SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 17 December 2025

Generated on 17 December 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-2025-63414	A Path Traversal vulnerability in the Allsky WebUI version v2024.12.06_06 allows an unauthenticated remote attacker to achieve arbitrary command execution. By sending a crafted HTTP request to the /html/execute.php endpoint with a malicious payload in the id parameter, an attacker can execute arbitrary commands on the underlying operating system, leading to full remote code execution (RCE).	10.0	More Details
CVE-2025-37164	A remote code execution issue exists in HPE OneView.	10.0	More Details
CVE-2025-68270	The Open edX Platform is a learning management platform. Prior to commit 05d0d0936daf82c476617257aa6c35f0cd4ca060, CourseLimitedStaffRole users are able to access and edit courses in studio if they are granted the role on an org rather than on a course, and CourseLimitedStaffRole users are able to list courses they have the role on in studio even though they are not meant to have any access on the studio side for the course. Commit 05d0d0936daf82c476617257aa6c35f0cd4ca060 fixes the issue.	9.9	More Details
CVE-2024-58311	Dormakaba Saflok System 6000 contains a predictable key generation algorithm that allows attackers to derive card access keys from a 32-bit unique identifier. Attackers can exploit the deterministic key generation process by calculating valid access keys using a simple mathematical transformation of the card's unique identifier.	9.8	More Details
CVE-2025-14665	A security flaw has been discovered in Tenda WH450 1.0.0.18. Impacted is an unknown function of the file /goform/DhcpListClient of the component HTTP Request Handler. The manipulation of the argument page results in stack-based buffer overflow. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	9.8	More Details
CVE-2025-14440	The JAY Login & Register plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.4.01. This is due to incorrect authentication checking in the 'jay_login_register_process_switch_back' function with the 'jay_login_register_process_switch_back' cookie value. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the user id.	9.8	More Details
CVE-2025-11693	The Export WP Page to Static HTML & PDF plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.3.4 through publicly exposed cookies.txt files containing authentication cookies. This makes it possible for unauthenticated attackers to cookies that may have been injected into the log file if the site administrator triggered a back-up using a specific user role like 'administrator.'	9.8	More Details
CVE-2025-10738	The URL Shortener Plugin For WordPress plugin for WordPress is vulnerable to SQL Injection via the ‘analytic_id’ parameter in all versions up to, and including, 3.0.7 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.	9.8	More Details
CVE-2025-14611	Gladinet CentreStack and Triofox prior to version 16.12.10420.56791 used hardcoded values for their implementation of the AES cryptoscheme. This degrades security for public exposed endpoints that may make use of it and may offer arbitrary local file inclusion when provided a specially crafted request without authentication. This opens the door for future exploitation and can be leveraged with previous vulnerabilities to gain a full system compromise.	9.8	More Details
CVE-2024-14010	Typora 1.7.4 contains a command injection vulnerability in the PDF export preferences that allows attackers to execute arbitrary system commands. Attackers can inject malicious commands into the 'run command' input field during PDF export to achieve remote code execution.	9.8	More Details
CVE-2024-58299	PCMan FTP Server 2.0 contains a buffer overflow vulnerability in the 'pwd' command that allows remote attackers to execute arbitrary code. Attackers can send a specially crafted payload during the FTP login process to overwrite memory and potentially gain system access.	9.8	More Details
	A vulnerability was identified in Shiguangwu sgwbox N3 2.0.25. This impacts an unknown function of the file		

CVE-2025-14706	/usr/sbin/http_eshell_server of the component NETREBOOT Interface. Such manipulation leads to command injection. The attack can be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2025-65854	Insecure permissions in the scheduled tasks feature of MineAdmin v3.x allows attackers to execute arbitrary commands and execute a full account takeover.	9.8	More Details
CVE-2025-54947	In Apache StreamPark versions 2.0.0 through 2.1.7, a security vulnerability involving a hard-coded encryption key exists. This vulnerability occurs because the system uses a fixed, immutable key for encryption instead of dynamically generating or securely configuring the key. Attackers may obtain this key through reverse engineering or code analysis, potentially decrypting sensitive data or forging encrypted information, leading to information disclosure or unauthorized system access. This issue affects Apache StreamPark: from 2.0.0 before 2.1.7. Users are recommended to upgrade to version 2.1.7, which fixes the issue.	9.8	More Details
CVE-2025-14344	The Multi Uploader for Gravity Forms plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'plupload_ajax_delete_file' function in all versions up to, and including, 1.1.7. This makes it possible for unauthenticated attackers to delete arbitrary files on the server.	9.8	More Details
CVE-2025-12963	The LazyTasks – Project & Task Management with Collaboration, Kanban and Gantt Chart plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.2.29. This is due to the plugin not properly validating a user's identity via the 'wp-json/lazytasks/api/v1/user/role/edit/' REST API endpoint prior to updating their details like email address. This makes it possible for unauthenticated attackers to change arbitrary user's email addresses, including administrators, and leverage that to reset the user's password and gain access to their account. It is also possible for attackers to abuse this endpoint to grant users with access to additional roles within the plugin	9.8	More Details
CVE-2025-14705	A vulnerability was determined in Shiguangwu sgwbox N3 2.0.25. This affects an unknown function of the component SHARESERVER Feature. This manipulation of the argument params causes command injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2025-14707	A security flaw has been discovered in Shiguangwu sgwbox N3 2.0.25. Affected is an unknown function of the file /usr/sbin/http_eshell_server of the component DOCKER Feature. Performing manipulation of the argument params results in command injection. The attack may be initiated remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2025-14535	A vulnerability was identified in UTT 进取 512W up to 3.1.7.7-171114. Affected is the function strcpy of the file /goform/formConfigFastDirectionW. The manipulation of the argument ssid leads to buffer overflow. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2025-14708	A weakness has been identified in Shiguangwu sgwbox N3 2.0.25. Affected by this vulnerability is an unknown functionality of the file /usr/sbin/http_eshell_server of the component WIREDCFGGET Interface. Executing manipulation of the argument params can lead to buffer overflow. The attack may be launched remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2025-14709	A security vulnerability has been detected in Shiguangwu sgwbox N3 2.0.25. Affected by this issue is some unknown functionality of the file /usr/sbin/http_eshell_server of the component WIRELESSCFGGET Interface. The manipulation of the argument params leads to buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2025-14156	The Fox LMS – WordPress LMS Plugin plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.0.5.1. This is due to the plugin not properly validating the 'role' parameter when creating new users via the `/fox-lms/v1/payments/create-order` REST API endpoint. This makes it possible for unauthenticated attackers to create new user accounts with arbitrary roles, including administrator, leading to complete site compromise.	9.8	More Details
CVE-2025-66434	An SSTI (Server-Side Template Injection) vulnerability exists in the get_dunning_letter_text method of Frappe ERPNext through 15.89.0. The function renders attacker-controlled Jinja2 templates (body_text) using frappe.render_template() with a user-supplied context (doc). Although Frappe uses a custom SandboxedEnvironment, several dangerous globals such as frappe.db.sql are still available in the execution context via get_safe_globals(). An authenticated attacker with access to configure Dunning Type and its child table Dunning Letter Text can inject arbitrary Jinja expressions, resulting in server-side code execution within a restricted but still unsafe context. This can leak database information.	9.8	More Details
CVE-2025-66438	A Server-Side Template Injection (SSTI) vulnerability exists in the Frappe ERPNext through 15.89.0 Print Format rendering mechanism. Specifically, the API frappe.www.printview.get_html_and_style() triggers the rendering of the html field inside a Print Format document using frappe.render_template(template, doc) via the get_rendered_template() call chain. Although ERPNext wraps Jinja2 in a SandboxedEnvironment, it exposes sensitive functions such as frappe.db.sql through get_safe_globals(). An authenticated attacker with permission to create or modify a Print Format can inject arbitrary Jinja expressions into the html field. Once the malicious Print Format is saved, the attacker can call get_html_and_style() with a target document (e.g., Supplier or Sales Invoice) to trigger the render process. This leads to information disclosure from the database, such as database version, schema details, or sensitive values, depending on the injected payload. Exploitation flow: Create a Print Format with SSTI payload in the html field; call the get_html_and_style() API; triggers frappe.render_template(template, doc) inside get_rendered_template(); leaks database information via frappe.db.sql or other exposed globals.	9.8	More Details
CVE-2025-66439	An issue was discovered in Frappe ERPNext through 15.89.0. Function get_outstanding_reference_documents() at erpnext.accounts.doctype.payment_entry.payment_entry.py is vulnerable to SQL Injection. It allows an attacker to extract arbitrary data from the database by injecting SQL payloads via the from_posting_date parameter, which is directly interpolated into the query without proper sanitization or parameter binding.	9.8	More Details
CVE-2025-66440	An issue was discovered in Frappe ERPNext through 15.89.0. Function get_outstanding_reference_documents() at erpnext/accounts/doctype/payment_entry/payment_entry.py is vulnerable to SQL Injection. It allows an attacker to extract arbitrary data from the database by injecting SQL payloads via the to_posting_date parameter, which is directly interpolated into the query without proper sanitization or parameter binding.	9.8	More Details
CVE-2025-65213	MooreThreads torch_musa through all versions contains an unsafe deserialization vulnerability in torch_musa.utils.compare_tool. The compare_for_single_op() and nan_inf_track_for_single_op() functions use pickle.load() on user-controlled file paths without validation, allowing arbitrary code execution. An attacker can craft a malicious pickle file that executes arbitrary Python code when loaded, enabling remote code execution with the privileges of the victim process.	9.8	More Details

CVE-2023-53894	phpfm 1.7.9 contains an authentication bypass vulnerability that allows attackers to log in by exploiting loose type comparison in password hash validation. Attackers can craft specific password hashes beginning with 0e or 00e to bypass authentication and upload malicious PHP files to the server.	9.8	More Details
CVE-2023-53895	PimpMyLog 1.7.14 contains an improper access control vulnerability that allows remote attackers to create admin accounts without authorization through the configuration endpoint. Attackers can exploit the unsanitized username field to inject malicious JavaScript, create a hidden backdoor account, and potentially access sensitive server-side log information and environmental variables.	9.8	More Details
CVE-2023-53899	PodcastGenerator 3.2.9 contains a blind server-side request forgery vulnerability that allows attackers to inject XML in the episode upload form. Attackers can manipulate the 'shortdesc' parameter to trigger external HTTP requests to arbitrary endpoints during podcast episode creation.	9.8	More Details
CVE-2025-46295	Apache Commons Text versions prior to 1.10.0 included interpolation features that could be abused when applications passed untrusted input into the text-substitution API. Because some interpolators could trigger actions like executing commands or accessing external resources, an attacker could potentially achieve remote code execution. This vulnerability has been fully addressed in FileMaker Server 22.0.4.	9.8	More Details
CVE-2025-36937	In AudioDecoder::HandleProduceRequest of audio_decoder.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2025-67728	Fireshare facilitates self-hosted media and link sharing. Versions 1.2.30 and below allow an authenticated user, or unauthenticated user if the Public Uploads setting is enabled, to craft a malicious filename when uploading a video file. The malicious filename is then concatenated directly into a shell command, which can be used for uploading files to arbitrary directories via path traversal, or executing system commands for Remote Code Execution (RCE). This issue is fixed in version 1.3.0.	9.8	More Details
CVE-2025-14534	A vulnerability was determined in UTT 进取 512W up to 3.1.7.7-171114. This impacts the function strcpy of the file /goform/formNatStaticMap of the component Endpoint. Executing manipulation of the argument NatBind can lead to buffer overflow. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2025-13764	The WP CarDealer plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.2.16. This is due to the 'WP_CarDealer_User::process_register' function not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site.	9.8	More Details
CVE-2025-67506	PipesHub is a fully extensible workplace AI platform for enterprise search and workflow automation. Versions prior to 0.1.0-beta expose POST /api/v1/record/buffer/convert through missing authentication. The endpoint accepts a file upload and converts it to PDF via LibreOffice by uploading payload to os.path.join(tmpdir, file.filename) without normalizing the filename. An attacker can submit a crafted filename containing ../ sequences to write arbitrary files anywhere the service account has permission, enabling remote file overwrite or planting malicious code. This issue is fixed in version 0.1.0-beta.	9.8	More Details
CVE-2025-13613	The Elated Membership plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.2. This is due to the plugin not properly logging in a user with the data that was previously verified through the 'eltdf_membership_check_facebook_user' and the 'eltdf_membership_login_user_from_social_network' function. This makes it possible for unauthenticated attackers to log in as administrative users, as long as they have an existing account on the site which can easily be created by default through the temp user functionality, and access to the administrative user's email.	9.8	More Details
CVE-2025-41730	An unauthenticated remote attacker can abuse unsafe sscanf calls within the check_account() function to write arbitrary data into fixed-size stack buffers which leads to full device compromise.	9.8	More Details
CVE-2025-41732	An unauthenticated remote attacker can abuse unsafe sscanf calls within the check_cookie() function to write arbitrary data into fixed-size stack buffers which leads to full device compromise.	9.8	More Details
CVE-2025-13184	Unauthenticated Telnet enablement via cstecgi.cgi (auth bypass) leading to unauthenticated root login with a blank password on factory/reset X5000R V9.1.0u.6369_B20230113 (arbitrary command execution). Earlier versions that share the same implementation, may also be affected.	9.8	More Details
CVE-2025-65820	An issue was discovered in Meatmeet Android Mobile Application 1.1.2.0. An exported activity can be spawned with the mobile application which opens a hidden page. This page, which is not available through the normal flows of the application, contains several devices which can be added to your account, two of which have not been publicly released. As a result of this vulnerability, the attacker can gain insight into unreleased Meatmeet devices.	9.8	More Details
CVE-2025-65826	The mobile application was found to contain stored credentials for the network it was developed on. If an attacker retrieved this, and found the physical location of the Wi-Fi network, they could gain unauthorized access to the Wi-Fi network of the vendor. Additionally, if an attacker were located in close physical proximity to the device when it was first set up, they may be able to force the device to auto-connect to an attacker-controlled access point by setting the SSID and password to the same as which was found in the firmware file.	9.8	More Details
CVE-2025-65294	Aqara Hub devices including Camera Hub G3 4.1.9_0027, Hub M2 4.3.6_0027, and Hub M3 4.3.6_0025 contain an undocumented remote access mechanism enabling unrestricted remote command execution.	9.8	More Details
CVE-2025-65823	The Meatmeet Pro was found to be shipped with hardcoded Wi-Fi credentials in the firmware, for the test network it was developed on. If an attacker retrieved this, and found the physical location of the Wi-Fi network, they could gain unauthorized access to the Wi-Fi network of the vendor. Additionally, if an attacker were located in close physical proximity to the device when it was first set up, they may be able to force the device to auto-connect to an attacker-controlled access point by setting the SSID and password to the same as which was found in the firmware file.	9.8	More Details
CVE-2025-66046	Several stack-based buffer overflow vulnerabilities exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.1. A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger these vulnerabilities.When Tag is 67	9.8	More Details
CVE-2025-66043	Several stack-based buffer overflow vulnerabilities exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.1. A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger these vulnerabilities.When Tag is 3	9.8	More Details

CVE-2025-66044	Several stack-based buffer overflow vulnerabilities exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.1. A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger these vulnerabilities.When Tag is 64	9.8	More Details
CVE-2025-66048	Several stack-based buffer overflow vulnerabilities exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.1. A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger these vulnerabilities.When Tag is 133	9.8	More Details
CVE-2025-66045	Several stack-based buffer overflow vulnerabilities exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.1. A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger these vulnerabilities.When Tag is 65	9.8	More Details
CVE-2025-66047	Several stack-based buffer overflow vulnerabilities exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.1. A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger these vulnerabilities.When Tag is 131	9.8	More Details
CVE-2025-67744	DeepChat is an open-source artificial intelligence agent platform that unifies models, tools, and agents. Prior to version 0.5.3, a security vulnerability exists in the Mermaid diagram rendering component that allows arbitrary JavaScript execution. Due to the exposure of the Electron IPC renderer to the DOM, this Cross-Site Scripting (XSS) flaw escalates to full Remote Code Execution (RCE), allowing an attacker to execute arbitrary system commands. Two concurrent issues, unsafe Mermaid configuration and an exposed IPC interface, cause this issue. Version 0.5.3 contains a patch.	9.6	More Details
CVE-2025-67511	Cybersecurity AI (CAI) is an open-source framework for building and deploying AI-powered offensive and defensive automation. Versions 0.5.9 and below are vulnerable to Command Injection through the run_ssh_command_with_credentials() function, which is available to AI agents. Only password and command inputs are escaped in run_ssh_command_with_credentials to prevent shell injection; while username, host and port values are injectable. This issue does not have a fix at the time of publication.	9.6	More Details
CVE-2025-67510	Neuron is a PHP framework for creating and orchestrating AI Agents. In versions 2.8.11 and below, the MySQLWriteTool executes arbitrary SQL provided by the caller using PDO::prepare() + execute() without semantic restrictions. This is consistent with the name (“write tool”), but in an LLM/agent context it becomes a high-risk capability: prompt injection or indirect prompt manipulation can cause execution of destructive queries such as DROP TABLE, TRUNCATE, DELETE, ALTER, or privilege-related statements (subject to DB permissions). Deployments that expose an agent with MySQLWriteTool enabled to untrusted input and/or run the tool with a DB user that has broad privileges are impacted. This issue is fixed in version 2.8.12.	9.4	More Details
CVE-2025-13607	A malicious actor can access camera configuration information, including account credentials, without authenticating when accessing a vulnerable URL.	9.4	More Details
CVE-2025-64537	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could lead to arbitrary code execution. An attacker could exploit this vulnerability by injecting malicious scripts into a web page that are executed in the context of the victim's browser. A successful attacker can abuse this to achieve session takeover, increasing the confidentiality and integrity impact as high. Exploitation of this issue requires user interaction in that a victim must visit a crafted malicious page.	9.3	More Details
CVE-2025-64539	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could lead to arbitrary code execution. An attacker could exploit this vulnerability by injecting malicious scripts into a web page that are executed in the context of the victim's browser. A successful attacker can abuse this to achieve session takeover, increasing the confidentiality and integrity impact as high. Exploitation of this issue requires user interaction in that a victim must visit a crafted malicious page.	9.3	More Details
CVE-2025-64538	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could lead to arbitrary code execution. An attacker could exploit this vulnerability by injecting malicious scripts into a web page that are executed in the context of the victim's browser. A successful attacker can abuse this to achieve session takeover, increasing the confidentiality and integrity impact as high. Exploitation of this issue requires user interaction in that a victim must visit a crafted malicious page.	9.3	More Details
CVE-2025-58130	Insufficiently Protected Credentials vulnerability in Apache Fineract. This issue affects Apache Fineract: through 1.11.0. The issue is fixed in version 1.12.1. Users are encouraged to upgrade to version 1.13.0, the latest release.	9.1	More Details
CVE-2025-66131	Missing Authorization vulnerability in yaadsarig Yaad Sarig Payment Gateway For WC yaad-sarig-payment-gateway-for-wc allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Yaad Sarig Payment Gateway For WC: from n/a through <= 2.2.10.	9.1	More Details
CVE-2025-55895	TOTOLINK A3300R V17.0.0cu.557_B20221024 and N200RE V9.3.5u.6448_B20240521 and V9.3.5u.6437_B20230519 are vulnerable to Incorrect Access Control. Attackers can send payloads to the interface without logging in (remote).	9.1	More Details
CVE-2025-61811	ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary code execution in the context of the current user. A high privileged attacker could leverage this vulnerability to bypass security measures and execute malicious code. Exploitation of this issue does not require user interaction and scope is changed.	9.1	More Details
CVE-2025-61809	ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized read and write access. Exploitation of this issue does not require user interaction and scope is unchanged.	9.1	More Details
CVE-2025-65473	An arbitrary file rename vulnerability in the /admin/filer.php component of EasyImages 2.0 v2.8.6 and below allows attackers with Administrator privileges to execute arbitrary code via injecting a crafted payload into an uploaded file name.	9.1	More Details
CVE-2025-65792	DataGear v5.5.0 is vulnerable to Arbitrary File Deletion.	9.1	More Details
CVE-2025-14265	In versions of ScreenConnect™ prior to 25.8, server-side validation and integrity checks within the extension subsystem could allow the installation and execution of untrusted or arbitrary extensions by authorized or administrative users. Abuse of this behavior could result in the execution of custom code on the server or unauthorized access to application configuration data. This issue affects only the ScreenConnect server component; host and guest clients are not impacted. ScreenConnect 25.8 introduces enhanced server-side configuration handling and integrity checks to ensure only trusted extensions can be installed.	9.1	More Details
CVE-2025-	In grav <1.7.49.5, a SSRF (Server-Side Request Forgery) vector may be triggered via Twig templates when page content is	9.1	More Details

66844	processed by Twig and the configuration allows undefined PHP functions to be registered		
CVE-2025-13888	A flaw was found in OpenShift GitOps. Namespace admins can create ArgoCD Custom Resources (CRs) that trick the system into granting them elevated permissions in other namespaces, including privileged namespaces. An authenticated attacker can then use these elevated permissions to create privileged workloads that run on master nodes, effectively giving them root access to the entire cluster.	9.1	More Details
CVE-2025-66430	Plesk 18.0 has Incorrect Access Control.	9.1	More Details
CVE-2025-13780	pgAdmin versions up to 9.10 are affected by a Remote Code Execution (RCE) vulnerability that occurs when running in server mode and performing restores from PLAIN-format dump files. This issue allows attackers to inject and execute arbitrary commands on the server hosting pgAdmin, posing a critical risk to the integrity and security of the database management system and underlying data.	9.1	More Details
CVE-2025-65827	The mobile application is configured to allow clear text traffic to all domains and communicates with an API server over HTTP. As a result, an adversary located "upstream" can intercept the traffic, inspect its contents, and modify the requests in transit. TThis may result in a total compromise of the user's account if the attacker intercepts a request with active authentication tokens or cracks the MD5 hash sent on login.	9.1	More Details
CVE-2025-65830	Due to a lack of certificate validation, all traffic from the mobile application can be intercepted. As a result, an adversary located "upstream" can decrypt the TLS traffic, inspect its contents, and modify the requests in transit. This may result in a total compromise of the user's account if the attacker intercepts a request with active authentication tokens or cracks the MD5 hash sent on login.	9.1	More Details
CVE-2025-61808	ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could lead to arbitrary code execution by a high priviledged attacker. Exploitation of this issue does not require user interaction and scope is changed.	9.1	More Details
CVE-2025-33210	NVIDIA Isaac Lab contains a deserialization vulnerability. A successful exploit of this vulnerability might lead to code execution.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2025-68116	FileRise is a self-hosted web file manager / WebDAV server. Versions prior to 2.7.1 are vulnerable to Stored Cross-Site Scripting (XSS) due to unsafe handling of brc renderable user uploads when served through the sharing and download endpoints. An attacker who can get a crafted SVG (primary) or HTML (secondary) file store FileRise instance can cause JavaScript execution when a victim opens a generated share link (and in some cases via the direct download endpoint). This impacts sh (`/api/file/share.php`) and direct file access / download path (`/api/file/download.php`), depending on browser/content-type behavior. Version 2.7.1 fixes the issue.
CVE-2025-56122	OS Command Injection vulnerability in Ruijie RG-EW1800GX PRO B11P226_EW1800GX-PRO_10223117 allowing attackers to execute arbitrary commands via a craf request to the module_get in file /usr/local/lua/dev_sta/networkConnect.lua.
CVE-2025-56107	OS Command Injection vulnerability in Ruijie RG-BCR RG-BCR600W allowing attackers to execute arbitrary commands via a crafted POST request to the submit_wif /usr/lib/lua/luci/controller/admin/common_quick_config.lua.
CVE-2025-56095	OS Command Injection vulnerability in Ruijie RG-EW1200G PRO RG-EW1200G PRO V1.00/V2.00/V3.00/V4.00 allowing attackers to execute arbitrary commands via POST request to the module_set in file /usr/local/lua/dev_sta/nbr_cwmp.lua.
CVE-2025-56096	OS Command Injection vulnerability in Ruijie RG-BCR RG-BCR600W allowing attackers to execute arbitrary commands via a crafted POST request to the restart_mo /usr/lib/lua/luci/controller/admin/common.lua.
CVE-2025-56097	OS Command Injection vulnerability in Ruijie RG-EW1800GX PRO B11P226_EW1800GX-PRO_10223117 allowing attackers to execute arbitrary commands via a craf request to the module_set in file /usr/local/lua/dev_config/config_retain.lua.
CVE-2025-56098	OS Command Injection vulnerability in Ruijie X30-PRO X30-PRO-V1_09241521 allowing attackers to execute arbitrary commands via a crafted POST request to the file /usr/local/lua/dev_sta/networkConnect.lua.
CVE-2025-56099	OS Command Injection vulnerability in Ruijie RG-YST AP_3.0(1)B11P280YST250F allowing attackers to execute arbitrary commands via a crafted POST request to th in file /usr/lib/lua/luci/modules/common.lua.
CVE-2025-56101	OS Command Injection vulnerability in Ruijie M18 EW_3.0(1)B11P226_M18_10223116 allowing attackers to execute arbitrary commands via a crafted POST request module_get in file /usr/local/lua/dev_sta/networkConnect.lua.
CVE-2025-56102	OS Command Injection vulnerability in Ruijie RG-EW1800GX B11P226_EW1800GX_10223121 allowing attackers to execute arbitrary commands via a crafted POST module_get in file /usr/local/lua/dev_sta/networkConnect.lua.
CVE-2025-56106	OS Command Injection vulnerability in Ruijie RG-EW1800GX B11P226_EW1800GX_10223121 allowing attackers to execute arbitrary commands via a crafted POST module_set in file /usr/local/lua/dev_sta/nbr_cwmp.lua.
CVE-2025-56108	OS Command Injection vulnerability in Ruijie X30-PRO X30-PRO-V1_09241521 allowing attackers to execute arbitrary commands via a crafted POST request to the file /usr/lib/lua/luci/modules/common.lua.
CVE-2025-	OS Command Injection vulnerability in Ruijie X30-PRO X30-PRO-V1_09241521 allowing attackers to execute arbitrary commands via a crafted POST request to the

