIR_FLAGS and EIR_TX_POWER without checking if that would fit.	N/A	More Details
CVE-2025-38304	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: Fix NULL pointer deference on eir_get_service_data The len parameter is considered optional so it can be NULL so it cannot be used for skipping to next entry of EIR_SERVICE_DATA.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: ptp: remove ptp->n_vclocks check logic in ptp_vclock_in_use() There is no disagreement that we should check both ptp->is_virtual_clock and ptp->n_vclocks to check if the ptp virtual clock is in use. However, when we acquire ptp->n_vclocks_mux to read ptp->n_vclocks in ptp_vclock_in_use(), we observe a recursive lock in the call trace starting from n_vclocks_store(). == WARNING: possible recursive locking detected 6.15.0-rc6 #1 Not tainted -- syz.0.1540/13807 is trying to acquire lock: ffff888035a24868 (&ptp->n_vclocks_mux){+.+.}-{4:4}, at: ptp_vclock_in_use drivers/ptp/ptp_private.h:103 [inline] ffff888035a24868 (&ptp->n_vclocks_mux){+.+.}-{4:4}, at: ptp_clock_unregister+0x21/0x250 drivers/ptp/ptp_clock.c:415 but task		More

2025-38305	is already holding lock: ffff888030704868 (&ptp->n_vclocks_mux){+.+.}-{4:4}, at: n_vclocks_store+0xf1/0x6d0 drivers/ptp/ptp_sysfs.c:215 other info that might help us debug this: Possible unsafe locking scenario: CPU0 ---- lock(&ptp->n_vclocks_mux); lock(&ptp->n_vclocks_mux); *** DEADLOCK *** .... == The best way to solve this is to remove the logic that checks ptp->n_vclocks in ptp_vclock_in_use(). The reason why this is appropriate is that any path that uses ptp->n_vclocks must unconditionally check if ptp->n_vclocks is greater than 0 before unregistering vclocks, and all functions are already written this way. And in the function that uses ptp->n_vclocks, we already get ptp->n_vclocks_mux before unregistering vclocks. Therefore, we need to remove the redundant check for ptp->n_vclocks in ptp_vclock_in_use() to prevent recursive locking.	N/A	Details
CVE-2025-6981	An incorrect authorization vulnerability allowed unauthorized read access to the contents of internal repositories for contractor accounts when the Contractors API feature was enabled. The Contractors API is a rarely-enabled feature in private preview. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.18 and was fixed in versions 3.14.15, 3.15.10, 3.16.6 and 3.17.3	N/A	More Details