56093	/usr/lib/lua/luci/modules/wireless.lua.
CVE-2025-56109	OS Command Injection vulnerability in Ruijie RG-BCR RG-BCR860 allowing attackers to execute arbitrary commands via a crafted POST request to the action_wirele /usr/lib/lua/luci/control/admin/wireless.lua.
CVE-2025-56110	OS Command Injection vulnerability in Ruijie RG-BCR RG-BCR860 allowing attackers to execute arbitrary commands via a crafted POST request to the action_deal_ /usr/lib/lua/luci/controller/api/rcmsAPI.lua.
CVE-2025-56111	OS Command Injection vulnerability in Ruijie RG-BCR RG-BCR860 allowing attackers to execute arbitrary commands via a crafted POST request to the network_set_ file /usr/lib/lua/luci/controller/admin/netport.lua.
CVE-2025-56113	OS Command Injection vulnerability in Ruijie RG-YST EST, YSTAP_3.0(1)B11P280YST250F V1.xxV2.xx allowing attackers to execute arbitrary commands via a crafte request to the pwdmodify in file /usr/lib/lua/luci/modules/common.lua.
CVE-2025-56114	OS Command Injection vulnerability in Ruijie M18 EW_3.0(1)B11P226_M18_10223116 allowing attackers to execute arbitrary commands via a crafted POST request module_set in file /usr/local/lua/dev_config/config_retain.lua.
CVE-2025-56117	OS Command Injection vulnerability in Ruijie X30-PRO X30-PRO-V1_09241521 allowing attackers to execute arbitrary commands via a crafted POST request to the file /usr/local/lua/dev_sta/nbr_cwmp.lua.
CVE-2025-56118	OS Command Injection vulnerability in Ruijie X60 PRO X60_10212014RG-X60 PRO V1.00/V2.00 allowing attackers to execute arbitrary commands via a crafted POS the module_set in file /usr/local/lua/dev_sta/nbr_cwmp.lua.
CVE-2025-56120	OS Command Injection vulnerability in Ruijie X60 PRO X60_10212014RG-X60 PRO V1.00/V2.00 allowing attackers to execute arbitrary commands via a crafted POS the module_set in file /usr/local/lua/dev_config/config_retain.lua.
CVE-2025-56094	OS Command Injection vulnerability in Ruijie X30-PRO X30-PRO-V1_09241521 allowing attackers to execute arbitrary commands via a crafted POST request to the file /usr/local/lua/dev_sta/host_access_delay.lua.
CVE-2025-56092	OS Command Injection vulnerability in Ruijie X30 PRO V1 X30-PRO-V1_09241521 allowing attackers to execute arbitrary commands via a crafted POST request to t module_get in file /usr/local/lua/dev_sta/networkConnect.lua.
CVE-2025-56123	OS Command Injection vulnerability in Ruijie RG-EW1200G PRO RG-EW1200G PRO V1.00/V2.00/V3.00/V4.00 allowing attackers to execute arbitrary commands via POST request to the module_get in file /usr/local/lua/dev_sta/networkConnect.lua.
CVE-2025-56082	OS Command Injection vulnerability in Ruijie RG-BCR RG-BCR600W allowing attackers to execute arbitrary commands via a crafted POST request to the check_cha /usr/lib/lua/luci/controller/admin/common.lua.
CVE-2024-58283	WBCE CMS version 1.6.2 contains a remote code execution vulnerability that allows authenticated attackers to upload malicious PHP files through the Elfinder file m Attackers can exploit the file upload functionality in the elfinder connector to upload a web shell and execute arbitrary system commands through a user-controlled
CVE-2025-44016	A vulnerability in TeamViewer DEX Client (former 1E client) - Content Distribution Service (NomadBranch.exe) prior version 25.11 for Windows allows malicious act file integrity validation via a crafted request. By providing a valid hash for a malicious file, an attacker can cause the service to incorrectly validate and process the trusted, enabling arbitrary code execution under the Nomad Branch service context.
CVE-2025-14526	A security flaw has been discovered in Tenda CH22 1.0.0.1. This affects the function frmL7ImForm of the file /goform/L7Im. Performing manipulation of the argume results in buffer overflow. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.
CVE-2025-65471	An arbitrary file upload vulnerability in the /admin/manager.php component of EasyImages 2.0 v2.8.6 and below allows attackers to execute arbitrary code via uplo crafted PHP file.
CVE-2025-65472	A Cross-Site Request Forgery (CSRF) in the /admin/admin.inc.php component of EasyImages 2.0 v2.8.6 and below allows attackers to escalate privileges to Adminis user interaction with a malicious web page.
CVE-2023-53900	Spip 4.1.10 contains a file upload vulnerability that allows attackers to upload malicious SVG files with embedded external links. Attackers can trick administrators crafted SVG logo that redirects to a potentially dangerous URL through improper file upload filtering.
CVE-2025-56077	OS Command Injection vulnerability in Ruijie RG-RAP2200(E) 247 2200 allowing attackers to execute arbitrary commands via a crafted POST request to the module /usr/local/lua/dev_sta/nbr_cwmp.lua.
CVE-2025-56079	OS Command Injection vulnerability in Ruijie RG-EW1300G EW1300G V1.00/V2.00/V4.00 allowing attackers to execute arbitrary commands via a crafted POST requ module_get in file /usr/local/lua/dev_sta/networkConnect.lua.
CVE-2025-56083	OS Command Injection vulnerability in Ruijie X30-PRO X30-PRO-V1_09241521 allowing attackers to execute arbitrary commands via a crafted POST request to the file /usr/local/lua/dev_sta/nbr_networkId_merge.lua.
CVE-2025-66918	edoc-doctor-appointment-system v1.0.1 is vulnerable to Cross Site Scripting (XSS) in admin/add-session.php via the "title" parameter.

CVE-2025-56084	OS Command Injection vulnerability in Ruijie RG-EW1800GX PRO B11P226_EW1800GX-PRO_10223117 allowing attackers to execute arbitrary commands via a craf request to the module_set in file /usr/local/lua/dev_sta/nbr_cwmp.lua.
CVE-2025-56085	OS Command Injection vulnerability in Ruijie RG-EW1200 EW_3.0(1)B11P227_EW1200_11130208RG-EW1200 V1.00 allowing attackers to execute arbitrary comma crafted POST request to the module_set in file /usr/local/lua/dev_config/config_retain.lua.
CVE-2025-56086	OS Command Injection vulnerability in Ruijie RG-EW1200 EW_3.0(1)B11P227_EW1200_11130208RG-EW1200 V1.00 allowing attackers to execute arbitrary comma crafted POST request to the module_get in file /usr/local/lua/dev_sta/networkConnect.lua.
CVE-2025-56087	OS Command Injection vulnerability in Ruijie RG-BCR RG-BCR600W allowing attackers to execute arbitrary commands via a crafted POST request to the run_tcpdur /usr/lib/lua/luci/controller/admin/common_tcpdump.lua.
CVE-2025-56088	OS Command Injection vulnerability in Ruijie RG-BCR RG-BCR860 allowing attackers to execute arbitrary commands via a crafted POST request to the action_servic /usr/lib/lua/luci/controller/admin/service.lua.
CVE-2025-56089	OS Command Injection vulnerability in Ruijie M18 EW_3.0(1)B11P226_M18_10223116 allowing attackers to execute arbitrary commands via a crafted POST request module_set in file /usr/local/lua/dev_sta/nbr_cwmp.lua.
CVE-2025-56090	OS Command Injection vulnerability in Ruijie RG-EW1200G PRO RG-EW1200G PRO V1.00/V2.00/V3.00/V4.00 allowing attackers to execute arbitrary commands via POST request to the module_set in file /usr/local/lua/dev_config/config_retain.lua.
CVE-2025-56091	OS Command Injection vulnerability in Ruijie RG-EW1800GX B11P226_EW1800GX_10223121 allowing attackers to execute arbitrary commands via a crafted POST module_set in file /usr/local/lua/dev_config/config_retain.lua.
CVE-2025-65824	An unauthenticated attacker within proximity of the Meatmeet device can perform an unauthorized Over The Air (OTA) firmware upgrade using Bluetooth Low Ener resulting in the firmware on the device being overwritten with the attacker's code. As the device does not perform checks on upgrades, this results in Remote Code (RCE) and the victim losing complete access to the Meatmeet.
CVE-2025-65950	WBCE CMS is a content management system. In versions 1.6.4 and below, the user management module allows a low-privileged authenticated user with permissio users to execute arbitrary SQL queries. This can be escalated to a full database compromise, data exfiltration, effectively bypassing all security controls. The vulne in the admin/users/save.php script, which handles updates to user profiles. The script improperly processes the groups[] parameter sent from the user edit form. Th fixed in version 1.6.5.
CVE-2024-2104	Due to improper BLE security configurations on the device's GATT server, an adjacent unauthenticated attacker can read and write device control commands throu app service wich could render the device unusable.
CVE-2025-14655	A security flaw has been discovered in Tenda AC20 16.03.08.12. The impacted element is the function formSetRebootTimer of the file /goform/SetSysAutoRebbotC component httpd. Performing manipulation of the argument rebootTime results in stack-based buffer overflow. The attack is possible to be carried out remotely. Th been released to the public and may be exploited.
CVE-2025-43539	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. Processing a file may lead to memory
CVE-2025-56127	OS Command Injection vulnerability in Ruijie RG-BCR RG-BCR600W allowing attackers to execute arbitrary commands via a crafted POST request to the get_wanob /usr/lib/lua/luci/controller/admin/common.lua.
CVE-2025-13094	The WP3D Model Import Viewer plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the handle_import_file() function in up to, and including, 1.0.7. This makes it possible for authenticated attackers, with Author-level access and above, to upload arbitrary files on the affected site's se may make remote code execution possible.
CVE-2025-14397	The Postem Ipsum plugin for WordPress is vulnerable to unauthorized modification of data to Privilege Escalation due to a missing capability check on the postem_ipsum_generate_users() function in all versions up to, and including, 3.0.1. This makes it possible for authenticated attackers, with Subscriber-level access create arbitrary user accounts with the administrator role.
CVE-2025-14476	The Doubly – Cross Domain Copy Paste for WordPress plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.0.46 via dese untrusted input from the content.txt file within uploaded ZIP archives. This makes it possible for authenticated attackers, with Subscriber-level access and above, t Object. The additional presence of a POP chain allows attackers to execute arbitrary code, delete files, retrieve sensitive data, or perform other actions depending available gadgets. This is only exploitable by subscribers, when administrators have explicitly enabled that access.
CVE-2025-14654	A vulnerability was identified in Tenda AC20 16.03.08.12. The affected element is the function formSetPPTPUserList of the file /goform/setPptpUserList of the comp Such manipulation of the argument list leads to stack-based buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be us
CVE-2025-14656	A weakness has been identified in Tenda AC20 16.03.08.12. This affects the function httpd of the file /goform/openSchedWifi. Executing manipulation of the argum schedStartTime/schedEndTime can lead to buffer overflow. The attack may be performed from remote. The exploit has been made available to the public and coul exploited.
CVE-2024-58314	Atcom 100M IP Phones firmware version 2.7.x.x contains an authenticated command injection vulnerability in the web configuration CGI script that allows attackers arbitrary system commands. Attackers can inject shell commands through the 'cmd' parameter in web_cgi_main.cgi, enabling remote code execution with adminis credentials.
CVE-2025-14659	A vulnerability was detected in D-Link DIR-860LB1 and DIR-868LB1 203b01/203b03. Affected is an unknown function of the component DHCP Daemon. The manipu argument Hostname results in command injection. It is possible to launch the attack remotely. The exploit is now public and may be used.
CVE-2024-	FNT Command 13.4.0 is vulnerable to Code Execution via the C Base Module.

44598	
CVE-2025-60786	A Zip Slip vulnerability in the import a Project component of iceScrum v7.54 Pro On-prem allows attackers to execute arbitrary code via uploading a crafted Zip file
CVE-2025-66437	An SSTI (Server-Side Template Injection) vulnerability exists in the get_address_display method of Frappe ERPNext through 15.89.0. This function renders address using frappe.render_template() with a context derived from the address_dict parameter, which can be either a dictionary or a string referencing an Address docum ERPNext uses a custom Jinja2 SandboxedEnvironment, dangerous functions like frappe.db.sql remain accessible via get_safe_globals(). An authenticated attacker permission to create or modify an Address Template can inject arbitrary Jinja expressions into the template field. By creating an Address document with a matchin then calling the get_address_display API with address_dict="address_name", the system will render the malicious template using attacker-controlled data. This lea side code execution or database information disclosure.
CVE-2025-9121	Pentaho Data Integration and Analytics Community Dashboard Editor plugin versions before 10.2.0.4, including 9.3.0.x and 8.3.x, deserialize untrusted JSON data constraining the parser to approved classes and methods.
CVE-2025-66449	ConvertXis a self-hosted online file converter. In versions prior to 0.16.0, the endpoint `/upload` allows an authenticated user to write arbitrary files on the system, binaries and allowing code execution. The upload function takes `file.name` directly from user supplied data without doing any sanitization on the name thus allow arbitrary file write. This can be used to overwrite system binaries with ones provided from an attacker allowing full code execution. Version 0.16.0 contains a patch
CVE-2025-14174	Out of bounds memory access in ANGLE in Google Chrome on Mac prior to 143.0.7499.110 allowed a remote attacker to perform out of bounds memory access via HTML page. (Chromium security severity: High)
CVE-2025-14572	A vulnerability was found in UTT 进取 512W up to 1.7.7-171114. This affects an unknown part of the file /goform/formWebAuthGlobalConfig. Performing manipulatio argument hidcontact results in memory corruption. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The vendor contacted early about this disclosure but did not respond in any way.
CVE-2024-58305	WonderCMS 4.3.2 contains a cross-site scripting vulnerability that allows attackers to inject malicious JavaScript through the module installation endpoint. Attacker specially designed XSS payload to install a reverse shell module and execute remote commands by tricking an authenticated administrator into accessing a malicio
CVE-2025-66446	MaxKB is an open-source AI assistant for enterprise. Versions 2.3.1 and below have improper file permissions which allow attackers to overwrite the built-in dynam other critical files, potentially resulting in privilege escalation. This issue is fixed in version 2.4.0.
CVE-2025-56129	OS Command Injection vulnerability in Ruijie RG-BCR RG-BCR860 allowing attackers to execute arbitrary commands via a crafted POST request to the action_diagn /usr/lib/lua/luci/controller/admin/diagnosis.lua.
CVE-2025-56130	OS Command Injection vulnerability in Ruijie RG-S1930 S1930SWITCH_3.0(1)B11P230 allowing attackers to execute arbitrary commands via a crafted POST reques module_update in file /usr/local/lua/dev_config/ace_sw.lua.
CVE-2025-13481	IBM Aspera Orchestrator 4.0.0 through 4.1.0 could allow an authenticated user to execute arbitrary commands with elevated privileges on the system due to impro of user supplied input.
CVE-2025-14390	The Video Merchant plugin for WordPress is vulnerable to Cross-Site Request Forgery in version <= 5.0.4. This is due to missing or incorrect nonce validation on th video_merchant_add_video_file() function. This makes it possible for unauthenticated attackers to upload arbitrary files that make remote code execution possible request granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-66429	An issue was discovered in cPanel 110 through 132. A directory traversal vulnerability within the Team Manager API allows for overwrite of an arbitrary file. This ca privilege escalation to the root user.
CVE-2024-58294	FreePBX 16 contains an authenticated remote code execution vulnerability in the API module that allows attackers with valid session credentials to execute arbitra Attackers can exploit the 'generatedocs' endpoint by crafting malicious POST requests with bash command injection to establish remote shell access.
CVE-2025-34506	WBCE CMS version 1.6.3 and prior contains an authenticated remote code execution vulnerability that allows administrators to upload malicious modules. Attacker specially designed ZIP module with embedded PHP reverse shell code to gain remote system access when the module is installed.
CVE-2025-66419	MaxKB is an open-source AI assistant for enterprise. In versions 2.3.1 and below, the tool module allows an attacker to escape the sandbox environment and escal under certain concurrent conditions. This issue is fixed in version 2.4.0.
CVE-2025-12824	The Player Leaderboard plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.0.2 via the 'player_leaderboard' shortcode. T the plugin using an unsanitized user-supplied value from the shortcode's 'mode' attribute in a call to include() without proper path validation. This makes it possibl authenticated attackers, with Contributor-level access and above, to include and execute arbitrary PHP files on the server, allowing the execution of any PHP code This can be used to bypass access controls, obtain sensitive data, or achieve full remote code execution if combined with file upload capabilities.
CVE-2025-12968	The Infility Global plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation and capability checks in all versions up to, and inclu This is due to the `upload_file` function in the `infility_import_file` class only validating the MIME type which can be easily spoofed, and the `import_data` function capability checks. This makes it possible for authenticated attackers, with subscriber level access and above, to upload arbitrary files on the affected site's server make remote code execution possible.
CVE-2025-26866	A remote code execution vulnerability exists where a malicious Raft node can exploit insecure Hessian deserialization within the PD store. The fix enforces IP-based authentication to restrict cluster membership and implements a strict class whitelist to harden the Hessian serialization process against object injection attacks. Us recommended to upgrade to version 1.7.0, which fixes the issue.
CVE-2025-13506	Execution with Unnecessary Privileges vulnerability in Nebim Neyir Computer Industry and Services Inc. Nebim V3 ERP allows Expanding Control over the Operating the Database.This issue affects Nebim V3 ERP: from 2.0.59 before 3.0.1.
CVE-	

2025-65530	An eval injection in the malware de-obfuscation routines of CloudLinux ai-bolit before v32.7.4 allows attackers to overwrite arbitrary files as root via scanning a cra
CVE-2025-11393	A flaw was found in runtimes-inventory-rhel8-operator. An internal proxy component is incorrectly configured. Because of this flaw, the proxy attaches the cluster's administrative credentials to any command it receives, instead of only the specific reports it is supposed to handle. This allows a standard user within the cluster to unauthorized commands to the management platform, effectively acting with the full permissions of the cluster administrator. This could lead to unauthorized char cluster's configuration or status on the Red Hat platform.
CVE-2025-12716	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.4 before 18.4.6, 18.5 before 18.5.4, and 18.6 before 18.6.2 that, under certain condit have allowed an authenticated user to perform unauthorized actions on behalf of another user by creating wiki pages with malicious content.
CVE-2025-8083	The Preset configuration https://v2.vuetifyjs.com/en/features/presets feature of Vuetify is vulnerable to Prototype Pollution https://cheatsheetseries.owasp.org/cheatsheets/Prototype_Pollution_Prevention_Cheat_Sheet.html due to the internal 'mergeDeep' utility function used to merge c defaults. Using a specially-crafted, malicious preset can result in polluting all JavaScript objects with arbitrary properties, which can further negatively affect all asp application's behavior. This can lead to a wide range of security issues, including resource exhaustion/denial of service or unauthorized access to data. If the applic utilizes Server-Side Rendering (SSR), this vulnerability could affect the whole server process. This issue affects Vuetify versions greater than or equal to 2.2.0-beta. than 3.0.0-alpha.10. Note: Version 2.x of Vuetify is End-of-Life and will not receive any updates to address this issue. For more information see here https://v2.vuetifyjs.com/en/about/eol/ .
CVE-2025-68055	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themefic Hydra Booking hydra-booking allows SQL Injection affects Hydra Booking: from n/a through <= 1.1.32.
CVE-2025-68054	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup CountDown With Image or Video Background countdown_with_background allows Blind SQL Injection.This issue affects CountDown With Image or Video Background: from n/a through <= 1.5.
CVE-2025-67738	squid/cachemgr.cgi in Webmin before 2.600 does not properly quote arguments. This is relevant if Webmin's Squid module and its Cache Manager feature are avai untrusted party is able to authenticate to Webmin and has certain Cache Manager permissions (the "cms" security option).
CVE-2025-68053	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup xPromoter top_bar_promoter allows Blind SQI issue affects xPromoter: from n/a through <= 1.3.4.
CVE-2025-68056	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup LBG Zoominoutslider lbg_zoominoutslider allo Injection.This issue affects LBG Zoominoutslider: from n/a through <= 5.4.5.
CVE-2025-67950	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Syed Balkhi All In One SEO Pack all-in-one-seo-pack allows B Injection.This issue affects All In One SEO Pack: from n/a through <= 4.9.1.
CVE-2025-14443	A flaw was found in ose-openshift-apiserver. This vulnerability allows internal network enumeration, service discovery, limited information disclosure, and potential service (DoS) through Server-Side Request Forgery (SSRF) due to missing IP address and network-range validation when processing user-supplied image reference
CVE-2025-67505	Okta Java Management SDK facilitates interactions with the Okta management API. In versions 11.0.0 through 20.0.0, race conditions may arise from concurrent re the ApiClient class. This could cause a status code or response header from one request's response to influence another request's response. This issue is fixed in v
CVE-2025-61812	ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Improper Input Validation vulnerability that could allow a high privileged attacker to g code execution. Exploitation of this issue does not require user interaction.
CVE-2025-67750	Lightning Flow Scanner provides a A CLI plugin, VS Code Extension and GitHub Action for analysis and optimization of Salesforce Flows. Versions 6.10.5 and below maliciously crafted flow metadata file to cause arbitrary JavaScript execution during scanning. The APIVersion rule uses new Function() to evaluate expression strin an attacker to supply a malicious expression within rule configuration or crafted flow metadata. This could compromise developer machines, CI runners, or editor e This issue is fixed in version 6.10.6.
CVE-2025-61810	ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execu context of the current user. A high privileged attacker could exploit this vulnerability by providing maliciously crafted serialized data to the application. Exploitation requires user interaction and scope is changed.
CVE-2025-65807	An issue in sd command v1.0.0 and before allows attackers to escalate privileges to root via a crafted command.
CVE-2025-33225	NVIDIA Resiliency Extension for Linux contains a vulnerability in log aggregation, where an attacker could cause predictable log-file names. A successful exploit of t vulnerability may lead to escalation of privileges, code execution, denial of service, information disclosure, and data tampering.
CVE-2024-44599	FNT Command 13.4.0 is vulnerable to Directory Traversal.
CVE-2025-65742	An unauthenticated Broken Function Level Authorization (BFLA) vulnerability in Newgen OmniDocs v11.0 allows attackers to obtain sensitive information and execu account takeover via a crafted API request.
CVE-2025-66675	Denial of Service vulnerability in Apache Struts, file leak in multipart request processing causes disk exhaustion. This issue affects Apache Struts: from 2.0.0 throug 7.0.0 through 7.0.3. Users are recommended to upgrade to version 6.8.0 or 7.1.1, which fixes the issue. It's related to https://cve.org/CVERecord?id=CVE-2025-64 addresses missing affected version 6.7.4
CVE-2025-14523	A flaw in libsoup's HTTP header handling allows multiple Host: headers in a request and returns the last occurrence for server-side processing. Common front proxi the first Host: header, so this mismatch can cause vhost confusion where a proxy routes a request to one backend but the backend interprets it as destined for anc This discrepancy enables request-smuggling style attacks, cache poisoning, or bypassing host-based access controls when an attacker supplies duplicate Host hea

CVE-2025-66492	Masa CMS is an open source Enterprise Content Management platform. Versions 7.2.8 and below, 7.3.1 through 7.3.13, 7.4.0-alpha.1 through 7.4.8 and 7.5.0 throu vulnerable to XSS when an unsanitized value of the ajax URL query parameter is directly included within the <head> section of the HTML page. An attacker can ex arbitrary scripts in the context of the user's session, potentially leading to Session Hijacking, Data Theft, Defacement and Malware Distribution. This issue is fixed i 7.5.2, 7.4.9, 7.3.14, and 7.2.9. To work around this issue, configure a Web Application Firewall (WAF) rule (e.g., ModSecurity) to block requests containing common characters in the ajax query parameter. Alternatively, implement server-side sanitization using middleware to strip or escape dangerous characters from the ajax p before it reaches the vulnerable rendering logic.
CVE-2025-67509	Neuron is a PHP framework for creating and orchestrating AI Agents. Versions 2.8.11 and below use MySQLSelectTool, which is vulnerable to Read-Only Bypass. My is intended to be a read-only SQL tool (e.g., for LLM agent querying, however, validation based on the first keyword (e.g., SELECT) and a forbidden-keyword list doe file-writing constructs such as INTO OUTFILE / INTO DUMPFILE. As a result, an attacker who can influence the tool input (e.g., via prompt injection through a public endpoint) may write arbitrary files to the DB server if the MySQL/MariaDB account has the FILE privilege and server configuration permits writes to a useful locatio accessible directory). This issue is fixed in version 2.8.12.
CVE-2025-65781	An issue was discovered in Wekan The Open Source kanban board system up to version 18.15, fixed in 18.16. Attachment upload API treats the Authorization bear userId and enters a non-terminating body-handling branch for any non-empty bearer token, enabling trivial application-layer DoS and latent identity-spoofing.
CVE-2025-61813	ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files on the server. Exploitation of this issue does not require user interacti is changed.
CVE-2025-10451	Unchecked output buffer may allowed arbitrary code execution in SMM and potentially result in SMM memory corruption.
CVE-2025-14002	The WPCOM Member plugin for WordPress is vulnerable to authentication bypass via brute force in all versions up to, and including, 1.7.16. This is due to weak OTP Password) generation using only 6 numeric digits combined with a 10-minute validity window and no rate limiting on verification attempts. This makes it possible f unauthenticated attackers to brute-force the verification code and authenticate as any user, including administrators, if they know the target's phone number, and does not notice or ignores the SMS notification with the OTP.
CVE-2025-68154	systeminformation is a System and OS information library for node.js. In versions prior to 5.27.14, the `fsSize()` function in systeminformation is vulnerable to OS c injection on Windows systems. The optional `drive` parameter is directly concatenated into a PowerShell command without sanitization, allowing arbitrary commar when user-controlled input reaches this function. The actual exploitability depends on how applications use this function. If an application does not pass user-contr `fsSize()`, it is not vulnerable. Version 5.27.14 contains a patch.
CVE-2025-67900	NXLog Agent before 6.11 can load a file specified by the OPENSSL_CONF environment variable.
CVE-2025-58137	Authorization Bypass Through User-Controlled Key vulnerability in Apache Fineract. This issue affects Apache Fineract: through 1.11.0. The issue is fixed in version are encouraged to upgrade to version 1.13.0, the latest release.
CVE-2025-14044	The Visitor Logic Lite plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.0.3 via deserialization of untrusted input from cookie. This is due to the `lp_track()` function passing unsanitized cookie data directly to the `unserialize()` function. This makes it possible for unauthenticated at inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on the target sy allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code granted they can access the WordPress site.
CVE-2025-67507	Filament is a collection of full-stack components for accelerated Laravel development. Versions 4.0.0 through 4.3.0 contain a flaw in the handling of recovery code based multi-factor authentication, allowing the same recovery code to be reused indefinitely. This issue does not affect email-based MFA. It also only applies when codes are enabled. This issue is fixed in version 4.3.1.
CVE-2025-14475	The Extensive VC Addons for WPBakery page builder plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.9.1 via the `extensive_vc_get_module_template_part` function. This is due to insufficient path normalization and validation of the user-supplied `shortcode_name` parameter `extensive_vc_init_shortcode_pagination` AJAX action. This makes it possible for unauthenticated attackers to include and execute arbitrary PHP files on the server execution of any PHP code in those files via the `shortcode_name` parameter.
CVE-2025-13334	The Blaze Demo Importer plugin for WordPress is vulnerable to unauthorized database resets and file deletion due to a missing capability check on the "blaze_demo_importer_install_demo" function in all versions up to, and including, 1.0.13. This makes it possible for authenticated attackers, with subscriber level a above, to reset the database by truncating all tables (except options, usermeta, and users), delete all sidebar widgets, theme modifications, and content of the upl
CVE-2025-65778	An issue was discovered in Wekan The Open Source kanban board system up to version 18.15, fixed in 18.16. Uploaded attachments can be served with attacker-c Content-Type (text/html), allowing execution of attacker-supplied HTML/JS in the application's origin and enabling session/token theft and CSRF actions.
CVE-2025-13148	IBM Aspera Orchestrator 4.0.0 through 4.1.0 could allow could an authenticated user to change the password of another user without prior knowledge of that passv
CVE-2025-65295	Multiple vulnerabilities in Aqara Hub firmware update process in the Camera Hub G3 4.1.9_0027, Hub M2 4.3.6_0027, and Hub M3 4.3.6_0025 devices, allow attack malicious firmware without proper verification. The device fails to validate firmware signatures during updates, uses outdated cryptographic methods that can be e forge valid signatures, and exposes information through improperly initialized memory.
CVE-2025-36923	In NrmmDecoder::DecodeSORTransparentContext of cn_NrmmDecoder.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead t (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-67641	Jenkins Coverage Plugin 2.3054.ve1ff7b_a_a_123b_ and earlier does not validate the configured coverage results ID when creating coverage results, only when sub job configuration through the UI, allowing attackers with Item/Configure permission to use a `javascript:` scheme URL as identifier by configuring the job through th resulting in a stored cross-site scripting (XSS) vulnerability.
CVE-2025-13970	OpenPLC_V3 is vulnerable to a cross-site request forgery (CSRF) attack due to the absence of proper CSRF validation. This issue allows an unauthenticated attacke logged-in administrator into visiting a maliciously crafted link, potentially enabling unauthorized modification of PLC settings or the upload of malicious programs w lead to significant disruption or damage to connected systems.
CVE-2025-	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.11 before 18.4.6, 18.5 before 18.5.4, and 18.6 before 18.6.2 that could have, under c circumstances, allowed an unauthenticated user to perform unauthorized actions on behalf of another user by injecting malicious external scripts into the Swagger

12029	
CVE-2025-36924	In ss_DecodeLcsAssistDataReqMsg(void) of ss_LcsManagement.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remo (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-33226	NVIDIA NeMo Framework for all platforms contains a vulnerability where malicious data created by an attacker may cause a code injection. A successful exploit of t vulnerability may lead to code execution, escalation of privileges, information disclosure, and data tampering.
CVE-2025-33235	NVIDIA Resiliency Extension for Linux contains a vulnerability in the checkpointing core, where an attacker may cause a race condition. A successful exploit of this might lead to information disclosure, data tampering, denial of service, or escalation of privileges.
CVE-2025-64669	Improper access control in Windows Admin Center allows an authorized attacker to elevate privileges locally.
CVE-2025-36925	In WAVES_send_data_to_dsp of libaoc_waves.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privileg additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-40829	A vulnerability has been identified in Simcenter Femap (All versions < V2512). The affected applications contains an uninitialized memory vulnerability while parsir crafted SLDPRT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-27146)
CVE-2025-55314	An issue was discovered in Foxit PDF and Editor for Windows and macOS before 13.2 and 2025 before 2025.2. When pages in a PDF are deleted via JavaScript, the may fail to properly update internal states. Subsequent annotation management operations assume these states are valid, causing dereference of invalid or releas This can lead to memory corruption, application crashes, and potentially allow an attacker to execute arbitrary code.
CVE-2025-55313	An issue was discovered in Foxit PDF and Editor for Windows and macOS before 13.2 and 2025 before 2025.2. They allow potential arbitrary code execution when crafted PDF files. The vulnerability stems from insufficient handling of memory allocation failures after assigning an extremely large value to a form field's charLimi JavaScript. This can result in memory corruption and may allow an attacker to execute arbitrary code by persuading a user to open a malicious file.
CVE-2025-55312	An issue was discovered in Foxit PDF and Editor for Windows before 13.2 and 2025 before 2025.2. When pages in a PDF are deleted via JavaScript, the application properly update internal states. Subsequent annotation management operations assume these states are valid, causing dereference of invalid or released memory lead to memory corruption, application crashes, and potentially allow an attacker to execute arbitrary code.
CVE-2025-10882	AA maliciously crafted X_T file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage thi to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.
CVE-2025-43320	The issue was addressed by adding additional logic. This issue is fixed in macOS Sequoia 15.7.3. An app may be able to bypass launch constraint protections and e malicious code with elevated privileges.
CVE-2025-43402	The issue was addressed with improved memory handling. This issue is fixed in macOS Tahoe 26.1. An app may be able to cause unexpected system termination c process memory.
CVE-2025-43467	This issue was addressed with improved checks. This issue is fixed in macOS Tahoe 26.1. An app may be able to gain root privileges.
CVE-2025-43512	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. An app may be able to elevate privileges.
CVE-2025-36927	In GetTachyonCommand of tachyon_server_common.h, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of no additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-43527	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.3. An app may be able to gain root privileges.
CVE-2025-46285	An integer overflow was addressed by adopting 64-bit timestamps. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. An app may be able to gai privileges.
CVE-2025-67460	Protection Mechanism Failure of Software Downgrade in Zoom Rooms for Windows before 6.6.0 may allow an unauthenticated user to conduct an escalation of priv access.
CVE-2025-10881	A maliciously crafted CATPRODUCT file, when parsed through certain Autodesk products, can force a Heap-Based Overflow vulnerability. A malicious actor can leve vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
CVE-2025-65199	A command injection vulnerability exists in Windscribe for Linux Desktop App that allows a local user who is a member of the windscribe group to execute arbitrary as root via the 'adapterName' parameter of the 'changeMTU' function. Fixed in Windscribe v2.18.3-alpha and v2.18.8.
CVE-2025-10883	A maliciously crafted CATPRODUCT file, when parsed through certain Autodesk products, can force an Out-of-Bounds Read vulnerability. A malicious actor can leve vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
CVE-2025-9455	A maliciously crafted CATPRODUCT file, when parsed through certain Autodesk products, can force an Out-of-Bounds Read vulnerability. A malicious actor can leve vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.

CVE-2025-9457	A maliciously crafted PRT file, when parsed through certain Autodesk products, can force a Memory corruption vulnerability. A malicious actor can leverage this vul execute arbitrary code in the context of the current process.
CVE-2025-9460	A maliciously crafted SLDPRT file, when parsed through certain Autodesk products, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage t vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
CVE-2025-36928	In GetHostAddress of gxp_buffer.h, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-13155	An improper permissions vulnerability was reported in Lenovo Baiying Client that could allow a local authenticated user to execute code with elevated privileges.
CVE-2025-10884	AA maliciously crafted CATPART file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may levera vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.
CVE-2025-36919	In aocc_read of aoc_channel_dev.c, there is a possible double free due to improper locking. This could lead to local escalation of privilege with no additional execut needed. User interaction is not needed for exploitation.
CVE-2025-13152	A potential DLL hijacking vulnerability was reported in Lenovo One Client during an internal security assessment that could allow a local authenticated user to exec elevated privileges.
CVE-2025-12046	A DLL hijacking vulnerability was reported in the Lenovo App Store and Lenovo Browser applications that could allow a local authenticated user to execute code wi privileges under certain conditions.
CVE-2025-36918	In aoc_service_read_message of aoc_ipc_core.c, there is a possible out of bounds read due to improper input validation. This could lead to local escalation of privile System execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-36930	In GetHostAddress of gxp_buffer.h, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no ad execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-14252	An Improper Access Control vulnerability in Advantech SUSI driver (susi.sys) allows attackers to read/write arbitrary memory, I/O ports, and MSRs, resulting in privi escalation, arbitrary code execution, and information disclosure. This issue affects Advantech SUSI: 5.0.24335 and prior.
CVE-2025-56124	OS Command Injection vulnerability in Ruijie X60 PRO X60_10212014RG-X60 PRO V1.00/V2.00 allowing attackers to execute arbitrary commands via a crafted POS the module_get in file /usr/local/lua/dev_sta/networkConnect.lua.
CVE-2025-36931	In GetHostAddress of gxp_buffer.h, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no ad execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-36936	In GetTachyonCommand of tachyon_server_common.h, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of priv additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-36935	In trusty_ffa_mem_reclaim of shared-mem-smcall.c, there is a possible memory corruption due to uninitialized data. This could lead to local escalation of privilege v additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-9456	A maliciously crafted SLDPRT file, when parsed through certain Autodesk products, can force a Memory corruption vulnerability. A malicious actor can leverage this to execute arbitrary code in the context of the current process.
CVE-2025-9459	A maliciously crafted SLDPRT file, when parsed through certain Autodesk products, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage t vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
CVE-2025-9454	A maliciously crafted PRT file, when parsed through certain Autodesk products, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage this v cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
CVE-2025-14593	A maliciously crafted CATPART file, when parsed through certain Autodesk products, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
CVE-2025-10886	A maliciously crafted MODEL file, when parsed through certain Autodesk products, can force a Memory corruption vulnerability. A malicious actor can leverage this to execute arbitrary code in the context of the current process.
CVE-2025-10887	A maliciously crafted MODEL file, when parsed through certain Autodesk products, can force a Memory corruption vulnerability. A malicious actor can leverage this to execute arbitrary code in the context of the current process.
CVE-2025-10888	AA maliciously crafted MODEL file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.

CVE-2025-10889	A maliciously crafted CATPART file, when parsed through certain Autodesk products, can force a Memory corruption vulnerability. A malicious actor can leverage th vulnerability to execute arbitrary code in the context of the current process.
CVE-2025-10898	AA maliciously crafted MODEL file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.
CVE-2025-10899	AA maliciously crafted MODEL file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.
CVE-2025-10900	AA maliciously crafted MODEL file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.
CVE-2025-9453	A maliciously crafted PRT file, when parsed through certain Autodesk products, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage this v cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
CVE-2025-36932	In tracepoint_msg_handler of cpm/google/lib/tracepoint/tracepoint_ipc.c, there is a possible memory overwrite due to improper input validation. This could lead to l escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-9452	A maliciously crafted SLDPRT file, when parsed through certain Autodesk products, can force a Memory corruption vulnerability. A malicious actor can leverage this to execute arbitrary code in the context of the current process.
CVE-2025-8405	GitLab has remediated a security issue in GitLab CE/EE affecting all versions from 17.1 before 18.4.6, 18.5 before 18.5.4, and 18.6 before 18.6.2 that could have al authenticated user to perform unauthorized actions on behalf of other users by injecting malicious HTML into vulnerability code flow displays.
CVE-2025-14022	LINE client for iOS prior to 15.4 allows man-in-the-middle attacks due to improper SSL/TLS certificate validation in an integrated financial SDK. The SDK interfered v application's network processing, causing server certificate verification to be disabled for a significant portion of network traffic, which could allow a network-adjac intercept or modify encrypted communications.
CVE-2025-24857	Improper access control for volatile memory containing boot code in Universal Boot Loader (U-Boot) before 2017.11 and Qualcomm chips IPQ4019, IPQ5018, IPQ53 IPQ8064, IPQ8074, and IPQ9574 could allow an attacker to execute arbitrary code.
CVE-2025-67962	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AIOSEO Plugin Team Broken Link Checker broken-link-check SQL Injection.This issue affects Broken Link Checker: from n/a through <= 1.2.6.
CVE-2025-13003	Authorization Bypass Through User-Controlled Key vulnerability in Aksis Computer Services and Consulting Inc. AxOnboard allows Exploitation of Trusted Identifiers affects AxOnboard: from 3.2.0 before 3.3.0.
CVE-2025-13214	IBM Aspera Orchestrator 4.0.0 through 4.1.0 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the a view, add, modify, or delete information in the back-end database.
CVE-2025-13124	Authorization Bypass Through User-Controlled Key vulnerability in Netiket Information Technologies Ltd. Co. ApplyLogic allows Exploitation of Trusted Identifiers.Th affects ApplyLogic: through 01.12.2025.
CVE-2025-65831	The application uses an insecure hashing algorithm (MD5) to hash passwords. If an attacker obtained a copy of these hashes, either through exploiting cloud servic performing TLS downgrade attacks on the traffic from a mobile device, or through another means, they may be able to crack the hash in a reasonable amount of ti unauthorized access to the victim's account.
CVE-2025-13077	The افزونه پیامک ووکامرس فوق حرفه ای (جدید) payamito sms woocommerce plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'columns' param versions up to, and including, 1.3.5. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the da
CVE-2025-43542	This issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.7.3. Password fields may be unintentionally revealed when re controlling a device over FaceTime.
CVE-2025-65821	As UART download mode is still enabled on the ESP32 chip on which the firmware runs, an adversary can dump the flash from the device and retrieve sensitive info as details about the current and previous Wi-Fi network from the NVS partition. Additionally, this allows the adversary to reflash the device with their own firmware contain malicious modifications.
CVE-2025-14542	The vulnerability arises when a client fetches a tools' JSON specification, known as a Manual, from a remote Manual Endpoint. While a provider may initially serve a manual (e.g., one defining an HTTP tool call), earning the clients' trust, a malicious provider can later change the manual to exploit the client.
CVE-2025-43494	A mail header parsing issue was addressed with improved checks. This issue is fixed in watchOS 26.1, iOS 18.7.2 and iPadOS 18.7.2, macOS Tahoe 26.1, visionOS 2 Sonoma 14.8.2, macOS Sequoia 15.7.2, iOS 26.1 and iPadOS 26.1. An attacker may be able to cause a persistent denial-of-service.
CVE-2025-13089	The WP Directory Kit plugin for WordPress is vulnerable to SQL Injection via the 'hide_fields' and the 'attr_search' parameter in all versions up to, and including, 1.4 insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attack additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2025-65512	A Server-Side Request Forgery (SSRF) vulnerability was discovered in the webpage-to-markdown conversion feature of markdownify-mcp v0.0.2 and before. This v allows an attacker to bypass private IP restrictions through hostname-based bypass and HTTP redirect chains, enabling access to internal network services.
CVE-	The WPNakama plugin for WordPress is vulnerable to time-based SQL Injection via the 'order_by' parameter in all versions up to, and including, 0.6.3 due to insuffi

2025-14068	on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additio queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2025-66628	ImageMagick is a software suite to create, edit, compose, or convert bitmap images. In versions 7.1.2-9 and prior, the TIM (PSX TIM) image parser contains a critica overflow vulnerability in its ReadTIMImage function (coders/tim.c). The code reads width and height (16-bit values) from the file header and calculates image_size height without checking for overflow. On 32-bit systems (or where size_t is 32-bit), this calculation can overflow if width and height are large (e.g., 65535), wrappin small value. This results in a small heap allocation via AcquireQuantumMemory and later operations relying on the dimensions can trigger an out of bounds read. T fixed in version 7.1.2-10.
CVE-2025-67779	It was found that the fix addressing CVE-2025-55184 in React Server Components was incomplete and does not prevent a denial of service attack in a specific case Server Components versions 19.0.2, 19.1.3 and 19.2.2 are affected, allowing unsafe deserialization of payloads from HTTP requests to Server Function endpoints. T an infinite loop that hangs the server process and may prevent future HTTP requests from being served.
CVE-2025-13886	The LT Unleashed plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.1.1 via the 'template' parameter in the `book` sho insufficient path sanitization. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on t allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where f wp-config.php can be included.
CVE-2025-63895	An issue in the Bluetooth firmware of JXL 9 Inch Car Android Double Din Player Android v12.0 allows attackers to cause a Denial of Service (DoS) via sending a craf Manager Protocol (LMP) packet.
CVE-2025-68155	@vitejs/plugin-rs provides React Server Components (RSC) support for Vite. Prior to version 0.5.8, the `/__vite_rsc_findSourceMapURL` endpoint in `@vitejs/plugin-r unauthenticated arbitrary file read during development mode. An attacker can read any file accessible to the Node.js process by sending a crafted HTTP request w URL in the `filename` query parameter. Version 0.5.8 fixes the issue.
CVE-2025-68156	Expr is an expression language and expression evaluation for Go. Prior to version 1.17.7, several builtin functions in Expr, including `flatten`, `min`, `max`, `mean `median`, perform recursive traversal over user-provided data structures without enforcing a maximum recursion depth. If the evaluation environment contains de cyclic data structures, these functions may recurse indefinitely until exceed the Go runtime stack limit. This results in a stack overflow panic, causing the host appl crash. While exploitability depends on whether an attacker can influence or inject cyclic or pathologically deep data into the evaluation environment, this behavior denial-of-service (DoS) risk and affects overall library robustness. Instead of returning a recoverable evaluation error, the process may terminate unexpectedly. In versions, evaluation of expressions that invoke certain builtin functions on untrusted or insufficiently validated data structures can lead to a process-level crash du exhaustion. This issue is most relevant in scenarios where Expr is used to evaluate expressions against externally supplied or dynamically constructed environmen references (directly or indirectly) can be introduced into arrays, maps, or structs; and there are no application-level safeguards preventing deeply nested input dat use cases with controlled, acyclic data, the issue may not manifest. However, when present, the resulting panic can be used to reliably crash the application, const denial of service. The issue has been fixed in the v1.17.7 versions of Expr. The patch introduces a maximum recursion depth limit for affected builtin functions. Wh exceeded, evaluation aborts gracefully and returns a descriptive error instead of panicking. Additionally, the maximum depth can be customized by users via `builtin.MaxDepth`, allowing applications with legitimate deep structures to raise the limit in a controlled manner. Users are strongly encouraged to upgrade to the release, which includes both the recursion guard and comprehensive test coverage to prevent regressions. For users who cannot immediately upgrade, some mitig recommended. Ensure that evaluation environments cannot contain cyclic references, validate or sanitize externally supplied data structures before passing them and/or wrap expression evaluation with panic recovery to prevent a full process crash (as a last-resort defensive measure). These workarounds reduce risk but do eliminate the issue without the patch.
CVE-2023-53896	D-Link DAP-1325 firmware version 1.01 contains a broken access control vulnerability that allows unauthenticated attackers to download device configuration setti authentication. Attackers can exploit the /cgi-bin/ExportSettings.sh endpoint to retrieve sensitive configuration information by directly accessing the export setting
CVE-2025-59802	Foxit PDF Editor and Reader before 2025.2.1 allow signature spoofing via OCG. When Optional Content Groups (OCG) are supported, the state property of an OCG i only and not included in the digital signature computation buffer. An attacker can leverage JavaScript or PDF triggers to dynamically change the visibility of OCG co signing (Post-Sign), allowing the visual content of a signed PDF to be modified without invalidating the signature. This may result in a mismatch between the signe what the signer or verifier sees, undermining the trustworthiness of the digital signature. The fixed versions are 2025.2.1, 14.0.1, and 13.2.1.
CVE-2025-67725	Tornado is a Python web framework and asynchronous networking library. In versions 6.5.2 and below, a single maliciously crafted HTTP request can block the serv loop for an extended period, caused by the HTTPHeaders.add method. The function accumulates values using string concatenation when the same header name is causing a Denial of Service (DoS). Due to Python string immutability, each concatenation copies the entire string, resulting in O(n²) time complexity. The severity c high if max_header_size has been increased from its default, to low if it has its default value of 64KB. This issue is fixed in version 6.5.3.
CVE-2025-55184	A pre-authentication denial of service vulnerability exists in React Server Components versions 19.0.0, 19.0.1 19.1.0, 19.1.1, 19.1.2, 19.2.0 and 19.2.1, including th packages: react-server-dom-parcel, react-server-dom-turbopack, and react-server-dom-webpack. The vulnerable code unsafely deserializes payloads from HTTP re Server Function endpoints, which can cause an infinite loop that hangs the server process and may prevent future HTTP requests from being served.
CVE-2024-58304	SPA-CART CMS 1.9.0.3 contains a stored cross-site scripting vulnerability in the product description parameter that allows authenticated administrators to inject ma scripts. Attackers can submit JavaScript payloads through the 'descr' parameter in the product edit form to execute arbitrary code in administrative users' browser
CVE-2025-67726	Tornado is a Python web framework and asynchronous networking library. Versions 6.5.2 and below use an inefficient algorithm when parsing parameters for HTTP values, potentially causing a DoS. The _parseparam function in httputil.py is used to parse specific HTTP header values, such as those in multipart/form-data and re string.count() within a nested loop while processing quoted semicolons. If an attacker sends a request with a large number of maliciously crafted parameters in a C Disposition header, the server's CPU usage increases quadratically (O(n²)) during parsing. Due to Tornado's single event loop architecture, a single malicious reque the entire server to become unresponsive for an extended period. This issue is fixed in version 6.5.3.
CVE-2025-54981	Weak Encryption Algorithm in StreamPark, The use of an AES cipher in ECB mode and a weak random number generator for encrypting sensitive data, including JW have risked exposing sensitive authentication data This issue affects Apache StreamPark: from 2.0.0 before 2.1.7. Users are recommended to upgrade to version 2 fixes the issue.
CVE-2025-12562	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 11.10 before 18.4.6, 18.5 before 18.5.4, and 18.6 before 18.6.2 that could have allowed unauthenticated user to create a denial of service condition by sending crafted GraphQL queries that bypass query complexity limits.
CVE-2025-13339	The Hippoo Mobile App for WooCommerce plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.7.1 via the template_redirect() makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.
CVE-2024-58316	Online Shopping System Advanced 1.0 contains a SQL injection vulnerability in the payment_success.php script that allows attackers to inject malicious SQL throug unfiltered 'cm' parameter. Attackers can exploit the vulnerability by sending crafted SQL queries to retrieve sensitive database information by manipulating the us parameter.

CVE-2025-67635	Jenkins 2.540 and earlier, LTS 2.528.2 and earlier does not properly close HTTP-based CLI connections when the connection stream becomes corrupted, allowing unauthenticated attackers to cause a denial of service.
CVE-2025-14169	The FunnelKit - Funnel Builder for WooCommerce Checkout plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'opid' parameter in all versi including, 3.13.1.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2025-65297	Aqara Hub devices including Camera Hub G3 4.1.9_0027, Hub M2 4.3.6_0027, and Hub M3 4.3.6_0025 automatically collect and upload unencrypted sensitive infor that this occurs without disclosure or consent from the manufacturer.
CVE-2025-68067	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Stockholm Core stockholm PHP Local File Inclusion.This issue affects Stockholm Core: from n/a through <= 2.4.6.
CVE-2025-13126	The wpForo Forum plugin for WordPress is vulnerable to generic SQL Injection via the `post_args` and `topic_args` parameters in all versions up to, and including, insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attack additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2025-14712	Student Learning Assessment and Support System developed by JHENG GAO has a Exposure of Sensitive Information vulnerability, allowing unauthenticated remot view a specific page and obtain test accounts and password.
CVE-2025-65176	An issue was discovered in Dynatrace OneAgent before 1.325.47. When attempting to access a remote network share from a machine where OneAgent is installed a "STATUS_LOGON_FAILURE" error, the agent will retrieve every user token on the machine and repeatedly attempt to access the network share while impersonati exploitation of this vulnerability can allow an unprivileged attacker with access to the affected system to perform NTLM relay attacks.
CVE-2025-13474	Authorization Bypass Through User-Controlled Key vulnerability in Menulux Software Inc. Mobile App allows Exploitation of Trusted Identifiers.This issue affects Mob before 9.5.8.
CVE-2025-68068	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Stockholm stockholm allov File Inclusion.This issue affects Stockholm: from n/a through <= 9.14.1.
CVE-2025-14383	The Booking Calendar plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'dates_to_check' parameter in all versions up to, and including, 1 insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attack additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2025-68062	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove MinimogWP minimog allows F Inclusion.This issue affects MinimogWP: from n/a through <= 3.9.6.
CVE-2025-68066	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in PenciDesign Soledad soledad allows PHP I Inclusion.This issue affects Soledad: from n/a through <= 8.7.0.
CVE-2025-68065	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in LiquidThemes Hub Core hub-core allows P Inclusion.This issue affects Hub Core: from n/a through <= 5.0.8.
CVE-2025-68061	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove EduMall edumall allows PHP I Inclusion.This issue affects EduMall: from n/a through <= 4.4.7.
CVE-2025-53619	An out-of-bounds read vulnerability exists in the JPEGBITSCodec::InternalCode functionality of Grassroot DICOM 3.024. A specially crafted DICOM file can lead to an leak. An attacker can provide a malicious file to trigger this vulnerability.The function `null_convert` is called based of the value of the malicious DICOM file specify intended interpretation of the image pixel data
CVE-2025-48429	An out-of-bounds read vulnerability exists in the RLECodec::DecodeByStreams functionality of Grassroot DICOM 3.024. A specially crafted DICOM file can lead to le data. An attacker can provide a malicious file to trigger this vulnerability.
CVE-2025-52582	An out-of-bounds read vulnerability exists in the Overlay::GrabOverlayFromPixelData functionality of Grassroot DICOM 3.024. A specially crafted DICOM file can lea information leak. An attacker can provide a malicious file to trigger this vulnerability.
CVE-2025-65290	Aqara Hub devices including Camera Hub G3 4.1.9_0027, Hub M2 4.3.6_0027, and Hub M3 4.3.6_0025 fail to validate server certificates during HTTPS firmware dov allowing man-in-the-middle attackers to intercept firmware update traffic and potentially serve modified firmware files.
CVE-2025-53618	An out-of-bounds read vulnerability exists in the JPEGBITSCodec::InternalCode functionality of Grassroot DICOM 3.024. A specially crafted DICOM file can lead to an leak. An attacker can provide a malicious file to trigger this vulnerability.The function `grayscale_convert` is called based of the value of the malicious DICOM file s intended interpretation of the image pixel data
CVE-2025-65292	Command injection vulnerability in Aqara Hub devices including Camera Hub G3 4.1.9_0027, Hub M2 4.3.6_0027, and Hub M3 4.3.6_0025 allows attackers to execu commands with root privileges through malicious domain names.
CVE-2025-14644	A vulnerability was determined in itsourcecode Student Management System 1.0. The impacted element is an unknown function of the file /update_subject.php. Ex manipulation of the argument ID can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.
CVE-2025-14514	A flaw has been found in Campcodes Supplier Management System 1.0. Affected is an unknown function of the file /admin/add_distributor.php. This manipulation o argument txtDistributorAddress causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.

CVE-2025-14649	A vulnerability was detected in itsourcecode Online Cake Ordering System 1.0. Affected by this issue is some unknown functionality of the file /cakeshop/supplier.p Performing manipulation of the argument supplier results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.
CVE-2025-14704	A vulnerability was found in Shiguangwu sgwbox N3 2.0.25. The impacted element is an unknown function of the file /eshell of the component API. The manipulatio path traversal. It is possible to launch the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclos not respond in any way.
CVE-2025-14645	A vulnerability was identified in code-projects Student File Management System 1.0. This affects an unknown function of the file /admin/delete_user.php. The manip argument user_id leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.
CVE-2025-14646	A security flaw has been discovered in code-projects Student File Management System 1.0. This impacts an unknown function of the file /admin/delete_student.php manipulation of the argument stud_id results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be e
CVE-2025-14647	A weakness has been identified in code-projects Computer Book Store 1.0. Affected is an unknown function of the file /admin_delete.php. This manipulation of the a bookisbn causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.
CVE-2025-14673	A vulnerability has been found in gmg137 snap7-rs up to 1.142.1. Affected is the function snap7_rs::client::S7Client::as_ct_write of the file /tests/snap7-rs/src/client manipulation leads to heap-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-14666	A weakness has been identified in itsourcecode COVID Tracking System 1.0. The affected element is an unknown function of the file /admin/?page=user. This mani the argument Username causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exp
CVE-2025-14650	A flaw has been found in itsourcecode Online Cake Ordering System 1.0. This affects an unknown part of the file /cakeshop/product.php. Executing manipulation of Product can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used.
CVE-2025-14570	A flaw has been found in projectworlds Advanced Library Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /view_admin manipulation of the argument admin_id causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.
CVE-2025-14672	A flaw has been found in gmg137 snap7-rs up to 1.142.1. This impacts the function TSnap7MicroClient::opWriteArea of the file s7_micro_client.cpp. Executing mani lead to heap-based buffer overflow. It is possible to launch the attack remotely. The exploit has been published and may be used.
CVE-2025-14653	A vulnerability was determined in itsourcecode Student Management System 1.0. Impacted is an unknown function of the file /addrecord.php. This manipulation of ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.
CVE-2025-14578	A weakness has been identified in itsourcecode Student Management System 1.0. The affected element is an unknown function of the file /update_account.php. Th manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be e
CVE-2025-14643	A vulnerability was found in code-projects Simple Attendance Record System 2.0. The affected element is an unknown function of the file /check.php. Performing m the argument student results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.
CVE-2025-67644	LangGraph SQLite Checkpoint is an implementation of LangGraph CheckpointSaver that uses SQLite DB (both sync and async, via aiosqlite). Versions 3.0.0 and bel vulnerable to SQL injection through the checkpoint implementation. Checkpoint allows attackers to manipulate SQL queries through metadata filter keys, affecting that accept untrusted metadata filter keys (not just filter values) in checkpoint search operations. The _metadata_predicate() function constructs SQL queries by in filter keys directly into f-strings without validation. This issue is fixed in version 3.0.1.
CVE-2025-14668	A vulnerability was detected in campcodes Advanced Online Examination System 1.0. This affects an unknown function of the file /query/loginExe.php. Performing of the argument Username results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.
CVE-2025-14667	A security vulnerability has been detected in itsourcecode COVID Tracking System 1.0. The impacted element is an unknown function of the file /admin/?page=sys Such manipulation of the argument meta_value leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may
CVE-2025-14565	A vulnerability was identified in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. The affected element is an unknown functio /Profilers/SProfile/login1.php. Such manipulation of the argument Username leads to sql injection. The attack may be performed from remote. The exploit is publicly and might be used.
CVE-2025-14661	A vulnerability has been found in itsourcecode Student Managemen System 1.0. Affected by this issue is some unknown functionality of the file /advisers.php. Such of the argument sy leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-12835	The WooMulti WordPress plugin through 17 does not validate a file parameter when deleting files, which could allow any authenticated users, such as subscriber to arbitrary files on the server.
CVE-2025-14571	A vulnerability has been found in projectworlds Advanced Library Management System 1.0. Affected by this issue is some unknown functionality of the file /borrow_ Such manipulation of the argument roll_number leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may
CVE-2025-14652	A vulnerability was found in itsourcecode Online Cake Ordering System 1.0. This issue affects some unknown processing of the file /admindetail.php?action=edit. T manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.
CVE-2025-14584	A vulnerability has been found in itsourcecode COVID Tracking System 1.0. Affected is an unknown function of the file /admin/login.php of the component Admin Lo manipulation of the argument Username leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used

CVE-2025-14640	A flaw has been found in code-projects Student File Management System 1.0. The affected element is an unknown function of the file /admin/save_student.php. Ex manipulation of the argument stud_no can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.
CVE-2025-14515	A vulnerability has been found in Campcodes Supplier Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/add_un manipulation of the argument txtunitDetails leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be u
CVE-2025-14536	A security flaw has been discovered in code-projects Class and Exam Timetable Management 1.0. Affected by this vulnerability is an unknown functionality of the fi of the component Login. The manipulation of the argument username/password results in sql injection. The attack may be launched remotely. The exploit has beer the public and may be exploited.
CVE-2025-14620	A vulnerability was determined in code-projects Student File Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/login_ Executing manipulation of the argument Username can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and ma
CVE-2025-14619	A vulnerability was found in code-projects Student File Management System 1.0. Affected by this vulnerability is an unknown functionality of the file login_query.ph manipulation of the argument stud_no results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.
CVE-2025-14590	A security vulnerability has been detected in code-projects Prison Management System 2.0. Impacted is an unknown function of the file /admin/search1.php. The m the argument keyname leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.
CVE-2025-14588	A security flaw has been discovered in itsourcecode Student Management System 1.0. This vulnerability affects unknown code of the file /update_program.php. Per manipulation of the argument ID results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be e
CVE-2025-14587	A vulnerability was identified in itsourcecode Online Pet Shop Management System 1.0. This affects an unknown part of the file /pet1/available.php. Such manipula argument Name leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.
CVE-2025-14537	A weakness has been identified in code-projects Class and Exam Timetable Management 1.0. Affected by this issue is some unknown functionality of the file /previ manipulation of the argument course_year_section/semester causes sql injection. Remote exploitation of the attack is possible. The exploit has been made availabl public and could be exploited.
CVE-2025-33212	NVIDIA NeMo Framework contains a vulnerability in model loading that could allow an attacker to exploit improper control mechanisms if a user loads a maliciously successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, and data tampering.
CVE-2025-14529	A flaw has been found in Campcodes Retro Basketball Shoes Online Store 1.0. The affected element is an unknown function of the file /admin/admin_running.php. T manipulation of the argument pid causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.
CVE-2025-14621	A vulnerability was identified in code-projects Student File Management System 1.0. This affects an unknown part of the file /admin/update_user.php. The manipula argument user_id leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.
CVE-2025-14527	A weakness has been identified in projectworlds Advanced Library Management System 1.0. This vulnerability affects unknown code of the file /view_book.php. Exe manipulation of the argument book_id can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could
CVE-2025-14622	A security flaw has been discovered in code-projects Student File Management System 1.0. This vulnerability affects unknown code of the file /admin/save_user.ph manipulation of the argument firstname results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be explo
CVE-2025-14623	A weakness has been identified in code-projects Student File Management System 1.0. This issue affects some unknown processing of the file /admin/update_stude manipulation of the argument stud_id causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and exploited.
CVE-2025-55310	An issue was discovered in Foxit PDF and Editor for Windows and macOS before 13.2 and 2025 before 2025.2. An attacker able to alter or replace the static HTML f the StartPage feature can cause the application to load malicious or compromised content upon startup. This may result in information disclosure, unauthorized da other security impacts.
CVE-2025-14637	A weakness has been identified in itsourcecode Online Pet Shop Management System 1.0. This vulnerability affects unknown code of the file /pet1/addcnp.php. Thi manipulation of the argument cnpname causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be e
CVE-2025-14711	A flaw has been found in FantasticLBP Hotels Server up to 67b44df162fab26df209bd5d5d542875fcbec1d0. This vulnerability affects unknown code of the file /controller/api/hotelList.php. This manipulation of the argument pickedHotelName/type causes sql injection. The attack is possible to be carried out remotely. The e been published and may be used. This product adopts a rolling release strategy to maintain continuous delivery The vendor was contacted early about this disclosu respond in any way.
CVE-2025-14710	A vulnerability was detected in FantasticLBP Hotels Server up to 67b44df162fab26df209bd5d5d542875fcbec1d0. This affects an unknown part of the file /controller/api/OrderList.php. The manipulation of the argument telephone results in sql injection. The attack can be executed remotely. The exploit is now public a used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The vendor early about this disclosure but did not respond in any way.
CVE-2025-14638	A security vulnerability has been detected in itsourcecode Online Pet Shop Management System 1.0. This issue affects some unknown processing of the file /pet1/update_cnp.php. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly a used.
CVE-2025-14639	A vulnerability was detected in itsourcecode Student Management System 1.0. Impacted is an unknown function of the file /uprec.php. Performing manipulation of ID results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used.
CVE-2025-	A vulnerability was found in itsourcecode COVID Tracking System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/?page=zone. The

14585	of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.
CVE-2025-14566	A security flaw has been discovered in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. The impacted element is an unknown the file /Profilers/SProfile/reg.php. Performing manipulation of the argument USN results in sql injection. It is possible to initiate the attack remotely. The exploit has released to the public and may be exploited.
CVE-2025-14583	A flaw has been found in campcodes Online Student Enrollment System 1.0. This impacts an unknown function of the file /admin/register.php. Executing manipulat argument photo can lead to unrestricted upload. The attack can be launched remotely. The exploit has been published and may be used.
CVE-2025-14664	A vulnerability was identified in Campcodes Supplier Management System 1.0. This issue affects some unknown processing of the file /admin/view_unit.php. The m the argument chkId[] leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.
CVE-2025-12570	The Fancy Product Designer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 6.4.8 due to i input sanitization and output escaping in the data-to-image.php and pdf-to-image.php files. This makes it possible for unauthenticated attackers to inject arbitrary pages that will execute whenever a user accesses the SVG file.
CVE-2025-14503	An overly-permissive IAM trust policy in the Harmonix on AWS framework may allow IAM principals in the same AWS account to escalate privileges via role assump sample code for the EKS environment provisioning role is configured to trust the account root principal, which may enable any IAM principal in the same AWS acco sts:AssumeRole permissions to assume the role with administrative privileges. We recommend customers upgrade to Harmonix on AWS v0.4.2 or later if you have framework using versions v0.3.0 through v0.4.1.
CVE-2025-67751	ChurchCRM is an open-source church management system. Prior to version 6.5.0, a SQL injection vulnerability exists in the `EventEditor.php` file. When creating a and selecting an event type, the `EN_tyid` POST parameter is not sanitized. This allows an authenticated user with event management permissions (`isAddEvent`) arbitrary SQL queries. Version 6.5.0 fixes the issue.
CVE-2025-64986	A command injection vulnerability was discovered in TeamViewer DEX (former 1E DEX), specifically within the 1E-Explorer-TachyonCore-DevicesListeningOnAPort i prior V21. Improper input validation, allowing authenticated attackers with Actioner privileges to inject arbitrary commands. Exploitation enables remote execution commands on devices connected to the platform.
CVE-2025-64987	A command injection vulnerability was discovered in TeamViewer DEX (former 1E DEX), specifically within the 1E-Explorer-TachyonCore-CheckSimpleIoC instructio input validation, allowing authenticated attackers with Actioner privileges to inject arbitrary commands. Exploitation enables remote execution of elevated comma devices connected to the platform.
CVE-2025-64988	A command injection vulnerability was discovered in TeamViewer DEX (former 1E DEX), specifically within the 1E-Nomad-GetCmContentLocations instruction prior Improper input validation, allowing authenticated attackers with Actioner privileges to inject arbitrary commands. Exploitation enables remote execution of elevate on devices connected to the platform.
CVE-2025-64989	A command injection vulnerability was discovered in TeamViewer DEX (former 1E DEX), specifically within the 1E-Explorer-TachyonCore-FindFileBySizeAndHash ins V21.1. Improper input validation, allowing authenticated attackers with Actioner privileges to inject arbitrary commands. Exploitation enables remote execution of commands on devices connected to the platform.
CVE-2025-67818	An issue was discovered in Weaviate OSS before 1.33.4. An attacker with access to insert data into the database can craft an entry name with an absolute path (e. use parent directory traversal (../../..) to escape the restore root when a backup is restored, potentially creating or overwriting files in arbitrary locations within the privilege scope.
CVE-2025-1161	Incorrect Use of Privileged APIs vulnerability in NomySoft Information Technology Training and Consulting Inc. Nomysem allows Privilege Escalation.This issue affec through May 2025.
CVE-2025-12684	The URL Shortify WordPress plugin before 1.11.3 does not sanitize and escape a parameter before outputting it back in the page, leading to a reflected cross site s could be used against high-privilege users such as admins.
CVE-2025-13072	The HandL UTM Grabber / Tracker WordPress plugin before 2.8.1 does not sanitize and escape a parameter before outputting it back in the page, leading to a Refle Site Scripting which could be used against high privilege users such as admin.
CVE-2025-67648	Shopware is an open commerce platform. Versions 6.4.6.0 through 6.6.10.9 and 6.7.0.0 through 6.7.5.0 have a Reflected XSS vulnerability in AuthController.php. A parameter from the login page URL is directly rendered within the Twig template of the Storefront login page without further processing or input validation. This all code injection into the template via the URL parameter, waitTime, which lacks proper input validation. This issue is fixed in versions 6.6.10.10 and 6.7.5.1.
CVE-2025-43520	A memory corruption issue was addressed with improved memory handling. This issue is fixed in watchOS 26.1, iOS 18.7.2 and iPadOS 18.7.2, macOS Tahoe 26.1, 26.1, tvOS 26.1, macOS Sonoma 14.8.2, macOS Sequoia 15.7.2, iOS 26.1 and iPadOS 26.1. A malicious application may be able to cause unexpected system termi kernel memory.
CVE-2025-13073	The HandL UTM Grabber / Tracker WordPress plugin before 2.8.1 does not sanitize and escape a parameter before outputting it back in the page, leading to a Refle Site Scripting which could be used against high privilege users such as admin
CVE-2025-13355	The URL Shortify WordPress plugin before 1.11.4 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site which could be used against high privilege users such as admin.
CVE-2025-14038	EDB Hybrid Manager contains a flaw that allows an unauthenticated attacker to directly access certain gRPC endpoints. This could allow an attacker to read potent data or possibly cause a denial-of-service by writing malformed data to certain gRPC endpoints. This flaw has been remediated in EDB Hybrid Manager 1.3.3, and c should consider upgrading to 1.3.3 as soon as possible. The flaw is due to a misconfiguration in the Istio Gateway, which manages authentication and authorizatio affected endpoints. The security policy relies on an explicit definition of required permissions in the Istio Gateway configuration, and the affected endpoints were n the configuration. This allowed requests to bypass both authentication and authorization within a Hybrid Manager service. All versions of Hybrid Manager - LTS sho upgraded to 1.3.3, and all versions of Hybrid Manager - Innovation should be upgraded to 2025.12.
CVE-2025-36916	In PrepareWorkloadBuffers of gxp_main_actor.cc, there is a possible double fetch due to a race condition. This could lead to local escalation of privilege with no add execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-	A command injection vulnerability was discovered in TeamViewer DEX (former 1E DEX), specifically within the 1E-ConfigMgrConsoleExtensions instructions. Improp validation, allowing authenticated attackers with Actioner privileges to inject arbitrary commands. Exploitation enables remote execution of elevated commands or

64993	connected to the platform.
CVE-2025-13320	The WP User Manager plugin for WordPress is vulnerable to Arbitrary File Deletion in all versions up to, and including, 2.9.12. This is due to insufficient validation of file paths in the profile update functionality combined with improper handling of array inputs by PHP's filter_input() function. This makes it possible for authenticate with Subscriber-level access and above, to delete arbitrary files on the server via the 'current_user_avatar' parameter in a two-stage attack which can make remote execution possible. This only affects sites with the custom avatar setting enabled.
CVE-2025-37731	Improper Authentication in Elasticsearch PKI realm can lead to user impersonation via specially crafted client certificates. A malicious actor would need to have suc client certificate signed by a legitimate, trusted Certificate Authority.
CVE-2025-64990	A command injection vulnerability was discovered in TeamViewer DEX (former 1E DEX), specifically within the 1E-Explorer-TachyonCore-LogoffUser instruction prio Improper input validation, allowing authenticated attackers with Actioner privileges to inject arbitrary commands. Exploitation enables remote execution of elevate on devices connected to the platform.
CVE-2025-64991	A command injection vulnerability was discovered in TeamViewer DEX (former 1E DEX), specifically within the 1E-PatchInsights-Deploy instruction prior V15. Impro validation, allowing authenticated attackers with Actioner privileges to inject arbitrary commands. Exploitation enables remote execution of elevated commands or connected to the platform.
CVE-2025-64992	A command injection vulnerability was discovered in TeamViewer DEX (former 1E DEX), specifically within the 1E-Nomad-PauseNomadJobQueue instruction prior V input validation, allowing authenticated attackers with Actioner privileges to inject arbitrary commands. Exploitation enables remote execution of elevated comma devices connected to the platform.
CVE-2025-65822	The ESP32 system on a chip (SoC) that powers the Meatmeet Pro was found to have JTAG enabled. By leaving JTAG enabled on an ESP32 in a commercial product a with physical access to the device can connect over this port and reflash the device's firmware with malicious code which will be executed upon running. As a resu will lose access to the functionality of their device and the attack may gain unauthorized access to the victim's Wi-Fi network by re-connecting to the SSID defined partition of the device.
CVE-2025-11984	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 13.1 before 18.4.6, 18.5 before 18.5.4, and 18.6 before 18.6.2 that could have allowed a authenticated user to bypass WebAuthn two-factor authentication by manipulating the session state under certain conditions.
CVE-2025-61821	ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and data on the server. Exploitation of this issue does not require use and scope is changed.
CVE-2025-65829	The ESP32 system on a chip (SoC) that powers the Meatmeet basestation device was found to lack Secure Boot. The Secure Boot feature ensures that only authent software can execute on the device. The Secure Boot process forms a chain of trust by verifying all mutable software entities involved in the Application Startup Flo result, an attacker with physical access to the device can flash modified firmware to the device, resulting in the execution of malicious code upon startup.
CVE-2025-13664	A potential security vulnerability in Quartus® Prime Standard Edition Design Software may allow escalation of privilege.
CVE-2025-13663	Under certain circumstances, the Quartus Prime Pro Installer for Windows does not check the permissions of the Quartus target installation directory if the target ir directory already exists.
CVE-2025-55308	An issue was discovered in Foxit PDF and Editor for Windows before 13.2 and 2025 before 2025.2. A crafted PDF containing JavaScript that calls closeDoc() while in are still in use can cause premature release of these objects. This use-after-free vulnerability may lead to memory corruption, potentially resulting in information di when the PDF is opened.
CVE-2025-55309	An issue was discovered in Foxit PDF and Editor for Windows and macOS before 13.2 and 2025 before 2025.2. A crafted PDF can contain JavaScript that attaches a action on a form field that destroys an annotation. During user right-click interaction, the program's internal focus change handling prematurely releases the annot resulting in a use-after-free vulnerability that may cause memory corruption or application crashes.
CVE-2025-13668	A potential security vulnerability in Quartus® Prime Pro Edition Design Software may allow escalation of privilege.
CVE-2025-36934	In bigo_worker_thread of private/google-modules/video/gchips/bigo.c, there is a possible use after free due to a race condition. This could lead to local escalation of with no additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-36922	In bigo_map of bigo_iommu.c, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege in the OS Kernel level execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-13665	The System Console Utility for Windows is vulnerable to a DLL planting vulnerability
CVE-2025-13669	Uncontrolled Search Path Element vulnerability in Altera High Level Synthesis Compiler on Windows allows Search Order Hijacking.This issue affects High Level Syn Compiler: from 19.1 through 24.3.
CVE-2025-13670	The High Level Synthesis Compiler i++ command for Windows is vulnerable to a DLL planting vulnerability
CVE-2025-65293	Command injection vulnerabilities in Aqara Camera Hub G3 4.1.9_0027 allow attackers to execute arbitrary commands with root privileges through malicious QR co device setup and factory reset.
CVE-2025-67499	The CNI portmap plugin allows containers to emulate opening a host port, forwarding that traffic to the container. Versions 1.6.0 through 1.8.0 inadvertently forwa with the same destination port as the host port when the portmap plugin is configured with the nftables backend, thus ignoring the destination IP. This includes tra intended for the node itself, i.e. traffic to containers hosted on the node. Containers that request HostPort forwarding can intercept all traffic destined for that port. that the portmap plugin be explicitly configured to use the nftables backend. This issue is fixed in version 1.9.0. To workaround, configure the portmap plugin to us

	backend. It does not have this vulnerability.
CVE-2025-14693	A vulnerability has been found in Ugreen DH2100+ up to 5.3.0. This affects an unknown function of the component USB Handler. Such manipulation leads to symli The attack can be executed directly on the physical device. The exploit has been disclosed to the public and may be used. The vendor was contacted early about t but did not respond in any way.
CVE-2025-11266	An out-of-bounds write vulnerability exists in the Grassroots DICOM library (GDCM). The issue is triggered during parsing of a malformed DICOM file containing enc PixelData fragments (compressed image data stored as multiple fragments). This vulnerability leads to a segmentation fault caused by an out-of-bounds memory a unsigned integer underflow in buffer indexing. It is exploitable via file input, simply opening a crafted malicious DICOM file is sufficient to trigger the crash, resultin of-service condition.
CVE-2025-14148	IBM UCD - IBM DevOps Deploy 8.1 through 8.1.2.3 could allow an authenticated user with LLM integration configuration privileges to recover a previously saved LL
CVE-2025-66388	A vulnerability in Apache Airflow allowed authenticated UI users to view secret values in rendered templates due to secrets not being properly redacted, potentiall secrets to users without the appropriate authorization. Users are recommended to upgrade to version 3.1.4, which fixes this issue.
CVE-2025-55901	TOTOLINK A3300R V17.0.0cu.596_B20250515 is vulnerable to command injection in the function NTPSyncWithHost via the host_time parameter.
CVE-2025-14446	The Popup Builder (Easy Notify Lite) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the easynotify_cp function in all versions up to, and including, 1.1.37. This makes it possible for authenticated attackers, with Subscriber-level access and above, to reset plugin setti default values.
CVE-2025-52493	PagerDuty Runbook through 2025-06-12 exposes stored secrets directly in the webpage DOM at the configuration page. Although these secrets appear masked as fields, the actual secret values are present in the page source and can be revealed by simply modifying the input field type from "password" to "text" using browse tools. This vulnerability is exploitable by administrative users who have access to the configuration page.
CVE-2025-68077	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Select-Themes Stockholm stockholm allows Stored XSS.This iss Stockholm: from n/a through <= 9.14.1.
CVE-2025-68079	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeNectar Salient Shortcodes salient-shortcodes allows Sto issue affects Salient Shortcodes: from n/a through <= 1.5.4.
CVE-2025-68080	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Saad Iqbal User Avatar - Reloaded user-avatar-reloaded allows XSS.This issue affects User Avatar - Reloaded: from n/a through <= 1.2.2.
CVE-2025-13231	The Fancy Product Designer plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 6.4.8. This is due to a time-of-ch use (TOCTOU) race condition in the 'url' parameter of the fpd_custom_uplod_file AJAX action. The plugin validates the URL by calling getimagesize() first, then later same URL using file_get_contents(). This makes it possible for unauthenticated attackers to exploit the timing gap to perform SSRF attacks by serving a valid imag validation, then changing the response to redirect to arbitrary internal or external URLs during the actual fetch.
CVE-2024-2105	An unauthorised attacker within bluetooth range may use an improper validation during the BLE connection request to deadlock the affected devices.
CVE-2025-66451	LibreChat is a ChatGPT clone with additional features. In versions 0.8.0 and below, when creating prompts, JSON requests are sent to define and modify the prompt endpoint for prompt groups (/api/prompts/groups/:groupId). However, the request bodies are not sufficiently validated for proper input, enabling users to modify pr way that was not intended as part of the front end system. The patchPromptGroup function passes req.body directly to updatePromptGroup() without filtering sens This issue is fixed in version 0.8.1.
CVE-2025-65814	A lack of security checks in the file import process of RHOPHI Analytics LLP Office App-Edit Word v6.4.1 allows attackers to execute a directory traversal.
CVE-2025-65815	A lack of security checks in the file import process of AB TECHNOLOGY Document Reader: PDF, DOC, PPT v65.0 allows attackers to execute a directory traversal.
CVE-2025-14293	The WP Job Portal plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 2.4.0 via the 'downloadCustomUploadedFile' functior it possible for authenticated attackers, with Subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive info
CVE-2025-14758	Incorrect configuration of replication security in the MariaDB component of the infra-operator in YAOOK Operator allows an on-path attacker to read database conte potentially including credentials
CVE-2025-14508	The MediaCommander – Bring Folders to Media, Posts, and Pages plugin for WordPress is vulnerable to unauthorized data deletion due to a missing capability chec import-csv REST API endpoint in all versions up to, and including, 2.3.1. This is due to the endpoint using `upload_files` capability check (Author level) for a destruc that can delete all folders. This makes it possible for authenticated attackers, with Author-level access and above, to delete all folder organization data created by and other users.
CVE-2025-55893	TOTOLINK N200RE V9.3.5u.6437_B20230519 is vulnerable to command Injection in setOpModeCfg via hostName.
CVE-2025-68113	ALTCHA is privacy-first software for captcha and bot protection. A cryptographic semantic binding flaw in ALTCHA libraries allows challenge payload splicing, which replay attacks. The HMAC signature does not unambiguously bind challenge parameters to the nonce, allowing an attacker to reinterpret a valid proof-of-work subr modified expiration value. This may allow previously solved challenges to be reused beyond their intended lifetime, depending on server-side replay handling and assumptions. The vulnerability primarily impacts abuse-prevention mechanisms such as rate limiting and bot mitigation. It does not directly affect data confidentia integrity. This issue has been addressed by enforcing explicit semantic separation between challenge parameters and the nonce during HMAC computation. Users upgrade to patched versions, which include version 1.0.0 of the altcha Golang package, version 1.0.0 of the altcha Rubygem, version 1.0.0 of the altcha pip packag

	1.0.0 of the altcha Erlang package, version 1.4.1 of the altcha-lib npm package, version 1.3.1 of the altcha-org/altcha Composer package, and version 1.3.0 of the org.altcha:altcha Maven package. As a mitigation, implementations may append a delimiter to the end of the `salt` value prior to HMAC computation (for example, expires=<time>&`). This prevents ambiguity between parameters and the nonce and is backward-compatible with existing implementations, as the delimiter is tr standard URL parameter separator.
CVE-2025-65427	An issue was discovered in Dbit N300 T1 Pro Easy Setup Wireless Wi-Fi Router on firmware version V1.0.0 does not implement rate limiting to /api/login allowing at brute force password enumerations.
CVE-2025-64520	GLPI is a free asset and IT management software package. Starting in version 9.1.0 and prior to version 10.0.21, an unauthorized user with an API access can read base entries. Users should upgrade to 10.0.21 to receive a patch.
CVE-2025-67735	Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.129.Final and 4.2.8.Final, the `io.netty.handler.codec.http.HttpRequ has a CRLF injection with the request URI when constructing a request. This leads to request smuggling when `HttpRequestEncoder` is used without proper sanitiz URI. Any application / framework using `HttpRequestEncoder` can be subject to be abused to perform request smuggling using CRLF injection. Versions 4.1.129.Fir 4.2.8.Final fix the issue.
CVE-2025-10163	The List category posts plugin for WordPress is vulnerable to time-based SQL Injection via the 'starting_with' parameter of the catlist shortcode in all versions up to including, 0.91.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible fo authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensit information from the database.
CVE-2025-65803	An integer overflow in the psdParser::ReadImageData function of FreeImage v3.18.0 and before allows attackers to cause a Denial of Service (DoS) via supplying a file.
CVE-2025-55311	An issue was discovered in Foxit PDF and Editor for Windows and macOS before 13.2 and 2025 before 2025.2. A crafted PDF can use JavaScript to alter annotation subsequently clear the file's modification status via JavaScript interfaces. This circumvents digital signature verification by hiding document modifications, allowing to mislead users about the document's integrity and compromise the trustworthiness of signed PDFs.
CVE-2025-43464	A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Tahoe 26.1. Visiting a website may lead to an app denial-of-se
CVE-2025-59935	GLPI is a free asset and IT management software package. Starting in version 10.0.0 and prior to version 10.0.21, an unauthenticated user can store an XSS payloa inventory endpoint. Users should upgrade to 10.0.21 to receive a patch.
CVE-2025-12687	A vulnerability in TeamViewer DEX Client (former 1E Client) - Content Distribution Service (NomadBranch.exe) prior version 25.11 for Windows allows malicious act denial of service (application crash) via a crafted command, resulting in service termination.
CVE-2025-67912	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Gal Dubinski Stars Testimonials stars-testimonials-with-slider-a grid allows Stored XSS.This issue affects Stars Testimonials: from n/a through <= 3.3.4.
CVE-2025-43511	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 18.7.2 and iPadOS 18.7.2. Processing maliciously crafted web lead to an unexpected process crash.
CVE-2025-14512	A flaw was found in glib. This vulnerability allows a heap buffer overflow and denial-of-service (DoS) via an integer overflow in GLib's GIO (GLib Input/Output) escape_byte_string() function when processing malicious file or remote filesystem attribute values.
CVE-2025-4097	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 11.10 before 18.4.6, 18.5 before 18.5.4, and 18.6 before 18.6.2 that could have allowed authenticated user to cause a denial of service condition by uploading specially crafted images.
CVE-2025-13891	The Image Gallery – Photo Grid & Video Gallery plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 2.13.3. This is due to the modula_list_folders AJAX endpoint that lacks proper path validation and base directory restrictions. While the endpoint verifies user capabilities (Author+ with uploa edit_posts permissions), it fails to validate that user-supplied directory paths reside within safe directories. This makes it possible for authenticated attackers, with access and above, to enumerate arbitrary directories on the server via the modula_list_folders endpoint.
CVE-2025-36917	In SwDcpItg of up_L2commonPdcpSecurity.cpp, there is a possible denial of service due to an incorrect bounds check. This could lead to remote denial of service w additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-68267	In JetBrains TeamCity before 2025.11.1 excessive privileges were possible due to storing GitHub personal access token instead of an installation token
CVE-2025-12960	The Simple CSV Table plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.0.1 via the `href` parameter in the `[csv]` sho due to insufficient path validation before concatenating user-supplied input to a base directory path. This makes it possible for authenticated attackers, with Contri access and above, to read the contents of arbitrary files on the server, which can contain sensitive information such as database credentials and authentication ke
CVE-2025-8872	On affected platforms running Arista EOS with OSPFv3 configured, a specially crafted packet can cause the OSFPv3 process to have high CPU utilization which may OSFPv3 process being restarted. This may cause disruption in the OSFPv3 routes on the switch. This issue was discovered internally by Arista and is not aware of a uses of this issue in customer networks.
CVE-2025-67951	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPZOOM WPZOOM Addons for Elementor wpzoom-elementor-a DOM-Based XSS.This issue affects WPZOOM Addons for Elementor: from n/a through <= 1.2.10.
CVE-2025-14157	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 6.3 before 18.4.6, 18.5 before 18.5.4, and 18.6 before 18.6.2 that could have allowed ar authenticated user to cause a Denial of Service condition by sending crafted API calls with large content parameters.

CVE-2025-67720	Pyrofork is a modern, asynchronous MTProto API framework. Versions 2.3.68 and earlier do not properly sanitize filenames received from Telegram messages in the download_media method before using them in file path construction. When downloading media, if the user does not specify a custom filename (which is the comm usage), the method falls back to using the file_name attribute from the media object. The attribute originates from Telegram's DocumentAttributeFilename and is c the message sender. This issue is fixed in version 2.3.69.
CVE-2025-68076	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Select-Themes Stockholm Core stockholm-core allows Stored X affects Stockholm Core: from n/a through <= 2.4.6.
CVE-2025-65296	NULL-pointer dereference vulnerabilities in Aqara Hub M2 4.3.6_0027, Hub M3 4.3.6_0025, and Camera Hub G3 4.1.9_0027 in the JSON processing enable denial-of attacks through malformed JSON inputs.
CVE-2025-36912	In cellular modem, there is a possible denial of service due to a logic error in the code. This could lead to remote denial of service with no additional execution privi User interaction is not needed for exploitation.
CVE-2023-53902	WebsiteBaker 2.13.3 contains a directory traversal vulnerability that allows authenticated attackers to delete arbitrary files by manipulating directory path parame can send crafted GET requests to /admin/media/delete.php with directory traversal sequences to delete files outside the intended directory.
CVE-2025-64994	A privilege escalation vulnerability was discovered in TeamViewer DEX (former 1E DEX), specifically within the 1E-Nomad-SetWorkRate instruction prior V17.1. The handling of executable search paths could allow local attackers with write access to a PATH directory on a device to escalate privileges and execute arbitrary code
CVE-2025-64995	A privilege escalation vulnerability was discovered in TeamViewer DEX (former 1E DEX), specifically within the 1E-Exchange-NomadClientHealth-ConfigureGeneralS instruction prior V3.4. Improper protection of the execution path on the local device allows attackers, with local access to the device during execution, to hijack the execute arbitrary code with SYSTEM privileges.
CVE-2025-68071	Authorization Bypass Through User-Controlled Key vulnerability in g5theme Essential Real Estate essential-real-estate allows Exploiting Incorrectly Configured Acce Security Levels.This issue affects Essential Real Estate: from n/a through <= 5.2.2.
CVE-2025-46287	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. An attac able to spoof their FaceTime caller ID.
CVE-2025-0969	The Brizy – Page Builder plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.7.16 via the get_users() functior it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive data including email addresses and hashed passwords of admi
CVE-2025-14064	The BuddyTask plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on multiple AJAX endpoints in up to, and including, 1.3.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to view, create, modify, and delete task boa to any BuddyPress group, including private and hidden groups they are not members of.
CVE-2025-12035	An integer overflow condition exists in Bluetooth Host stack, within the bt_br_acl_recv routine a critical path for processing inbound BR/EDR L2CAP traffic.
CVE-2025-8195	The JetWidgets For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Image Comparison and Subscribe widgets in all vers and including, 1.0.20 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-8780	The Livemesh SiteOrigin Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Hero Header and Pricing Table widgets in all vers and including, 3.9.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with c level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-7058	The Kingcabs theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘progressbarLayout’ parameter in all versions up to, and including, 1.1.9 due input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in will execute whenever a user accesses an injected page.
CVE-2025-9488	The Redux Framework plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘data’ parameter in all versions up to, and including, 4.5.8 due to ins sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in page execute whenever a user accesses an injected page.
CVE-2025-8199	The MarqueeAddons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Testimonial Marquee widget in all versions up to, and includin to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access a inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-11220	The Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Text Path widget in all versions up to, and including, 3.33.3 due to i neutralization of user-supplied input used to build SVG markup inside the widget. This makes it possible for authenticated attackers, with contributor-level access a inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-8617	The YITH WooCommerce Quick View plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's yith_quick_view shortcode in all versions up to including, 2.7.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contri access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-8687	The Enter Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown and Image Comparison widgets in all versions up to, including, 2.2.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contri access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-7960	The King Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Pricing Slider, Pricing Calculator, and Image Accord all versions up to, and including, 51.1.39 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authentica with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13850	The LS Google Map Router plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'map_type' parameter in all versions up to, and including, 1.1.0 insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary w pages that will execute whenever a user accesses an injected page.

CVE-2025-14278	The HT Slider for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'slide_title' parameter in all versions up to, and including, 1.7.4 insufficient input sanitization and output escaping in JavaScript. This makes it possible for authenticated attackers, with Contributor-level access and above, to inje web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-12109	The Header Footer Script Adder – Insert Code in Header, Body & Footer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the script adder presen all versions up to, and including, 2.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributo and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13367	The User Registration & Membership – Custom Registration Form Builder, Custom Login Form, User Profile, Content Restriction & Membership Plugin for WordPress to Stored Cross-Site Scripting via multiple shortcode attributes in all versions up to, and including, 4.4.6 due to insufficient input sanitization and output escaping. T possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses ar page.
CVE-2025-11670	Zohocorp ManageEngine ADManager Plus versions before 8025 are vulnerable to NTLM Hash Exposure. This vulnerability is exploitable only by technicians who ha “Impersonate as Admin” option enabled.
CVE-2025-13962	The Divelogs Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'latestdive' shortcode in all versions up to, and including, 1.5 insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13963	The FX Currency Converter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'fxcc_convert' shortcode in all versions up to, and inclu due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level acce to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13966	The Paypal Payment Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'buttom_image' parameter of the [paypal-shortcode] shortc versions up to, and including, 1.01 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-le and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13969	The Reviews Sorted plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'space' parameter of the [reviews-slider] shortcode in all versions up to including, 2.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and abo arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13989	The WP Dropzone plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'callback' shortcode attribute in all versions up to, and including, 1.1.1. T insufficient input sanitization and output escaping on user-supplied 'callback' attributes, which are evaluated as JavaScript code via the `new Function()` constructo 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 page.
CVE-2025-14032	The Bold Timeline Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' parameter in the 'bold_timeline_group' shortcode in all version including, 1.2.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and abo arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-11376	The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'colibri_loop' shortcode in all versions up to, and including, to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access a inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13839	The LJUsers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name' parameter of the 'ljuser' shortcode in all versions up to, and including, 1 insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-14143	The Ayo Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'color' parameter of the ayo_action shortcode in all versions up to, and due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbi scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-67896	Exim before 4.99.1 allows remote heap corruption that will be further described on 2025-12-18.
CVE-2025-14393	The Wpik WordPress Basic Ajax Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'dname' parameter in all versions up to, and including insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary w pages that will execute whenever a user accesses an injected page.
CVE-2025-12537	The Addon Elements for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 1.14.3. This is due to insuffi sanitization and output escaping on multiple widget parameters. This makes it possible for authenticated attackers, with Contributor-level access and above, to inj web scripts via multiple widget parameters in pages that will execute whenever a user accesses an injected page.
CVE-2025-13740	The Lightweight Accordion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `lightweight-accordion` shortcode in all versions up to, 1.5.20 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-lev above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-11876	The Mailgun Subscriptions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mailgun_subscription_form' shortcode in all versions up including, 1.3.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contri access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-12965	The Magical Posts Display plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mpac_title_tag' parameter in the Magical Posts Accordion widge versions up to, and including, 1.2.54 due to insufficient input sanitization and output escaping on user-supplied HTML tag names. This makes it possible for authent attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-14030	The AI Feeds plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'aife_post_meta' shortcode in all versions up to, and including, 1.0.22 due to i input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in will execute whenever a user accesses an injected page.
CVE-2025-13961	The Data Visualizer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'visualize' shortcode in all versions up to, and including, 1.1 du insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-	The GPXpress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'gpxpress' shortcode in all versions up to, and including, 1.3 due to i input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to in

13960	web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13906	The WP Flot plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'linechart' shortcode in all versions up to, and including, 0.2.2 due to i input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to in web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13904	The WPGancio plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'gancio-event' shortcode in all versions up to, and including, 1.12 du insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-12650	The Simple post listing plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class_name' parameter in the postlist shortcode in all versions up t including, 0.2. This is due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page via mouse interaction.
CVE-2025-14387	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 4.3.1 due to insufficien sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in page execute whenever a user accesses an injected page.
CVE-2025-12830	The Better Elementor Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Slider widget in all versions up to, and including, 1.5.4 due to input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to in web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-9856	The Popup Builder – Create highly converting, mobile friendly marketing popups. plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 's shortcode in all versions up to, and including, 4.4.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13728	The FluentAuth – The Ultimate Authorization & Security Plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `fluent_auth_reset_password` shortcode in all versions up to, and including, 2.0.3 due to insufficient input sanitization and output escaping on user supplied attribu 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 ac injected page.
CVE-2025-13610	The RegistrationMagic – Custom Registration Forms, User Registration, Payment, and User Login plugin for WordPress is vulnerable to Stored Cross-Site Scripting v 'RM_Forms' shortcode in all versions up to, and including, 6.0.6.7 due to insufficient input sanitization and output escaping on the 'theme' attribute. This makes it p authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected pa
CVE-2025-13747	The NewStatPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via a regex bypass in nsp_shortcode function in all versions up to, and including insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13705	The Custom Frames plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' parameter of the 'customframe' shortcode in all versions up to, 1.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to injec web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13840	The BUKAZU Search widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'shortcode' parameter of the 'bukazu_search' shortcode in all v and including, 3.3.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with C level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-9873	The a3 Lazy Load plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 2.7.5 due to insufficient input sanitization an escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in p execute whenever a user accesses an injected page.
CVE-2025-13843	The VigLink SpotLight By ShortCode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'float' parameter of the 'spotlight' shortcode in all vers and including, 1.0.a due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with C level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13846	The Easy Map Creator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'width' parameter in all versions up to, and including, 3.0.2 due to in input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in will execute whenever a user accesses an injected page.
CVE-2025-13608	The CC Child Pages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'child_pages' shortcode in all versions up to, and including, 2.0.0. This i insufficient input sanitization and output escaping on four user-supplied attributes (use_custom_link, use_custom_link_target, use_custom_thumbs, and use_custom the 'show_child_pages' function. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages execute whenever a user accesses an injected page.
CVE-2025-13866	The Flow-Flow Social Feed Stream plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the flow_flow_social action in versions 3.0.0 to 4.7.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify plugin settings and store arb JavaScript that executes whenever the plugin settings page is viewed.
CVE-2025-13884	The Hide Email Address plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'inline_css' parameter in the `bg-hide-email-address` shortcode in to, and including, 0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13885	The Zenost Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link' and 'target' parameters in the `button` shortcode in all versio including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-13889	The Simple Nivo Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' shortcode parameter in all versions up to, and including, 0.5.6 d insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary w pages that will execute whenever a user accesses an injected page.
CVE-2025-8779	The All-in-One Addons for Elementor – WidgetKit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Team and Countdown widgets in to, and including, 2.5.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, wit level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-14119	The App Landing Template Blocks for WPBakery (Visual Composer) Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'atvc_vide shortcode in all versions up to, and including, 2.0.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.

CVE-2025-9436	The Widgets for Google Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `trustindex` shortcode in all versions up to, and in 13.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-lev above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-14518	A vulnerability was identified in PowerJob up to 5.1.2. This vulnerability affects the function checkConnectivity of the file src/main/java/tech/powerjob/common/utils/net/PingPongUtils.java of the component Network Request Handler. The manipulation of the argument targetIp/targetPo server-side request forgery. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.
CVE-2025-14568	A security vulnerability has been detected in haxxorsid Stock-Management-System up to fbbbf213e9c93b87183a3891f77e3cc7095f22b0. This impacts an unknown the file model/User.php. The manipulation of the argument employee_id/id/admin leads to sql injection. The attack can be initiated remotely. The exploit has been publicly and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are availa vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maint
CVE-2025-14731	A weakness has been identified in CTCMS Content Management System up to 2.1.2. This affects an unknown function in the library /ctcms/apps/libraries/CT_Parser component Frontend/Template Management Module. This manipulation causes improper neutralization of special elements used in a template engine. The attack is be carried out remotely. The exploit has been made available to the public and could be exploited.
CVE-2025-14522	A vulnerability was detected in baowzh hfly up to 638ff9abe9078bc977c132b37acbe1900b63491c. The impacted element is an unknown function of the file /Public/Kindeditor/php/upload_json.php. Performing manipulation of the argument imgFile results in unrestricted upload. It is possible to initiate the attack remotely is now 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 The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-14780	A vulnerability was detected in Xiongwei Smart Catering Cloud Platform 2.1.6446.28761. The affected element is an unknown function of the file /dishtrade/dish_trade_detail_get. The manipulation of the argument filter results in sql injection. The attack can be executed remotely. The exploit is now public and used.
CVE-2025-14516	A vulnerability was found in Yalantis uCrop 2.2.11. Affected by this issue is the function downloadFile of the file com.yalantis.ucrop.task.BitmapLoadTask.java of the URL Handler. Performing manipulation results in server-side request forgery. The attack may be initiated remotely. The exploit has been made public and could be vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-14695	A vulnerability was determined in SamuNatsu HaloBot up to 026b01d4a896d93eaaf9d5163a287dc9f267515b. Affected is the function html_renderer of the file plugins/html_renderer/index.js of the component Inter-plugin API. Executing manipulation of the argument action can lead to dynamically-managed code resources can be launched remotely. The exploit has been publicly disclosed and may be utilized. This product does not use versioning. This is why information about affecte unaffected releases are unavailable. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products t longer supported by the maintainer.
CVE-2025-14674	A vulnerability was found in aizuda snail-job up to 1.6.0. Affected by this vulnerability is the function QLExpressEngine.doEval of the file snail-job-common/snail-job-core/src/main/java/com/aizuda/snailjob/common/core/expression/strategy/QLExpressEngine.java. The manipulation results in injection. The attack can be launched Upgrading to version 1.7.0-beta1 addresses this issue. The patch is identified as 978f316c38b3d68bb74d2489b5e5f721f6675e86. The affected component should
CVE-2025-14749	A vulnerability was identified in Ningyuanda TC155 57.0.2.0. This impacts an unknown function of the file /onvif/device_service of the component ONVIF PTZ Contro The manipulation leads to improper access controls. The attack requires being on the local network. The exploit is publicly available and might be used. The vendo contacted early about this disclosure but did not respond in any way.
CVE-2025-0836	Missing Authorization vulnerability in Milestone Systems XProtect VMS allows users with read-only access to Management Server to have full read/write access to M API.
CVE-2025-14607	A vulnerability was detected in OFFIS DCMTK up to 3.6.9. Affected by this issue is the function DcmByteString::makeDicomByteString of the file dcmdata/libsrc/dcb component dcmdata. The manipulation results in memory corruption. The attack can be launched remotely. Upgrading to version 3.7.0 can resolve this issue. The identified as 4c0e5c10079392c594d6a7abd95dd78ac0aa556a. You should upgrade the affected component.
CVE-2025-14586	A vulnerability was determined in TOTOLINK X5000R 9.1.0cu.2089_B20211224. Affected by this issue is the function snprintf of the file /cgi-bin/cstecgi.cgi?action=exportOvpn&type=user. This manipulation of the argument User causes os command injection. Remote exploitation of the attack is possible. The exploit ha publicly disclosed and may be utilized.
CVE-2025-14589	A weakness has been identified in code-projects Prison Management System 2.0. This issue affects some unknown processing of the file /admin/search.php. Execut manipulation of the argument keyname can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and exploited.
CVE-2025-68146	filelock is a platform-independent file lock for Python. In versions prior to 3.20.1, a Time-of-Check-Time-of-Use (TOCTOU) race condition allows local attackers to co truncate arbitrary user files through symlink attacks. The vulnerability exists in both Unix and Windows lock file creation where filelock checks if a file exists before with O_TRUNC. An attacker can create a symlink pointing to a victim file in the time gap between the check and open, causing os.open() to follow the symlink and t target file. All users of filelock on Unix, Linux, macOS, and Windows systems are impacted. The vulnerability cascades to dependent libraries. The attack requires lo access and ability to create symlinks (standard user permissions on Unix; Developer Mode on Windows 10+). Exploitation succeeds within 1-3 attempts when lock predictable. The issue is fixed in version 3.20.1. If immediate upgrade is not possible, use SoftFileLock instead of UnixFileLock/WindowsFileLock (note: different lock semantics, may not be suitable for all use cases); ensure lock file directories have restrictive permissions (chmod 0700) to prevent untrusted users from creating s and/or monitor lock file directories for suspicious symlinks before running trusted applications. These workarounds provide only partial mitigation. The race conditio exploitable. Upgrading to version 3.20.1 is strongly recommended.
CVE-2025-8082	Improper neutralization of the title date in the 'VDatePicker' component in Vuetify, allows unsanitized HTML to be inserted into the page. This can lead to a Cross-S (XSS) https://owasp.org/www-community/attacks/xss attack. The vulnerability occurs because the 'title-date-format' property of the 'VDatePicker' can accept a use function and assign its output to the 'innerHTML' property of the title element without sanitization. This issue affects Vuetify versions greater than or equal to 2.0.0 3.0.0. Note: Version 2.x of Vuetify is End-of-Life and will not receive any updates to address this issue. For more information see here https://v2.vuetifyjs.com/en/ab
CVE-2025-65835	The Cordova plugin cordova-plugin-x-socialsharing (SocialSharing-PhoneGap-Plugin) for Android 6.0.4, registers an exported broadcast receiver nl.xservices.plugins.ShareChooserPendingIntent with an android.intent.action.SEND intent filter. The onReceive implementation accesses Intent.EXTRA_CHOSEN_C without checking for null. If a broadcast is sent with extras present but without EXTRA_CHOSEN_COMPONENT, the code dereferences a null value and throws a NullPointerException. Because the receiver is exported and performs no permission or caller validation, any local application on the device can send crafted ACTIO broadcasts to this component and repeatedly crash the host application, resulting in a local, unauthenticated application-level denial of service for any app that inc plugin.
CVE-2025-61822	ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system write. A could exploit this vulnerability to write malicious files to arbitrary locations on the file system. Exploitation of this issue does not require user interaction and scope
CVE-2025-	Insecure defaults in the Server Agent component of Fortra's Core Privileged Access Manager (BoKS) can result in the selection of weak password hash algorithms. affects BoKS Server Agent 9.0 instances that support yescrypt and are running in a BoKS 8.1 domain.

13532	
CVE-2025-61823	ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could l arbitrary file system read. A high privileged attacker could exploit this vulnerability to access sensitive files and data on the server. Exploitation of this issue requir interaction and scope is changed.
CVE-2025-12834	The Accept Stripe Payments Using Contact Form 7 plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'failure_message' parameter in versic including, 3.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages if they can successfully trick a user into performing an action such as clicking on a link.
CVE-2025-14132	The Category Dropdown List plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute successfully trick a user into performing an action such as clicking on a link.
CVE-2025-34504	KodExplorer 4.52 contains an open redirect vulnerability in the user login page that allows attackers to manipulate the 'link' parameter. Attackers can craft malicio link parameter to redirect users to arbitrary external websites after authentication.
CVE-2025-14049	The VikRentItems Flexible Rental Management System plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'delto' parameter in all versions including, 1.2.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pag execute if they can successfully trick a user into performing an action such as clicking on a link.
CVE-2025-66452	LibreChat is a ChatGPT clone with additional features. In versions 0.8.0 and below, there is no handler for JSON parsing errors; SyntaxError from express.json() inclu input in the error message, which gets reflected in responses. User input (including HTML/JavaScript) can be exposed in error responses, creating an XSS risk if Cor isn't strictly enforced. This issue does not have a fix at the time of publication.
CVE-2025-14138	The WPLG Default Mail From plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that ex can successfully trick a user into performing an action such as clicking on a link.
CVE-2025-14137	The Simple AL Slider plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and includin to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if th successfully trick a user into performing an action such as clicking on a link.
CVE-2025-14372	Use after free in Password Manager in Google Chrome prior to 143.0.7499.110 allowed a remote attacker to potentially perform a sandbox escape via a crafted HT (Chromium security severity: Medium)
CVE-2025-12077	The WP to LinkedIn Auto Publish plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via PostMessage in all versions up to, and including, 1.9.8 due input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can succes user into performing an action such as clicking on a link.
CVE-2025-12076	The Social Media Auto Publish plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via PostMessage parameter in all versions up to, and including, 3 insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they successfully trick a user into performing an action such as clicking on a link.
CVE-2025-64250	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in wpWax Directorist directorist allows Phishing.This issue affects Directorist: from n/a through <=
CVE-2025-67986	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Barn2 Plugins Document Library Lite document-library-lite allo XSS.This issue affects Document Library Lite: from n/a through <= 1.1.7.
CVE-2025-13988	The 评论小秘书 plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 1.3. to insufficient input sanitization and output escaping on the `$_SERVER['PHP_SELF']` variable in the plugin's settings page. This makes it possible for unauthenticat to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.
CVE-2025-14125	The Complag plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 1.0.2 insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they successfully trick a user into performing an action such as clicking on a link.
CVE-2025-55816	HotelDruid v3.0.7 and before is vulnerable to Cross Site Scripting (XSS) in the /modifica_app.php file.
CVE-2025-51962	A HTML Injection vulnerability in the comment section of the project page in MicroStudio 24.01.29 allows remote attackers to inject arbitrary web script or HTML via parameter of add_project_comment function.
CVE-2023-36337	A reflected cross-site scripting (XSS) vulnerability in the component /index.php/cuzh4 of PHP Inventory Management System 1 allows attackers to execute arbitrary or HTML via a crafted payload.
CVE-2025-29231	A stored cross-site scripting (XSS) vulnerability in the page_save component of Linksys E5600 V1.1.0.26 allows attackers to execute arbitrary web scripts or HTML payload injected into the hostname and domainName parameters.
CVE-2025-14129	The Like DisLike Voting plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and includ to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if th successfully trick a user into performing an action such as clicking on a link.
CVE-2024-40593	A key management errors vulnerability in Fortinet FortiAnalyzer 7.4.0 through 7.4.2, FortiAnalyzer 7.2.0 through 7.2.5, FortiAnalyzer 7.0 all versions, FortiAnalyzer versions, FortiManager 7.4.0 through 7.4.2, FortiManager 7.2.0 through 7.2.5, FortiManager 7.0 all versions, FortiManager 6.4 all versions, FortiOS 7.6.0, FortiOS 7. 7.2.7, FortiOS 7.0.14, FortiPortal 6.0 all versions may allow an authenticated admin to retrieve a certificate's private key via the device's admin shell.
CVE-2025-	A flaw was found in Keycloak. An IDOR (Broken Access Control) vulnerability exists in the admin API endpoints for authorization resource management, specifically ResourceSetService and PermissionTicketService. The system checks authorization against the resourceServer (client) ID provided in the API request, but the back

14777	lookup and modification operations (findById, delete) only use the resourceId. This mismatch allows an authenticated attacker with fine-grained admin permissions (e.g., Client A) to delete or update resources belonging to another client (Client B) within the same realm by supplying a valid resource ID.
CVE-2025-10289	The Filter & Grids plugin for WordPress is vulnerable to SQL Injection via the 'phrase' parameter in all versions up to, and including, 3.2.0 due to insufficient escapir supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL que already existing queries that can be used to extract sensitive information from the database. This only works on MariaDB as the query results in a syntax error on M
CVE-2025-62330	HCL DevOps Deploy is susceptible to a cleartext transmission of sensitive information because the HTTP port remains accessible and does not redirect to HTTPS as a result, an attacker with network access could intercept or modify user credentials and session-related data via passive monitoring or man-in-the-middle attacks.
CVE-2025-13439	The Fancy Product Designer plugin for WordPress is vulnerable to Information Disclosure in all versions up to, and including, 6.4.8. This is due to insufficient validat supplied input in the 'url' parameter of the fpd_custom_uplod_file AJAX action, which flows directly into the getimagesize() function without sanitization. While direc via PHP filter chains is blocked on PHP 8+ due to a separate code bug in the plugin, the vulnerability can be exploited via a TOCTOU race condition (CVE-2025-1323 present in the same plugin, or may be directly exploitable on PHP 7.x installations. This makes it possible for unauthenticated attackers to read arbitrary sensitive f server, including wp-config.php.
CVE-2025-13489	IBM UCD - IBM DevOps Deploy 8.1 through 8.1.2.3 Deploy transmits data in clear text that could allow an attacker to obtain sensitive information using man in the techniques.
CVE-2025-53960	When issuing JSON Web Tokens (JWT), Apache StreamPark directly uses the user's password as the HMAC signing key (e.g., with the HS256 algorithm). An attacker this vulnerability to perform offline brute-force attacks on the user's password using a captured JWT, or to arbitrarily forge identity tokens for the user if the passwo known, ultimately leading to complete account takeover. This issue affects Apache StreamPark: from 2.0.0 before 2.1.7. Users are recommended to upgrade to ver which fixes the issue.
CVE-2025-9116	The WPS Visitor Counter Plugin WordPress plugin through 1.4.8 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, lead to Reflected Cross-Site Scripting in old web browsers.
CVE-2025-11467	The RSS Aggregator by Feedzy – Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to Blind Server-Side Requ all versions up to, and including, 5.1.1 via the feedzy_lazy_load function. This makes it possible for unauthenticated attackers to make web requests to arbitrary loc originating from the web application and can be used to query and modify information from internal services.
CVE-2025-13281	A half-blind Server Side Request Forgery (SSRF) vulnerability exists in kube-controller-manager when using the in-tree Portworx StorageClass. This vulnerability allo authorized users to leak arbitrary information from unprotected endpoints in the control plane’s host network (including link-local or loopback services).
CVE-2025-67716	The Auth0 Next.js SDK is a library for implementing user authentication in Next.js applications. Versions 4.9.0 through 4.12.1 contain an input-validation flaw in the parameter, which could allow attackers to inject unintended OAuth query parameters into the Auth0 authorization request. Successful exploitation may result in to issued with unintended parameters. This issue is fixed in version 4.13.0.
CVE-2025-66004	A Path Traversal vulnerability in usbmuxd allows local users to escalate to the service user.This issue affects usbmuxd: before 3ded00c9985a5108cfc7591a309f9a7
CVE-2025-14660	A flaw has been found in DecoCMS Mesh up to 1.0.0-alpha.31. Affected by this vulnerability is the function createTool of the file packages/sdk/src/mcp/teams/api.ts component Workspace Domain Handler. This manipulation of the argument domain causes improper access controls. The attack can be initiated remotely. The cor attack is rather high. The exploitation appears to be difficult. The exploit has been published and may be used. Upgrading to version 1.0.0-alpha.32 addresses this name: 5f7315e05852faf3a9c177c0a34f9ea9b0371d3d. It is recommended to upgrade the affected component.
CVE-2025-64897	ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Improper Access Control vulnerability. A low privileged attacker could leverage this vu bypass security measures and gain limited unauthorized write access potentially resulting in denial of service. Exploitation of this issue requires user interaction.
CVE-2025-14087	A flaw was found in GLib (Gnome Lib). This vulnerability allows a remote attacker to cause heap corruption, leading to a denial of service or potential code executio underflow in the GVariant parser when processing maliciously crafted input strings.
CVE-2025-43388	An injection issue was addressed with improved validation. This issue is fixed in macOS Tahoe 26.1. An app may be able to access sensitive user data.
CVE-2025-66963	An issue in Hitron HI3120 v.7.2.4.5.2b1 allows a local attacker to obtain sensitive information via the Logout option in the index.html
CVE-2025-43381	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Tahoe 26.1. A malicious app may be able to delete protected user data.
CVE-2025-43463	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Sonoma 14.8.3, macOS Tahoe 26.1, m 15.7.3. An app may be able to access sensitive user data.
CVE-2025-43406	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Tahoe 26.1. An app may be able to access sensitive user data.
CVE-2025-43461	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Tahoe 26.1. An app may be able to access protected user data.
CVE-2025-43466	An injection issue was addressed with improved validation. This issue is fixed in macOS Tahoe 26.1. An app may be able to access sensitive user data.
CVE-	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26.1. A standard user may be able to view files made from a disk

2025-43470	belonging to an administrator.
CVE-2025-43471	The issue was addressed with improved checks. This issue is fixed in macOS Tahoe 26.1. An app may be able to access sensitive user data.
CVE-2025-43473	This issue was addressed with improved state management. This issue is fixed in macOS Tahoe 26.1. An app may be able to access sensitive user data.
CVE-2025-43482	The issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. An app may be able to cause a denia
CVE-2025-43513	A permissions issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. An app may be able to r location information.
CVE-2025-43519	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. An app may be able to access data.
CVE-2025-43521	A downgrade issue affecting Intel-based Mac computers was addressed with additional code-signing restrictions. This issue is fixed in macOS Sequoia 15.7.3. An ap able to access sensitive user data.
CVE-2025-43523	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.3. An app may be able to access sensitive user data.
CVE-2025-43530	This issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. An app may be able to access sensitive user
CVE-2025-43538	A logging issue was addressed with improved data redaction. This issue is fixed in macOS Sonoma 14.8.3. An app may be able to access sensitive user data.
CVE-2025-46276	An information disclosure issue was addressed with improved privacy controls. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. An app may be access sensitive user data.
CVE-2025-43416	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. An app may be able to access protecte
CVE-2025-36929	In AreFencesRegistered of gxp_fence_manager.cc, there is a possible information leak due to improper input validation. This could lead to local information disclosu additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2025-13993	The MailerLite – Signup forms (official) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'form_description' and 'success_message' paramete up to, and including, 1.7.16 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator access inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-4970	The BSK PDF Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 3.7.1 due to insuffi sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pa execute whenever a user accesses the SVG file. This only affects multi-site installations and installations where unfiltered_html has been disabled.
CVE-2025-36921	In ProtocolPsUnthrottleApn() of protocolpsadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information di baseband firmware compromise required. User interaction is not needed for exploitation.
CVE-2025-43351	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26.1. An app may be able to access protected user data.
CVE-2025-36889	In onCreateTasks of CameraActivity.java, there is a possible permission bypass due to a confused deputy. This could lead to local information disclosure with no ad execution privileges needed. User interaction is not needed for exploitation.
CVE-2024-42197	HCL Workload Scheduler stores user credentials in plain text which can be read by a local user.
CVE-2025-64873	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64858	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64861	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-	Missing Authorization vulnerability in merkulove Reformer for Elementor reformer-elementor allows Exploiting Incorrectly Configured Access Control Security Level

2025-68086	affects Reformer for Elementor: from n/a through <= 1.0.6.
CVE-2025-64863	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64869	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-68085	Missing Authorization vulnerability in merkulove Buttoner for Elementor buttoner-elementor allows Exploiting Incorrectly Configured Access Control Security Levels affects Buttoner for Elementor: from n/a through <= 1.0.6.
CVE-2025-64881	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64875	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64853	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64887	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2025-64566	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2025-64888	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2023-53903	WebsiteBaker 2.13.3 contains a stored cross-site scripting vulnerability that allows authenticated users to upload malicious SVG files with embedded JavaScript. Att upload crafted SVG files with script tags that execute when the file is viewed, enabling persistent cross-site scripting attacks.
CVE-2023-53901	WBCE CMS 1.6.1 contains a cross-site scripting vulnerability that allows attackers to inject malicious HTML and CSS to capture user keystrokes. Attackers can uploa HTML file with CSS-based keylogging techniques to intercept password characters through background image requests.
CVE-2025-64857	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64852	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-68083	Cross-Site Request Forgery (CSRF) vulnerability in Meks Meks Quick Plugin Disabler meks-quick-plugin-disabler allows Cross Site Request Forgery.This issue affects Plugin Disabler: from n/a through <= 1.0.
CVE-2025-68087	Missing Authorization vulnerability in merkulove Modalier for Elementor modalier-elementor allows Exploiting Incorrectly Configured Access Control Security Levels affects Modalier for Elementor: from n/a through <= 1.0.6.
CVE-2025-64850	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-68088	Missing Authorization vulnerability in merkulove Huger for Elementor huger-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This Huger for Elementor: from n/a through <= 1.1.5.
CVE-2025-64847	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64845	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64841	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64840	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att

64839	malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64569	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2025-64833	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64829	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64827	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64826	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64825	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64565	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2025-64564	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2025-64597	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-66147	Missing Authorization vulnerability in merkulove Coder for Elementor coder-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This i Coder for Elementor: from n/a through <= 1.0.13.
CVE-2025-64547	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-67490	The Auth0 Next.js SDK is a library for implementing user authentication in Next.js applications. When using versions 4.11.0 through 4.11.2 and 4.12.0, simultaneou the same client may result in improper lookups in the TokenRequestCache for the request results. This issue is fixed in versions 4.11.2 and 4.12.1.
CVE-2025-64548	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64549	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64550	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2025-64551	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2025-64553	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-66167	Missing Authorization vulnerability in merkulove Lottier lottier-gutenberg allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects L n/a through <= 1.1.1.
CVE-2025-66166	Missing Authorization vulnerability in merkulove Lottier for Elementor lottier-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This Lottier for Elementor: from n/a through <= 1.0.9.
CVE-2025-66165	Missing Authorization vulnerability in merkulove Lottier for WPBakery lottier-wpbakery allows Exploiting Incorrectly Configured Access Control Security Levels.This i Lottier for WPBakery: from n/a through <= 1.1.7.
CVE-2025-66164	Missing Authorization vulnerability in merkulove Laser laser allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Laser: from n/ 1.1.1.
CVE-2025-	Missing Authorization vulnerability in merkulove Masker for Elementor masker-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.Th

66163	affects Masker for Elementor: from n/a through <= 1.1.4.
CVE-2025-66162	Missing Authorization vulnerability in merkulove Spoter for Elementor spoter-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This Spoter for Elementor: from n/a through <= 1.04.
CVE-2025-66161	Missing Authorization vulnerability in merkulove Grider for Elementor grider-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This Grider for Elementor: from n/a through <= 1.0.8.
CVE-2025-66134	Missing Authorization vulnerability in NinjaTeam FileBird Pro filebird-pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fi from n/a through <= 6.4.9.
CVE-2025-64563	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2025-64554	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64555	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-66127	Missing Authorization vulnerability in g5theme Essential Real Estate essential-real-estate allows Exploiting Incorrectly Configured Access Control Security Levels.Th affects Essential Real Estate: from n/a through <= 5.2.2.
CVE-2025-64556	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-66122	Missing Authorization vulnerability in Design Stylish Price List stylish-price-list allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affe Price List: from n/a through <= 7.2.2.
CVE-2025-64557	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64558	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64541	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64559	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64543	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2025-64560	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2025-64562	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2025-64544	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2025-14539	The The Shortcode Ajax plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.0. This is due to the software allo execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary sh
CVE-2025-64572	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64596	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64822	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi

64615	
CVE-2025-64613	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64614	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64590	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64586	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-66843	grav before v1.7.49.5 has a Stored Cross-Site Scripting (Stored XSS) vulnerability in the page editing functionality. An authenticated low-privileged user with permi content can inject malicious JavaScript payloads into editable fields. The payload is stored on the server and later executed when any other user views or edits the page.
CVE-2025-67502	Taguette is an open source qualitative research tool. In versions 1.5.1 and below, attackers can craft malicious URLs that redirect users to arbitrary external websit authentication. The application accepts a user-controlled next parameter and uses it directly in HTTP redirects without any validation. This can be exploited for phis where victims believe they are interacting with a trusted Taguette instance but are redirected to a malicious site designed to steal credentials or deliver malware. fixed in version 1.5.2.
CVE-2025-64616	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64626	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64619	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64620	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64585	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64622	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64583	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2025-64623	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64612	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64611	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64591	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64592	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64609	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64593	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64607	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att

64594	malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64606	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64605	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64604	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64603	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64602	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64601	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64600	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64599	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64598	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64582	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64627	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64821	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64803	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64799	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64800	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64801	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-67906	In MISP before 2.5.28, app/View/Elements/Workflows/executionPath.ctp allows XSS in the workflow execution path.
CVE-2025-64802	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64575	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64804	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64789	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi

64574	
CVE-2025-14748	A vulnerability was determined in Ningyuanda TC155 57.0.2.0. This affects an unknown function of the file /onvif/device_service of the component ONVIF Device Ma Service. Executing manipulation of the argument FactoryDefault with the input Hard can lead to improper access controls. The attack requires access to the local n exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-64808	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64814	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64817	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64820	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64797	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-14020	LINE client for Android versions prior to 14.20 contains a UI spoofing vulnerability in the in-app browser where the full-screen security Toast notification is not prope displayed when users return from another application, potentially allowing attackers to conduct phishing attacks by impersonating legitimate interfaces.
CVE-2025-64796	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64794	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64793	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64792	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64791	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-37732	Improper neutralization of input during web page generation ('Cross-site Scripting') (CWE-79) allows an authenticated user to render HTML tags within a user’s bro integration package upload functionality. This issue is related to ESA-2025-17 (CVE-2025-25018) bypassing that fix to achieve HTML injection.
CVE-2025-64790	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64576	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64577	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64578	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64579	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64580	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64581	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-65430	An issue was discovered in allauth-django before 65.13.0. IdP: marking a user as is_active=False after having handed tokens for that user while the account was st no effect. Fixed the access/refresh tokens are now rejected.
CVE-2025-65431	An issue was discovered in allauth-django before 65.13.0. Both Okta and NetIQ were using preferred_username as the identifier for third-party provider accounts. T may be mutable and should therefore be avoided for authorization decisions. The providers are now using sub instead.

CVE-2025-64823	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-64545	Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privile to execute malicious scripts in the context of the victim's browser. Exploitation of this issue requires user interaction, such as visiting a crafted URL or interacting w manipulated web page.
CVE-2025-68165	In JetBrains TeamCity before 2025.11 reflected XSS was possible on VCS Root setup
CVE-2025-14520	A weakness has been identified in baowzh hfly up to 638ff9abe9078bc977c132b37acbe1900b63491c. Impacted is an unknown function of the file /admin/index.php/datafile/delfile. This manipulation of the argument filename causes path traversal. The attack is possible to be carried out remotely. The exploit h made available to the public and could be exploited. This product adopts a rolling release strategy to maintain continuous delivery The vendor was contacted early disclosure but did not respond in any way.
CVE-2025-64546	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged att malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable fi
CVE-2025-68166	In JetBrains TeamCity before 2025.11 a DOM-based XSS was possible on the OAuth connections tab
CVE-2025-68269	In JetBrains IntelliJ IDEA before 2025.3 missing confirmation allowed opening of untrusted remote projects over SSH
CVE-2025-65590	nopCommerce 4.90.0 is vulnerable to Cross Site Scripting (XSS) via the Blog posts functionality in the Content Management area.
CVE-2025-65591	nopCommerce 4.90.0 is vulnerable to Cross Site Scripting (XSS) via the Currencies functionality.
CVE-2025-67724	Tornado is a Python web framework and asynchronous networking library. In versions 6.5.2 and below, the supplied reason phrase is used unescaped in HTTP heac could be used for header injection) or in HTML in the default error page (where it could be used for XSS) and can be exploited by passing untrusted or malicious da reason argument. Used by both RequestHandler.set_status and tornado.web.HTTPError, the argument is designed to allow applications to pass custom "reason" ph "Not Found" in HTTP/1.1 404 Not Found) to the HTTP status line (mainly for non-standard status codes). This issue is fixed in version 6.5.3.
CVE-2025-66450	LibreChat is a ChatGPT clone with additional features. In versions 0.8.0 and below, when a user posts a question, the iconURL parameter of the POST request can b an attacker. The malicious code is then stored in the chat which can then be shared to other users. When sharing chats with a potentially malicious “tracker”, reso can lead to loss of privacy for users who view the chat link that is sent to them. This issue is fixed in version 0.8.1.
CVE-2025-68268	In JetBrains TeamCity before 2025.11.1 reflected XSS was possible on the storage settings page
CVE-2025-46296	An authorization bypass vulnerability in FileMaker Server Admin Console allowed administrator roles with minimal privileges to access administrative features such license details and downloading application logs. This vulnerability has been fully addressed in FileMaker Server 22.0.4.
CVE-2025-67730	Frappe Learning Management System (LMS) is a learning system that helps users structure their content. Versions prior to 2.42.0 allow authenticated users to add HTML and JavaScript through description fields in the Job, Course and Batch forms. This issue is fixed in version 2.42.0.
CVE-2025-36746	SolarEdge monitoring platform contains a Cross-Site Scripting (XSS) flaw that allows an authenticated user to inject payloads into report names, which may execut browser during a deletion attempt.
CVE-2025-67734	Frappe Learning Management System (LMS) is a learning system that helps users structure their content. Versions prior to 2.42.0 allowed authenticated attackers JavaScript through the Company Website field of the Job Form, exposing users to an XSS attack. The script could then be executed in the browsers of users who op malicious job posting. This issue is fixed in version 2.42.0.
CVE-2025-14365	The Eyewear prescription form plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 6.0.1. This is due to missing capabilit the RemoveItems AJAX action. This makes it possible for unauthenticated attackers to delete arbitrary WooCommerce product categories, including all of their chil via the 'catIds' parameter.
CVE-2025-13093	The Devs CRM – Manage tasks, attendance and teams all together plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capabil the '/wp-json/devs-crm/v1/bulk-update' REST-API endpoint in all versions up to, and including, 1.1.8. This makes it possible for unauthenticated attackers to update
CVE-2025-12362	The myCred – Points Management System For Gamification, Ranks, Badges, and Loyalty Program plugin for WordPress is vulnerable to Missing Authorization in ver and including, 2.9.7. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attacl approve withdrawal requests, modify user point balances, and manipulate the payment processing system via the cashcred_pay_now AJAX action.
CVE-2025-12348	The Icegram Express - Email Subscribers, Newsletters and Marketing Automation Plugin for WordPress is vulnerable to Missing Authorization in versions up to, and 5.9.10. This is due to the plugin not properly verifying that a user is authorized to perform an action in the `run_action_scheduler_task` function. This makes it poss unauthenticated attackers to execute scheduled actions early or repeatedly by guessing action IDs, potentially triggering email sends, maintenance tasks, or other operations, causing unexpected state changes and resource usage.
CVE-2025-12809	The Dokan Pro plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the `/dokan/v1/wholesale/register` REST API versions up to, and including, 4.1.3. This makes it possible for unauthenticated attackers to enumerate users and retrieve their email addresses via the REST API b user ID, along with other information such as usernames, display names, user roles, and registration dates.
CVE-	

2025-64639	Missing Authorization vulnerability in WP Compress WP Compress for MainWP wp-compress-mainwp allows Exploiting Incorrectly Configured Access Control Securit issue affects WP Compress for MainWP: from n/a through <= 6.50.07.
CVE-2025-13092	The Devs CRM – Manage tasks, attendance and teams all together plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability ch /wp-json/devs-crm/v1/attendances REST API Endpoint in all versions up to, and including, 1.1.8. This makes it possible for unauthenticated attackers to retrieve priv including password hashes.
CVE-2025-12841	The Bookit WordPress plugin before 2.5.1 has a publicly accessible REST endpoint that allows unauthenticated update of the plugins Stripe payment options.
CVE-2025-9207	The TI WooCommerce Wishlist plugin for WordPress is vulnerable to HTML Injection in all versions up to, and including, 2.10.0. This is due to the plugin accepting h and not limiting the values or data that can input and is later output. This makes it possible for unauthenticated attackers to inject arbitrary HTML into wishlist item
CVE-2025-12408	The Events Manager – Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 7.2.2. 'get_location' action due to insufficient restrictions on which locations can be included. This makes it possible for unauthenticated attackers to extract data from pa protected, private, or draft event locations that they should not have access to.
CVE-2025-14065	The Simple Bike Rental plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'simpbire_carica_prenotazioni' A all versions up to, and including, 1.0.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve all booking records c customers' personally identifiable information (PII), including names, email addresses, and phone numbers.
CVE-2025-62181	Pega Platform versions 7.1.0 through Infinity 25.1.0 are affected by a User Enumeration. This issue occurs during user authentication process, where a difference in time could allow a remote unauthenticated user to determine if a username is valid or not. This only applies to deprecated basic-authentication feature and other r authentication mechanisms are recommended. A fix is being provided in the 24.1.4, 24.2.4, and 25.1.1 patch releases. Please note: Basic credentials authenticatio is deprecated started in 24.2 version: https://docs.pega.com/bundle/platform/page/platform/release-notes/security/whats-new-security-242.html.
CVE-2025-11991	The JetFormBuilder — Dynamic Blocks Form Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on th function in all versions up to, and including, 3.5.3. This makes it possible for unauthenticated attackers to generate forms using AI, consuming site's AI usage limits
CVE-2025-14617	A vulnerability has been found in Jehovahs Witnesses JW Library App up to 15.5.1 on Android. Affected is an unknown function of the component org.jw.jwlibrary.mobile.activity.SiloContainer. Such manipulation leads to path traversal. Local access is required to approach this attack. The exploit has been disc public and may be used.
CVE-2025-14442	The Secure Copy Content Protection and Content Locking plugin for WordPress is vulnerable to sensitive information exposure due to storage of exported CSV files accessible directory with predictable filenames in all versions up to, and including, 4.9.2. This makes it possible for unauthenticated attackers to access sensitive u including emails, IP addresses, usernames, roles, and location data by directly accessing the exported CSV file.
CVE-2025-64638	Missing Authorization vulnerability in OnPay.io OnPay.io for WooCommerce onpay-io-for-woocommerce allows Exploiting Incorrectly Configured Access Control Secu Levels.This issue affects OnPay.io for WooCommerce: from n/a through <= 1.0.47.
CVE-2025-14581	The HAPPY – Helpdesk Support Ticket System plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the 'submit_form_rep in all versions up to, and including, 1.0.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to submit replies to arbitrary tickets by manipulating the 'happy_topic_id' parameter, regardless of whether they are the ticket owner or have been assigned to the ticket.
CVE-2025-13403	The Employee Spotlight – Team Member Showcase & Meet the Team Plugin for WordPress is vulnerable to unauthorized tracking settings modification due to missi authorization validation on the employee_spotlight_check_optin() function in all versions up to, and including, 5.1.3. This makes it possible for authenticated attack Subscriber-level access and above, to enable or disable tracking settings.
CVE-2025-14447	The AnnunciFunebri Impresa plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the annfu_reset_options() all versions up to, and including, 4.7.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete all 29 plugin options, e resetting the plugin to its default state.
CVE-2025-64633	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in colabrio Norebro Extra norebro-extra allows Code Injection.This issu Norebro Extra: from n/a through <= 1.6.8.
CVE-2025-14367	The Easy Theme Options plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.0. This is due to missing authorization ch eto_import_settings function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to import arbitrary plugin settings via the 'eto_import_settings' parameter.
CVE-2025-14366	The Eyewear prescription form plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 6.0.1. This is due to missing authoriz on the SubmitCatProductRequest AJAX action. This makes it possible for unauthenticated attackers to create arbitrary WooCommerce products with custom names category assignments via the 'Name', 'Price', and 'Parent' parameters.
CVE-2025-64632	Missing Authorization vulnerability in Auctollo Google XML Sitemaps google-sitemap-generator allows Exploiting Incorrectly Configured Access Control Security Lev affects Google XML Sitemaps: from n/a through <= 4.1.21.
CVE-2025-14170	The Vimeo SimpleGallery plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 0.2. This is due to missing authorization ch `vimeogallery_admin` function hooked to `admin_menu`. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify arb settings via the `action` parameter.
CVE-2025-67897	In Sequoia before 2.1.0, aes_key_unwrap panics if passed a ciphertext that is too short. A remote attacker can take advantage of this issue to crash an application victim an encrypted message with a crafted PKESK or SKESK packet.
CVE-2025-14517	A vulnerability was determined in Yalantis uCrop 2.2.11. This affects the function UCropActivity of the file AndroidManifest.xml. Executing manipulation can lead to export of android application components. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized. The vendor was co about this disclosure but did not respond in any way.
CVE-2025-9122	Hitachi Vantara Pentaho Data Integration and Analytics Community Dashboard Framework prior to versions 10.2.0.4, including 9.3.0.x and 8.3.x display the full ser trace when encountering an error within the GetCdfResource servlet.

CVE-2025-13440	The Premmerce Wishlist for WooCommerce plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.1.10. This is due to a r capability check on the deleteWishlist() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary wis
CVE-2025-13314	The Product Filtering by Categories, Tags, Price Range for WooCommerce – Filter Plus plugin for WordPress is vulnerable to unauthorized modification of data in all to, and including, 1.1.5 due to a missing capability check on the 'filter_save_settings' and 'add_filter_options' AJAX actions. This makes it possible for unauthenticat to modify the plugin's settings and create arbitrary filter options.
CVE-2025-12883	The Campay Woocommerce Payment Gateway plugin for WordPress is vulnerable to Unauthenticated Payment Bypass in all versions up to, and including, 1.2.2. Th the plugin not properly validating that a transaction has occurred through the payment gateway. This makes it possible for unauthenticated attackers to bypass pa mark orders as successfully completed resulting in a loss of income.
CVE-2023-38913	SQL injection vulnerability in anirbandutta9 NEWS-BUZZ v.1.0 allows a remote attacker to execute arbitrary code via a crafted script.
CVE-2023-36338	Inventory Management System 1 was discovered to contain a SQL injection vulnerability.
CVE-2025-14528	A vulnerability was detected in D-Link DIR-803 up to 1.04. Impacted is an unknown function of the file /getcfg.php of the component Configuration Handler. The ma the argument AUTHORIZED_GROUP results in information disclosure. The attack may be performed from remote. The exploit is now public and may be used. This v only affects products that are no longer supported by the maintainer.
CVE-2025-59803	Foxit PDF Editor and Reader before 2025.2.1 allow signature spoofing via triggers. An attacker can embed triggers (e.g., JavaScript) in a PDF document that execut signing process. When a signer reviews the document, the content appears normal. However, once the signature is applied, the triggers modify content on other pa optional content layers without explicit warning. This can cause the signed PDF to differ from what the signer saw, undermining the trustworthiness of the digital si fixed versions are 2025.2.1, 14.0.1, and 13.2.1.
CVE-2025-46294	To enhance security, the FileMaker Server 22.0.4 installer now includes an option to disable IIS short filename enumeration by setting NtfsDisable8dot3NameCreati Windows registry. This prevents attackers from using the tilde character to discover hidden files and directories. This vulnerability has been fully addressed in FileM 22.0.4. The IIS Shortname Vulnerability exploits how Microsoft IIS handles legacy 8.3 short filenames, allowing attackers to infer the existence of files or directories requests with the tilde (~) character.
CVE-2025-13950	The OneSignal – Web Push Notifications plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the settings ha functionality in all versions up to, and including, 3.6.1. This is due to the plugin processing POST requests without verifying user capabilities or nonces. This makes unauthenticated attackers to overwrite the OneSignal App ID, REST API key, and notification behavior via direct POST requests.
CVE-2025-67492	Weblate is a web based localization tool. In versions prior to 5.15, it was possible to trigger repository updates for many repositories via a crafted webhook payloac fixes the issue. As a workaround, disabling webhooks completely using ENABLE_HOOKS avoids this vulnerability.
CVE-2025-14166	The WPMasterToolKit plugin for WordPress is vulnerable to PHP Code Injection in all versions up to, and including, 2.13.0. This is due to the plugin allowing Author-l create and execute arbitrary PHP code through the Code Snippets feature without proper capability checks. This makes it possible for authenticated attackers, with level access and above, to execute arbitrary PHP code on the server, leading to remote code execution, privilege escalation, and complete site compromise.
CVE-2025-11707	The Login Lockdown & Protection plugin for WordPress is vulnerable to IP Block Bypass in all versions up to, and including, 2.14. This is due to $unblock_key key be insufficiently random allowing unauthenticated users, with access to an administrative user email, to generate valid unblock keys for their IP Address. This makes i unauthenticated attackers to bypass blocks due to invalid login attempts.
CVE-2025-65581	An open redirect vulnerability exists in the Account module in Volosoft ABP Framework >= 5.1.0 and < 10.0.0-rc.2. Improper validation of the returnUrl parameter function allows an attacker to redirect users to arbitrary external domains.
CVE-2025-11363	The Royal Addons for Elementor WordPress plugin before 1.7.1037 does not have proper authorisation, allowing unauthenticated users to upload media files via th wpr_addons_upload_file action.
CVE-2025-14703	A vulnerability has been found in Shiguangwu sgwbox N3 2.0.25. The affected element is an unknown function of the file /fsnotify of the component POST Message manipulation of the argument token leads to improper authentication. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-14699	A security vulnerability has been detected in Municorn FAX App 3.27.0 on Android. This vulnerability affects unknown code of the component biz.faxapp.app. Such leads to path traversal. The attack needs to be performed locally. The exploit has been disclosed publicly and may be used. The vendor was contacted early about but did not respond in any way.
CVE-2025-14696	A vulnerability was identified in Shenzhen Sixun Software Sixun Shanghui Group Business Management System 4.10.24.3. Affected by this vulnerability is an unkno functionality of the file /api/GylOperator/UpdatePasswordBatch. The manipulation leads to weak password recovery. The attack may be initiated remotely. The expl available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-67901	openrsync through 0.5.0, as used in OpenBSD through 7.8 and on other platforms, allows a client to cause a server SIGSEGV by specifying a length of zero for bloc because the relationship between p->rem and p->len is not checked.
CVE-2025-67485	mad-proxy is a Python-based HTTP/HTTPS proxy server for detection and blocking of malicious web activity using custom security policies. Versions 0.3 and below attackers to bypass HTTP/HTTPS traffic interception rules, potentially exposing sensitive traffic. This issue does not have a fix at the time of publication.
CVE-2025-13956	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the statistic functio versions up to, and including, 4.3.1. This makes it possible for unauthenticated attackers to view the plugin's orders statistics, including total revenue summaries a status counts
CVE-2025-12655	The Hippoo Mobile App for WooCommerce plugin for WordPress is vulnerable to arbitrary file write via a missing authorization check in all versions up to, and inclu This is due to the REST API endpoint `/wp-json/hippoo/v1/wc/token/save_callback/{token_id}` being registered with `permission_callback => '__return_true'`, whic unauthenticated access. This makes it possible for unauthenticated attackers to write arbitrary JSON content to the server's publicly accessible upload directory via vulnerable endpoint.
CVE-	The Guest Support plugin for WordPress is vulnerable to User Email Disclosure in versions up to, and including, 1.2.3. This is due to the plugin exposing a public AJ

2025-13660	that allows anyone to search for and retrieve user email addresses without any authentication or capability checks. This makes it possible for unauthenticated atta enumerate user accounts and extract email addresses via the guest_support_handler=ajax endpoint with the request=get_users parameter.
CVE-2025-12696	The HelloLeads CRM Form Shortcode WordPress plugin through 1.0 does not have authorisation and CSRF check when resetting its settings, allowing unauthenticat reset them
CVE-2025-66120	Missing Authorization vulnerability in CatFolders CatFolders catfolders allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Cat n/a through <= 2.5.3.
CVE-2025-14074	The PDF for Contact Form 7 + Drag and Drop Template Builder plugin for WordPress is vulnerable to unauthorized post duplication due to a missing capability chec 'rednumber_duplicate' function in all versions up to, and including, 6.3.3. This makes it possible for authenticated attackers, with Subscriber-level access and abov arbitrary posts, including password protected or private ones.
CVE-2025-66129	Missing Authorization vulnerability in wppochipp Pochipp pochipp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Pochipp through <= 1.18.0.
CVE-2025-64702	quic-go is an implementation of the QUIC protocol in Go. Versions 0.56.0 and below are vulnerable to excessive memory allocation through quic-go's HTTP/3 client implementations by sending a QPACK-encoded HEADERS frame that decodes into a large header field section (many unique header names and/or large values). Th implementation builds an http.Header (used on the http.Request and http.Response, respectively), while only enforcing limits on the size of the (QPACK-compresse frame, but not on the decoded header, leading to memory exhaustion. This issue is fixed in version 0.57.0.
CVE-2025-66130	Missing Authorization vulnerability in etruel WP Views Counter wpecounter allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Counter: from n/a through <= 2.1.2.
CVE-2025-14466	A vulnerability in the web interface of the Güralp Fortimus Series, Minimus Series and Certimus Series allows an unauthenticated attacker with network access to s crafted HTTP requests that can cause the web service process to deliberately restart. Although this mechanism limits the impact of the attack, it results in a brief d service condition during the restart.
CVE-2025-55183	An information leak vulnerability exists in specific configurations of React Server Components versions 19.0.0, 19.0.1 19.1.0, 19.1.1, 19.1.2, 19.2.0 and 19.2.1, incl following packages: react-server-dom-parcel, react-server-dom-turbopack, and react-server-dom-webpack. A specifically crafted HTTP request sent to a vulnerable Function may unsafely return the source code of any Server Function. Exploitation requires the existence of a Server Function which explicitly or implicitly exposes argument.
CVE-2025-64012	InvoicePlane commit debb446c is vulnerable to Incorrect Access Control. The invoices/view handler fails to verify ownership before returning invoice data.
CVE-2025-66128	Missing Authorization vulnerability in Brevo Sendinblue for WooCommerce woocommerce-sendinblue-newsletter-subscription allows Exploiting Incorrectly Configur Control Security Levels.This issue affects Sendinblue for WooCommerce: from n/a through <= 4.0.49.
CVE-2025-14569	A vulnerability was detected in ggml-org whisper.cpp up to 1.8.2. Affected is the function read_audio_data of the file /whisper.cpp/examples/common-whisper.cpp. manipulation results in use after free. The attack requires a local approach. The exploit is now public and may be used. The project was informed of the problem ea an issue report but has not responded yet.
CVE-2025-66033	Okta Java Management SDK facilitates interactions with the Okta management API. In versions 21.0.0 through 24.0.0, specific multithreaded implementations may memory issues as threads are not properly cleaned up after requests are completed. Over time, this can degrade performance and availability in long-running appl may result in a denial-of-service condition under sustained load. In addition to using the affected versions, users may be at risk if they are implementing a long-run application using the ApiClient in a multi-threaded manner. This issue is fixed in version 24.0.1.
CVE-2025-13211	IBM Aspera Orchestrator 4.0.0 through 4.1.0 could allow an authenticated user to cause a denial of service in the email service due to improper control of interacti
CVE-2025-9056	Unprotected service in the AudioLink component allows a local attacker to overwrite system files via unauthorized service invocation.
CVE-2025-66125	Insertion of Sensitive Information Into Sent Data vulnerability in Nitesh Ultimate Auction ultimate-auction allows Retrieve Embedded Sensitive Data.This issue affec Auction : from n/a through <= 4.3.2.
CVE-2025-66124	Missing Authorization vulnerability in ZEEN101 Leaky Paywall leaky-paywall allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affec Paywall: from n/a through <= 4.22.5.
CVE-2025-67965	Missing Authorization vulnerability in favethemes Homey Core homey-core allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects from n/a through <= 2.4.3.
CVE-2025-14567	A weakness has been identified in haxxorsid Stock-Management-System up to fbbbf213e9c93b87183a3891f77e3cc7095f22b0. This affects an unknown function of /api/employees. Executing manipulation can lead to missing authentication. It is possible to launch the attack remotely. The exploit has been made available to the could be exploited. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases a available. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supporte maintainer.
CVE-2025-43393	A permissions issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Tahoe 26.1. An app may be able to break out of its sandbox.
CVE-2025-43497	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Tahoe 26.1. An app may be able to break out of its sandbox.

CVE-2025-36938	In U-Boot of append_uint32_le(), there is a possible fault injection due to a logic error in the code. This could lead to physical escalation of privilege with no additior privileges needed. User interaction is not needed for exploitation.
CVE-2025-66407	Weblate is a web based localization tool. The Create Component functionality in Weblate allows authorized users to add new translation components by specifying control system and a source code repository URL to pull from. However, prior to version 5.15, the repository URL field is not validated or sanitized, allowing an atta arbitrary protocols, hostnames, and IP addresses, including localhost, internal network addresses, and local filenames. When the Mercurial version control system i Weblate exposes the full server-side HTTP response for the provided URL. This effectively creates a server-side request forgery (SSRF) primitive that can probe inte and return their contents. In addition to accessing internal HTTP endpoints, the behavior also enables local file enumeration by attempting file:// requests. While file may not always be returned, the application’s error messages clearly differentiate between files that exist and files that do not, revealing information about the ser filesystem layout. In cloud environments, this behavior is particularly dangerous, as internal-only endpoints such as cloud metadata services may be accessible, po leading to credential disclosure and full environment compromise. This has been addressed in the Weblate 5.15 release. As a workaround, remove Mercurial from `VCS_BACKENDS`; the Git backend is not affected. The Git backend was already configured to block the file protocol and does not expose the HTTP response conte message.
CVE-2025-36360	IBM UCD - IBM UrbanCode Deploy 7.1 through 7.1.2.27, 7.2 through 7.2.3.20, and 7.3 through 7.3.2.15 and IBM UCD - IBM DevOps Deploy 8.0 through 8.0.1.10, an 8.1.2.3 is susceptible to a race condition in http-session client-IP binding enforcement which may allow a session to be briefly reused from a new IP address before invalidated, potentially enabling unauthorized access under certain network conditions.
CVE-2025-67640	Jenkins Git client Plugin 6.4.0 and earlier does not not correctly escape the path to the workspace directory as part of an argument in a temporary shell script gene plugin, allowing attackers able to control the workspace directory name to inject arbitrary OS commands.
CVE-2025-67461	External control of file name or path in Zoom Rooms for macOS before version 6.6.0 may allow an authenticated user to conduct a disclosure of information via loc
CVE-2025-14606	A security vulnerability has been detected in tiny-rdm Tiny RDM up to 1.2.5. Affected by this vulnerability is the function pickle.loads of the file pickle_convert.go of component Pickle Decoding. The manipulation leads to deserialization. The attack can be initiated remotely. A high degree of complexity is needed for the attack. T exploitation appears to be difficult. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue repor responded yet.
CVE-2025-14485	A weakness has been identified in EFM ipTIME A3004T 14.19.0. This vulnerability affects the function show_debug_screen of the file /sess-bin/timepro.cgi of the cor Administrator Password Handler. This manipulation of the argument aaksjdkfj with the input !@dnjsrureljrm*& causes command injection. The attack is possible to remotely. The complexity of an attack is rather high. It is stated that the exploitability is difficult. The exploit has been made available to the public and could be ex vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-62329	HCL DevOps Deploy / HCL Launch is susceptible to a race condition in http-session client-IP binding enforcement which may allow a session to be briefly reused fro address before it is invalidated. This could lead to unauthorized access under certain network conditions.
CVE-2025-14477	The 404 Solution plugin for WordPress is vulnerable to SQL Injection in all versions up to, and including, 3.1.0 due to insufficient escaping on the user supplied para lack of sufficient preparation on the existing SQL query. This is due to improper sanitization of the `filterText` parameter in the `ajaxUpdatePaginationLinks` AJAX a sanitization logic can be bypassed by using the sequence `*$/` which becomes `*/` after the `$` character is removed, allowing attackers to escape SQL comment makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can b extract sensitive information from the database via a time-based blind SQL injection technique.
CVE-2025-64251	Missing Authorization vulnerability in azzaroco Ultimate Learning Pro indeed-learning-pro allows Exploiting Incorrectly Configured Access Control Security Levels.Th affects Ultimate Learning Pro: from n/a through <= 3.9.3.
CVE-2025-13677	The Simple Download Counter plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 2.2.2. This is due to insufficient path validati `simple_download_counter_parse_path()` function. This makes it possible for authenticated attackers, with Administrator-level access and above, to read the conte arbitrary files on the server, which may contain sensitive information such as database credentials (wp-config.php) or system files. Please note that the vendor opt to allow remote file downloads from arbitrary locations on the server, however, has disabled this functionality on multi-sites and provided a warning to site owners readme.txt when they install the plugin. While not an optimal patch, we have considered this sufficient and recommend users proceed to use the plugin with cautio
CVE-2025-13972	The WatchTowerHQ plugin for WordPress is vulnerable to arbitrary file read via the 'wht_download_big_object_origin' parameter in all versions up to, and including, is due to insufficient path validation in the handle_big_object_download_request function. This makes it possible for authenticated attackers, with administrator-lev a valid access token, to read arbitrary files on the server, which can contain sensitive information such as database credentials and authentication keys.
CVE-2025-67819	An issue was discovered in Weaviate OSS before 1.33.4. Due to a lack of validation of the fileName field in the transfer logic, an attacker who can call the GetFile m shard is in the "Pause file activity" state and the FileReplicationService is reachable can read arbitrary files accessible to the service process.
CVE-2025-14050	The Design Import/Export plugin for WordPress is vulnerable to SQL Injection via XML File Import in all versions up to, and including, 2.2 due to insufficient escaping supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2025-64872	Adobe Experience Manager versions 6.5.23 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high privileged at inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulner
CVE-2025-14530	A vulnerability has been found in SourceCodester Real Estate Property Listing App 1.0. The impacted element is an unknown function of the file /admin/property.ph 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
CVE-2025-67809	An issue was discovered in Zimbra Collaboration (ZCS) 10.0 and 10.1. A hardcoded Flickr API key and secret are present in the publicly accessible Flickr Zimlet use Collaboration. Because these credentials are embedded directly in the Zimlet, any unauthorized party could retrieve them and misuse the Flickr integration. An att access to the exposed credentials could impersonate the legitimate application and initiate valid Flickr OAuth flows. If a user is tricked into approving such a reque attacker could gain access to the user s Flickr data. The hardcoded credentials have since been removed from the Zimlet code, and the associated key has been re
CVE-2025-14694	A vulnerability was found in ketr JEPaaS up to 7.2.8. This impacts the function readAllPostil of the file /je/postil/postil/readAllPostil. Performing manipulation of the a keyWord results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about t but did not respond in any way.
CVE-2025-	A security vulnerability has been detected in DedeBIZ up to 6.5.9. Affected by this vulnerability is an unknown functionality of the file /src/admin/catalog_add.php. manipulation leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.

14648	
CVE-2025-14451	The Solutions Ad Manager plugin for WordPress is vulnerable to Open Redirect in all versions up to, and including, 1.0.0. This is due to insufficient validation on the supplied via the 'sam-redirect-to' parameter. This makes it possible for unauthenticated attackers to redirect users to potentially malicious sites if they can success them into performing an action.
CVE-2025-14582	A vulnerability was detected in campcodes Online Student Enrollment System 1.0. This affects an unknown function of the file /admin/index.php?page=user-profile manipulation of the argument userphoto results in unrestricted upload. The attack can be initiated remotely. The exploit is now public and may be used.
CVE-2025-14641	A flaw has been found in code-projects Computer Laboratory System 1.0. This issue affects some unknown processing of the file admin/admin_pic.php. This manipu argument image causes unrestricted upload. The attack may be initiated remotely. The exploit has been published and may be used.
CVE-2025-14642	A vulnerability has been found in code-projects Computer Laboratory System 1.0. Impacted is an unknown function of the file technical_staff_pic.php. Such manipu argument image leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-14730	A security flaw has been discovered in CTCMS Content Management System up to 2.1.2. The impacted element is an unknown function in the library /ctcms/libs/Ct_ the component Backend System Configuration Module. The manipulation of the argument Cj_Add/Cj_Edit results in code injection. The attack can be executed rem exploit has been released to the public and may be exploited.
CVE-2025-14729	A vulnerability was identified in CTCMS Content Management System up to 2.1.2. The affected element is the function Save of the file /ctcms/libs/Ct_App.php of the Backend App Configuration Module. The manipulation of the argument CT_App_Paytype leads to code injection. Remote exploitation of the attack is possible. The e publicly available and might be used.
CVE-2023-53898	Rukovoditel 3.4.1 contains a stored cross-site scripting vulnerabilities that allow authenticated attackers to inject malicious scripts. Attackers can insert iframe and payloads in application copyright text to execute arbitrary JavaScript in victim browsers.
CVE-2023-53897	Rukovoditel 3.4.1 contains multiple stored cross-site scripting vulnerabilities that allow authenticated attackers to inject malicious scripts. Attackers can insert XSS project task comments to execute arbitrary JavaScript in victim browsers.
CVE-2025-67741	In JetBrains TeamCity before 2025.11 stored XSS was possible via session attribute
CVE-2025-67341	jshERP versions 3.5 and earlier are affected by a stored XSS vulnerability. This vulnerability allows attackers to upload PDF files containing XSS payloads. Additiona files can be accessed via static URLs, making them accessible to all users.
CVE-2025-65825	The firmware on the basestation of the Meatmeet is not encrypted. An adversary with physical access to the Meatmeet device can disassemble the device, connec and retrieve the firmware dump for analysis. Within the NVS partition they may discover the credentials of the current and previous Wi-Fi networks. This informatio used to gain unauthorized access to the victim's Wi-Fi network.
CVE-2025-67342	RuoYi versions 4.8.1 and earlier is affected by a stored XSS vulnerability in the /system/menu/edit endpoint. While the endpoint is protected by an XSS filter, the pr be bypassed. Additionally, because the menu is shared across all users, any user with menu modification permissions can impact all users by exploiting this stored vulnerability.
CVE-2025-65832	The mobile application insecurely handles information stored within memory. By performing a memory dump on the application after a user has logged out and ter Wi-Fi credentials sent during the pairing process, JWTs used for authentication, and other sensitive details can be retrieved. As a result, an attacker with physical a device of a victim can retrieve this information and gain unauthorized access to their home Wi-Fi network and Meatmeet account.
CVE-2025-67344	jshERP v3.5 and earlier is affected by a stored Cross Site Scripting (XSS) vulnerability via the /msg/add endpoint.
CVE-2025-67898	MJML through 4.18.0 allows mj-include directory traversal to test file existence and (in the type="css" case) read files. NOTE: this issue exists because of an incomp CVE-2020-12827.
CVE-2025-13971	The TWW Protein Calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Header' setting in all versions up to, and including, 1.0.24 due input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages t execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.
CVE-2025-13975	The Contact Form 7 with ChatWork plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'api_token' and 'roomid' settings in all versions up to, a 1.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitra in pages that will execute whenever a user accesses the settings page. This only affects multi-site installations and installations where unfiltered_html has been dis
CVE-2025-11970	The Emplibot – AI Content Writer with Keyword Research, Infographics, and Linking | SEO Optimized | Fully Automated plugin for WordPress is vulnerable to Server- Forgery in all versions up to, and including, 1.0.9 via the emplibot_call_webhook_with_error() and emplibot_process_zip_data() functions. This makes it possible for attackers, with Administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query a information from internal services.
CVE-2025-14702	A flaw has been found in Smartbit CommV Smartschool App up to 10.4.4. Impacted is an unknown function of the component be.smartschool.mobile.SplashActivity manipulation can lead to path traversal. The attack requires local access. The exploit has been published and may be used. The vendor was contacted early about but did not respond in any way.
CVE-2025-14056	The Custom Post Type UI plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'label' parameter during custom post type import in all versions u including, 1.18.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access, to in web scripts in pages that will execute whenever a user accesses the Tools → Get Code page.
CVE-2025-67634	The CISA Software Acquisition Guide Supplier Response Web Tool before 2025-12-11 was vulnerable to cross-site scripting via text fields. If an attacker could convi import a specially-crafted JSON file, the Tool would load JavaScript from the file into the page. The JavaScript would execute in the context of the user's browser wh submits the page (clicks 'Next').
CVE-	The Quick Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.1 due to insufficie

2025-14378	sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.
CVE-2025-14698	A weakness has been identified in atlaszz AI Photo Team Galleryit App 1.3.8.2 on Android. This affects an unknown part of the component gallery.photogallery.pictures.vault.album. This manipulation causes path traversal. The attack needs to be launched locally. The exploit has been made available to and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-14467	The WP Job Portal plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 2.3.9. This is due to the plugin explicitly whit `<script>` tag in its `WPJOBPORTAL_ALLOWED_TAGS` configuration and using insufficient input sanitization when saving job descriptions. This makes it possible fo authenticated attackers, with Editor-level access and above, to inject arbitrary web scripts into job description fields via the job creation/editing interface. These sc execute whenever a user accesses an injected page, enabling session hijacking, credential theft, and other malicious activities.This only impacts multi-site installat with unfiltered_html disabled.
CVE-2025-14048	The SimplyConvert plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'simplyconvert_hash' option in all versions up to, and including, 1.0 due input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages t execute whenever a user accesses an injected page.
CVE-2025-14035	The DebateMaster plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the color options in the plugin settings in all versions up to, and including, 1 insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary in pages that will execute whenever a user accesses a page with the debate shortcode. This only affects multi-site installations and installations where unfiltered_h disabled.
CVE-2025-67715	Weblate is a web based localization tool. In versions prior to 5.15, it was possible to retrieve user notification settings or list all users via API. Version 5.15 fixes the
CVE-2025-14062	The Animated Pixel Marquee Creator plugin for WordPress is vulnerable to Cross-Site Request Forgery via the 'marquee' parameter in all versions up to, and includi is due to missing nonce validation on the marquee deletion function. This makes it possible for unauthenticated attackers to delete arbitrary marquees via a forgec granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-14356	The Ultra Addons for Contact Form 7 plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'uacf7_get_generat function in all versions up to, and including, 3.5.33. This makes it possible for authenticated attackers, with Subscriber-level access and above, to generate and get submission PDF, when the "PDF Generator" and the "Database" addons are enabled (disabled by default).
CVE-2025-11247	GitLab has remediated an issue in GitLab EE affecting all versions from 13.2 before 18.4.6, 18.5 before 18.5.4, and 18.6 before 18.6.2 that could have allowed an a user to disclose sensitive information from private projects by executing specifically crafted GraphQL queries.
CVE-2025-14521	A security vulnerability has been detected in baowzh hfly up to 638ff9abe9078bc977c132b37acbe1900b63491c. The affected element is an unknown function of th /admin/index.php/datafile/download. Such manipulation of the argument filename leads to path traversal. The attack may be performed from remote. The exploit h disclosed publicly and may be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated disclosed. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-14045	The URL Media Uploader plugin for WordPress is vulnerable to unauthorized safe file uploads due to a missing capability check on the url_media_uploader_url_upload_ajax_handler() function in all versions up to, and including, 1.0.1. This makes it possible for authenticated attackers, with Contribute and above, to upload safe media files.
CVE-2025-13125	Authorization Bypass Through User-Controlled Key vulnerability in Im Park Information Technology, Electronics, Press, Publishing and Advertising, Education Ltd. Co allows Exploitation of Trusted Identifiers.This issue affects DijiDemi: through 28.11.2025.
CVE-2025-14158	The Coding Blocks plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.0. This is due to missing nonce validatio settings update functionality. This makes it possible for unauthenticated attackers to update plugin settings including the theme configuration via a forged request can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-14160	The Upcoming for Calendly plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.4. This is due to missing nonce the settings update functionality. This makes it possible for unauthenticated attackers to update the plugin's Calendly API key via a forged request granted they ca administrator into performing an action such as clicking on a link.
CVE-2025-14161	The Truefy Embed plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.0. This is due to missing nonce validatio 'truefy_embed_options_update' settings update action. This makes it possible for unauthenticated attackers to update the plugin's settings, including the API key, v request granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-14162	The BMLT WordPress Plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.11.4. This is due to missing nonce valid 'BMLTPlugin_create_option' and 'BMLTPlugin_delete_option ' action. This makes it possible for unauthenticated attackers to create new plugin settings via a forged granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-14165	The Kirim.Email WooCommerce Integration plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.9. This is due to nonce validation on the plugin's settings page. This makes it possible for unauthenticated attackers to modify the plugin's API credentials and integration settings v request granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-14746	A vulnerability has been found in Ningyuanda TC155 57.0.2.0. The affected element is an unknown function of the component RTSP Live Video Stream Endpoint. Su manipulation leads to improper authentication. The attack must be carried out from within the local network. The exploit has been disclosed to the public and may vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-14691	A vulnerability was detected in Mayan EDMS up to 4.10.1. The affected element is an unknown function of the file /authentication/. The manipulation results in cros scripting. The attack may be performed from remote. The exploit is now public and may be used. Upgrading to version 4.10.2 is sufficient to fix this issue. You shou the affected component. The vendor confirms that this is "[f]ixed in version 4.10.2". Furthermore, that "[b]ackports for older versions in process and will be out as s respective CI pipelines complete."
CVE-2025-14021	The in-app browser in LINE client for iOS versions prior to 14.14 is vulnerable to address bar spoofing, which could allow attackers to execute malicious JavaScript v while displaying trusted URLs, enabling phishing attacks through overlaid malicious content.
CVE-2025-13978	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.5 before 18.4.6, 18.5 before 18.5.4, and 18.6 before 18.6.2 that could have allowed a authenticated user to discover the names of private projects they do not have access through API requests.

CVE-2025-14531	A vulnerability was found in code-projects Rental Management System 2.0. This affects an unknown function of the file Transaction.java of the component Log Han Performing manipulation results in crlf injection. The attack can be initiated remotely. The exploit has been made public and could be used.
CVE-2025-14354	The Resource Library for Logged In Users plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4. This is due to mi validation on multiple administrative functions. This makes it possible for unauthenticated attackers to perform various unauthorized actions including creating, ed deleting resources and categories via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-14391	The Simple Theme Changer plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0. This is due to missing or incorrec validation. This makes it possible for unauthenticated attackers to update the plugin's settings via a forged request granted they can trick a site administrator into action such as clicking on a link.
CVE-2025-14392	The Simple Theme Changer plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the user_theme_admin, display_method_admin, and set_change_theme_button_name actions actions in all versions up to, and including, 1.0. This makes it possible for authenticated attac subscriber-level access and above, to modify the plugin's settings.
CVE-2025-46266	A vulnerability in TeamViewer DEX Client (former 1E Client) - Content Distribution Service (NomadBranch.exe) prior version 25.11 for Windows allows malicious act the service into transmitting data to an arbitrary internal IP address, potentially leaking sensitive information.
CVE-2025-13987	The Purchase and Expense Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.2. This is due to missi validation on the 'sup_pt_handle_deletion' function. This makes it possible for unauthenticated attackers to delete arbitrary purchase records via a forged request g can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-13741	The Schedule Post Changes With PublishPress Future: Unpublish, Delete, Change Status, Trash, Change Categories plugin for WordPress is vulnerable to unauthoriz data due to a missing capability check on the getAuthors function in all versions up to, and including, 4.9.2. This makes it possible for authenticated attackers, with level access and above, to retrieve emails for all users with edit_posts capability.
CVE-2025-67948	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in SendPulse SendPulse Email Marketing Newsletter sendpulse-email-ma newsletter allows Retrieve Embedded Sensitive Data.This issue affects SendPulse Email Marketing Newsletter: from n/a through <= 2.2.1.
CVE-2025-14003	The Image Gallery – Photo Grid & Video Gallery plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `add_images_to_gallery_callback()` function in all versions up to, and including, 2.13.3. This makes it possible for authenticated attackers, with Author-level access to add images to arbitrary Modula galleries owned by other users.
CVE-2025-64011	Nextcloud Server 30.0.0 is vulnerable to an Insecure Direct Object Reference (IDOR) in the /core/preview endpoint. Any authenticated user can access previews of belonging to other users by manipulating the fileId parameter. This allows unauthorized disclosure of sensitive data, such as text files or images, without prior shar permissions.
CVE-2025-14747	A vulnerability was found in Ningyuanda TC155 57.0.2.0. The impacted element is an unknown function of the component RTSP Service. Performing manipulation r denial of service. The attack must originate from the local network. The exploit has been made public and could be used. The vendor was contacted early about thi but did not respond in any way.
CVE-2025-14692	A flaw has been found in Mayan EDMS up to 4.10.1. The impacted element is an unknown function of the file /authentication/. This manipulation causes open redire possible to initiate the attack remotely. The exploit has been published and may be used. Upgrading to version 4.10.2 is sufficient to resolve this issue. The affecte should be upgraded. The vendor confirms that this is "[f]ixed in version 4.10.2". Furthermore, that "[b]ackports for older versions in process and will be out as soon respective CI pipelines complete."
CVE-2025-10684	The Construction Light WordPress theme before 1.6.8 does not have authorisation and CSRF when activating via an AJAX action, allowing any authenticated users, subscriber to activate arbitrary .
CVE-2025-66436	An SSTI (Server-Side Template Injection) vulnerability exists in the get_terms_and_conditions method of Frappe ERPNext through 15.89.0. The function renders atta controlled Jinja2 templates (terms) using frappe.render_template() with a user-supplied context (doc). Although Frappe uses a custom SandboxedEnvironment, sev dangerous globals such as frappe.db.sql are still available in the execution context via get_safe_globals(). An authenticated attacker with access to create or modif Conditions document can inject arbitrary Jinja expressions into the terms field, resulting in server-side code execution within a restricted but still unsafe context. Th vulnerability can be used to leak database information.
CVE-2025-14373	Inappropriate implementation in Toolbar in Google Chrome on Android prior to 143.0.7499.110 allowed a remote attacker to perform domain spoofing via a crafted (Chromium security severity: Medium)
CVE-2025-67638	Jenkins 2.540 and earlier, LTS 2.528.2 and earlier does not mask build authorization tokens displayed on the job configuration form, increasing the potential for att observe and capture them.
CVE-2025-64238	Missing Authorization vulnerability in NicolasKulka WPS Bidouille wps-bidouille allows Exploiting Incorrectly Configured Access Control Security Levels.This issue aff Bidouille: from n/a through <= 1.33.1.
CVE-2025-64239	Cross-Site Request Forgery (CSRF) vulnerability in Yoav Farhi RTL Tester rtl-tester allows Cross Site Request Forgery.This issue affects RTL Tester: from n/a through
CVE-2025-64240	Cross-Site Request Forgery (CSRF) vulnerability in freshchat Freshchat freshchat allows Cross Site Request Forgery.This issue affects Freshchat: from n/a through <
CVE-2025-64242	Missing Authorization vulnerability in Merv Barrett Easy Property Listings easy-property-listings allows Exploiting Incorrectly Configured Access Control Security Lev affects Easy Property Listings: from n/a through <= 3.5.15.
CVE-2025-64243	Missing Authorization vulnerability in e-plugins Directory Pro directory-pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects from n/a through <= 2.5.6.
CVE-	Missing Authorization vulnerability in Codexpert, Inc Restrict Elementor Widgets, Columns and Sections restrict-elementor-widgets allows Exploiting Incorrectly Cor

2025-64244	Access Control Security Levels.This issue affects Restrict Elementor Widgets, Columns and Sections: from n/a through <= 1.12.
CVE-2025-64245	Missing Authorization vulnerability in ryanpcmcquen Import external attachments import-external-attachments allows Exploiting Incorrectly Configured Access Con Levels.This issue affects Import external attachments: from n/a through <= 1.5.12.
CVE-2025-64246	Missing Authorization vulnerability in netopsae Accessibility by AudioEye accessibility-by-audioeye allows Exploiting Incorrectly Configured Access Control Security issue affects Accessibility by AudioEye: from n/a through <= 1.0.49.
CVE-2025-67636	A missing permission check in Jenkins 2.540 and earlier, LTS 2.528.2 and earlier allows attackers with View/Read permission to view encrypted password values in
CVE-2025-14159	The Secure Copy Content Protection and Content Locking plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.9.2 to missing nonce validation on the 'ays_sccp_results_export_file' AJAX action. This makes it possible for unauthenticated attackers to export sensitive plugin data in addresses, IP addresses, physical addresses, user IDs, and other user information via a forged request granted they can trick a site administrator into performing a as clicking on a link. The exported data is stored in a publicly accessible file, allowing attackers to receive the sensitive information even though they are not authe
CVE-2025-12783	The Premmerce Brands for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the saveBr function in all versions up to, and including, 1.2.13. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify brand per settings.
CVE-2025-67637	Jenkins 2.540 and earlier, LTS 2.528.2 and earlier stores build authorization tokens unencrypted in job config.xml files on the Jenkins controller where they can be v users with Item/Extended Read permission or access to the Jenkins controller file system.
CVE-2025-14540	The Userback plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the userback_get_json function in all versions including, 1.0.15. This makes it possible for authenticated attackers, with Subscriber-level access and above, to extract plugin's configuration data including the Us access token and site's posts/pages contents, including those that have private and draft status.
CVE-2025-59009	Cross-Site Request Forgery (CSRF) vulnerability in Astoundify Listify listify allows Cross Site Request Forgery.This issue affects Listify: from n/a through <= 3.2.5.
CVE-2025-67642	Jenkins HashiCorp Vault Plugin 371.v884a_4dd60fb_6 and earlier does not set the appropriate context for Vault credentials lookup, allowing attackers with Item/Co permission to access and potentially capture Vault credentials they are not entitled to.
CVE-2025-13363	The IMAQ Core plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.1. This is due to missing nonce validation o structure settings update functionality. This makes it possible for unauthenticated attackers to update the plugin's URL structure settings via a forged request gran trick a site administrator into performing an action such as clicking on a link.
CVE-2025-13366	The Rabbit Hole plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1. This is due to missing or incorrect nonce v the plugin's reset functionality. This makes it possible for unauthenticated attackers to reset the plugin's settings via a forged request granted they can trick a site into performing an action such as clicking on a link. The vulnerability is exacerbated by the fact that the reset operation is performed via a GET request, making ex trivial via image tags or hyperlinks.
CVE-2025-14462	The Lucky Draw Contests plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.2. This is due to missing or incorre validation in misc-settings.php. This makes it possible for unauthenticated attackers to update plugin settings via a forged request granted they can trick a site adr into performing an action such as clicking on a link.
CVE-2025-14454	The Image Slider by Ays- Responsive Slider and Carousel plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.7.0 to missing or incorrect nonce validation on the bulk delete functionality. This makes it possible for unauthenticated attackers to delete arbitrary sliders via a forged granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-13408	The Foxtool All-in-One: Contact chat button, Custom login, Media optimize images plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions u including, 2.5.2. This is due to missing or incorrect nonce validation on the foxtool_login_google() function. This makes it possible for unauthenticated attackers to OAuth Connection via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-14395	The Popover Windows plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on multiple ajax actions (e.g., pop_ poptheme_submit) in all versions up to, and including, 1.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to modify th settings and content.
CVE-2025-14394	The Popover Windows plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2. This is due to missing or incorrect non This makes it possible for unauthenticated attackers to update the plugin's settings via a forged request granted they can trick a site administrator into performing such as clicking on a link.
CVE-2025-14288	The Gallery Blocks with Lightbox. Image Gallery, (HTML5 video , YouTube, Vimeo) Video Gallery and Lightbox for native gallery plugin for WordPress is vulnerable t unauthorized modification of plugin settings in all versions up to, and including, 3.3.0. This is due to the plugin using the `edit_posts` capability check instead of `manage_options` for the `update_option` action type in the `pgc_sgb_action_wizard` AJAX handler. This makes it possible for authenticated attackers, with Contri access and above, to modify arbitrary plugin settings prefixed with `pgc_sgb_*`.
CVE-2025-67643	Jenkins Redpen - Pipeline Reporter for Jira Plugin 1.054.v7b_9517b_6b_202 and earlier does not correctly perform path validation of the workspace directory while u artifacts to Jira, allowing attackers with Item/Configure permission to retrieve files present on the Jenkins controller workspace directory.
CVE-2025-12512	The GenerateBlocks plugin for WordPress is vulnerable to information exposure due to missing object-level authorization checks in versions up to, and including, 2. due to the plugin registering multiple REST API routes under `generateblocks/v1/meta/` that gate access with `current_user_can('edit_posts')`, which is granted to roles such as Contributor. The handlers accept arbitrary entity IDs (user IDs, post IDs, etc.) and meta keys, returning any requested metadata with only a short bla password-like keys for protection. There is no object-level authorization ensuring the caller is requesting only their own data, and there is no allowlist of safe keys. possible for authenticated attackers, with Contributor-level access and above, to exfiltrate personally identifiable information (PII) and other sensitive profile data o administrator accounts or any other users by directly querying user meta keys via the exposed endpoints via the `get_user_meta_rest` function. In typical WordPre WooCommerce setups, this includes names, email, phone, and address fields that WooCommerce stores in user meta, enabling targeted phishing, account takeove and privacy breaches.
CVE-	The Mavix Education theme for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'mavix_education_activate_p

2025-11164	action in all versions up to, and including, 1.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to activate the Creativ D plugin.
CVE-2025-64237	Cross-Site Request Forgery (CSRF) vulnerability in Graham Quick Interest Slider quick-interest-slider allows Cross Site Request Forgery.This issue affects Quick Inte from n/a through <= 3.1.5.
CVE-2025-64898	ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Insufficiently Protected Credentials vulnerability that could result in limited unauthoriz access. An attacker could leverage this vulnerability to gain unauthorized access by exploiting improperly stored or transmitted credentials. Exploitation of this issu require user interaction.
CVE-2025-66435	An SSTI (Server-Side Template Injection) vulnerability exists in the get_contract_template method of Frappe ERPNext through 15.89.0. The function renders attacke Jinja2 templates (contract_terms) using frappe.render_template() with a user-supplied context (doc). Although Frappe uses a custom SandboxedEnvironment, seve globals such as frappe.db.sql are still available in the execution context via get_safe_globals(). An authenticated attacker with access to create or modify a Contrac can inject arbitrary Jinja expressions into the contract_terms field, resulting in server-side code execution within a restricted but still unsafe context. This vulnerabil used to leak database information.
CVE-2025-12407	The Events Manager – Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, due to missing or incorrect nonce validation on the 'location_delete' action. This makes it possible for unauthenticated attackers to delete locations via a forged rec they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-59001	Missing Authorization vulnerability in ThemeNectar Salient Core salient-core allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affec Core: from n/a through <= 3.0.8.
CVE-2025-13794	The Auto Featured Image (Auto Post Thumbnail) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the bulk_action_generate_handler function in all versions up to, and including, 4.2.1. This makes it possible for authenticated attackers, with Contributor-level access a delete or generate featured images on posts they do not own.
CVE-2025-12900	The FileBird – WordPress Media Library Folders & File Manager plugin for WordPress is vulnerable to missing authorization in all versions up to, and including, 6.5.1 "ConvertController::insertToNewTable" function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with author l and above, to inject global folders and reassign arbitrary media attachments to those folders under certain circumstances.
CVE-2025-54005	Missing Authorization vulnerability in sonalsinha21 SKT Page Builder skt-builder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue a Page Builder: from n/a through <= 4.9.
CVE-2025-58999	Cross-Site Request Forgery (CSRF) vulnerability in loopus WP Attractive Donations System - Easy Stripe & Paypal donations WP_AttractiveDonationsSystem allows C Request Forgery.This issue affects WP Attractive Donations System - Easy Stripe & Paypal donations: from n/a through <= 1.25.
CVE-2025-54045	Missing Authorization vulnerability in CreativeMindsSolutions CM On Demand Search And Replace cm-on-demand-search-and-replace allows Exploiting Incorrectly C Access Control Security Levels.This issue affects CM On Demand Search And Replace: from n/a through <= 1.5.4.
CVE-2025-67780	SpaceX Starlink Dish devices with firmware 2024.12.04.mr46620 (e.g., on Mini1_prod2) allow administrative actions via unauthenticated LAN gRPC requests, aka M The cross-origin policy can be bypassed by omitting a Referer header. In some cases, an attacker's ability to read tilt, rotation, and elevation data via gRPC can ma infer the geographical location of the dish.
CVE-2025-67742	In JetBrains TeamCity before 2025.11 path traversal was possible via file upload
CVE-2025-14651	A vulnerability has been found in MartialBE one-hub up to 0.14.27. This vulnerability affects unknown code of the file docker-compose.yml. The manipulation of the SESSION_SECRET leads to use of hard-coded cryptographic key . The attack may be initiated remotely. The complexity of an attack is rather high. It is stated that t exploitability is difficult. The exploit has been disclosed to the public and may be used. It is recommended to change the configuration settings. The code maintain recommends (translated from Chinese): "The default docker-compose example file is not recommended for production use. If you intend to use it in production, ple check and modify every configuration and environment variable yourself!"
CVE-2025-14697	A security flaw has been discovered in Shenzhen Sixun Software Sixun Shanghui Group Business Management System 4.10.24.3. Affected by this issue is some unk functionality of the file /ExportFiles/. The manipulation results in files or directories accessible. The attack may be launched remotely. This attack is characterized b complexity. The exploitation is known to be difficult. The exploit has been released to the public and may be exploited. The vendor was contacted early about this did not respond in any way.
CVE-2025-14636	A security flaw has been discovered in Tenda AX9 22.03.01.46. This affects the function image_check of the component httpd. The manipulation results in use of w possible to launch the attack remotely. A high complexity level is associated with this attack. It is indicated that the exploitability is difficult. The exploit has been r public and may be exploited.
CVE-2025-9218	The rtMedia for WordPress, BuddyPress and bbPress plugin for WordPress is vulnerable to to Information Disclosure due to missing authorization in the handle_rest_pre_dispatch() function when the Godam plugin is active, in versions 4.7.0 to 4.7.3. This makes it possible for unauthenticated attackers to retrieve me associated with draft or private posts.
CVE-2025-67500	Mastodon is a free, open-source social network server based on ActivityPub. Versions 4.2.27 and prior, 4.3.0-beta.1 through 4.3.14, 4.4.0-beta.1 through 4.4.9, 4.5. through 4.5.2 have discrepancies in error handling which allow checking whether a given status exists by sending a request with a non-English Accept-Language h this behavior, an attacker who knows the identifier of a particular status they are not allowed to see can confirm whether this status exists or not. This cannot be u the contents of the status or any other property besides its existence. This issue is fixed in versions 4.2.28, 4.3.15, 4.4.10 and 4.5.3.
CVE-2025-12734	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.6 before 18.4.6, 18.5 before 18.5.4, and 18.6 before 18.6.2 that could have allowed a authenticated user to, under certain conditions, render content in dialogs to other users by injecting malicious HTML content into merge request titles.
CVE-2025-67639	A cross-site request forgery (CSRF) vulnerability in Jenkins 2.540 and earlier, LTS 2.528.2 and earlier allows attackers to trick users into logging in to the attacker's
CVE-2025-	TableProgressTracking is a MediaWiki extension to track progress against specific criterion. Versions 1.2.0 and below do not enforce CSRF token validation in the R result, an attacker could craft a malicious webpage that, when visited by an authenticated user on a wiki with the extension enabled, would trigger unintended aut actions through the victim's browser. Due to the lack of token validation, an attacker can delete or track progress against tables. This issue is patched in version 1.

67646	extension.
CVE-2025-14519	A security flaw has been discovered in baowzh hfly up to 638ff9abe9078bc977c132b37acbe1900b63491c. This issue affects some unknown processing of the file /admin/index.php/advtext/add of the component advtext Module. The manipulation results in cross site scripting. The attack can be executed remotely. The exploit released to the public and may be exploited. This product implements a rolling release for ongoing delivery, which means version information for affected or updat unavailable. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-10583	The WP Fastest Cache plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.7.4 via the 'get_server_time_ajax_re action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to make web requests to arbitrary locations originating from the application and can be used to query and modify information from internal services.
CVE-2025-14538	A security vulnerability has been detected in yangshare warehouseManager 仓库管理系统 1.1.0. This affects the function addCustomer of the file CustomerManageH Such manipulation of the argument Name leads to cross site scripting. The attack can be executed remotely. The exploit has been disclosed publicly and may be u
CVE-2025-68163	In JetBrains TeamCity before 2025.11 stored XSS was possible on agentpushInstall page
CVE-2025-14580	A security vulnerability has been detected in Qualitor up to 8.24.73. The impacted element is an unknown function of the file /Qualitor/html/bc/bcdocumento9/biblioteca/request/viewDocumento.php. Such manipulation of the argument cdscript leads to cross site scripting. It is possible to l attack remotely. The exploit has been disclosed publicly and may be used. It is suggested to upgrade the affected component. The vendor confirms the existence "We became aware of the issue through an earlier direct notification from the original reporter, and our engineering team promptly investigated and implemented corrective measures. (...) Updated versions containing the fix have already been provided to our customer base".
CVE-2025-13127	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in TAC Information Services Internal and External Trade In allows Cross-Site Scripting (XSS).This issue affects GoldenHorn: before 4.25.1121.1.
CVE-2025-14019	LINE client for Android versions from 13.8 to 15.5 is vulnerable to UI spoofing in the in-app browser where a specific layout could obscure the full-screen warning pr potentially allowing attackers to conduct phishing attacks.
CVE-2025-43517	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. An app ma access protected user data.
CVE-2025-43522	A downgrade issue affecting Intel-based Mac computers was addressed with additional code-signing restrictions. This issue is fixed in macOS Sequoia 15.7.3. An ap able to access user-sensitive data.
CVE-2025-43518	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. An app may be able to inappropriately acc through the spellcheck API.
CVE-2025-43465	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Tahoe 26.1. An app may be able to ac user data.
CVE-2025-43516	A session management issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. A user with Voice Control e be able to transcribe another user's activity.
CVE-2025-43404	A permissions issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Tahoe 26.1. An app may be able to access sensitive user data
CVE-2025-55307	An issue was discovered in Foxit PDF and Editor for Windows before 13.2 and 2025 before 2025.2. Opening a malicious PDF containing a crafted JavaScript call to s with a crafted cDIPath parameter (e.g., "/") may cause an out-of-bounds read in internal path-parsing logic, potentially leading to information disclosure or memory
CVE-2025-43437	An information disclosure issue was addressed with improved privacy controls. This issue is fixed in iOS 26.1 and iPadOS 26.1. An app may be able to fingerprint th
CVE-2023-29144	Malwarebytes 1.0.14 for Linux doesn't properly compute signatures in some scenarios. This allows a bypass of detection.
CVE-2025-14023	LINE client for iOS prior to 15.19 allows UI spoofing due to inconsistencies between the navigation state and the in-app browser's user interface, which could create about the trust context of displayed pages or interactive elements under specific conditions.
CVE-2025-67739	In JetBrains TeamCity before 2025.11.2 improper repository URL validation could lead to local paths disclosure
CVE-2025-67737	AzuraCast is a self-hosted, all-in-one web radio management suite. Versions 0.23.1 mistakenly include an API endpoint that is intended for internal use by the SFTP sftpgo, exposing it to the public-facing HTTP API for AzuraCast installations. A user with specific internal knowledge of a station's operations can craft a custom HTT would affect the contents of a station's database, without revealing any internal information about the station. In order to carry out an attack, a malicious user wou know a valid SFTP station username and the coordinating internal filesystem structure. This issue is fixed in version 0.23.2.
CVE-2025-67899	uriparser through 0.9.9 allows unbounded recursion and stack consumption, as demonstrated by ParseMustBeSegmentNzNc with large input containing many com
CVE-	A memory corruption issue was addressed with improved bounds checking. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. Processing malicio

2025-43532	lead to unexpected app termination.
CVE-2025-67740	In JetBrains TeamCity before 2025.11 improper access control could expose GitHub App token's metadata
CVE-2025-68162	In JetBrains TeamCity before 2025.11 maven embedder allowed loading extensions via project configuration
CVE-2025-68164	In JetBrains TeamCity before 2025.11 port enumeration was possible via the Perforce connection test
CVE-2025-14082	A flaw was found in Keycloak Admin REST (Representational State Transfer) API. This vulnerability allows information disclosure of sensitive role metadata via insuf authorization checks on the /admin/realms/{realm}/roles endpoint.
CVE-2025-49300	Insertion of Sensitive Information Into Sent Data vulnerability in shinetheme Traveler Option Tree custom-option-tree allows Retrieve Embedded Sensitive Data.This Traveler Option Tree: from n/a through <= 2.8.
CVE-2025-55703	An error-based SQL injection vulnerability exists in the Sunbird Power IQ 9.2.0 API. The vulnerability is due to an outdated API endpoint that applied arrays without validation. This can allow attackers to manipulate SQL queries. This has been addressed in Power IQ version 9.2.1, where the API call code was updated to ensure s of input values.
CVE-2025-14663	A vulnerability was determined in code-projects Student File Management System 1.0. This vulnerability affects unknown code of the file /admin/update_student.ph manipulation can lead to cross site scripting. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.
CVE-2025-14722	A vulnerability was determined in vion707 DMadmin up to 3403cafdb42537a648c30bf8cbc8148ec60437d1. This impacts the function Add of the file Admin/Controller/AddonsController.class.php of the component Backend. Executing manipulation can lead to cross site scripting. The attack can be executed remo exploit has been publicly disclosed and may be utilized. This product implements a rolling release for ongoing delivery, which means version information for affecte releases is unavailable. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-14662	A vulnerability was found in code-projects Student File Management System 1.0. This affects an unknown part of the file /admin/update_user.php of the component Page. Performing manipulation results in cross site scripting. The attack may be initiated remotely. The exploit has been made public and could be used.
CVE-2025-43410	The issue was addressed with improved handling of caches. This issue is fixed in macOS Sequoia 15.7.2, macOS Sonoma 14.8.2. An attacker with physical access r view deleted notes.
CVE-2025-68266	In the Linux kernel, the following vulnerability has been resolved: bfs: Reconstruct file type when loading from disk syzbot is reporting that S_IFMT bits of inode->i_ become bogus when the S_IFMT bits of the 32bits "mode" field loaded from disk are corrupted or when the 32bits "attributes" field loaded from disk are corrupted. documentation says that BFS uses only lower 9 bits of the "mode" field. But I can't find an explicit explanation that the unused upper 23 bits (especially, the S_IFMT initialized with 0. Therefore, ignore the S_IFMT bits of the "mode" field loaded from disk. Also, verify that the value of the "attributes" field loaded from disk is eithe BFS_VDIR (because BFS supports only regular files and the root directory).
CVE-2025-68265	In the Linux kernel, the following vulnerability has been resolved: nvme: fix admin request_queue lifetime The namespaces can access the controller's admin reque and stale references on the namespaces may exist after tearing down the controller. Ensure the admin request_queue is active by moving the controller's 'put' to a controller references have been released to ensure no one is can access the request_queue. This fixes a reported use-after-free bug: BUG: KASAN: slab-use-after-fr blk_queue_enter+0x41c/0x4a0 Read of size 8 at addr ffff88c0a53819f8 by task nvme/3287 CPU: 67 UID: 0 PID: 3287 Comm: nvme Tainted: G E 6.13.2-ga1582f1a0 Tainted: [E]=UNSIGNED_MODULE Hardware name: Jabil /EGS 2S MB1, BIOS 1.00 06/18/2025 Call Trace: <TASK> dump_stack_lvl+0x4f/0x60 print_report+0xc4/0x6 _raw_spin_lock_irqsave+0x70/0xb0 ? _raw_read_unlock_irqrestore+0x30/0x30 ? blk_queue_enter+0x41c/0x4a0 kasan_report+0xab/0xe0 ? blk_queue_enter+0x41 blk_queue_enter+0x41c/0x4a0 ? __irq_work_queue_local+0x75/0x1d0 ? blk_queue_start_drain+0x70/0x70 ? irq_work_queue+0x18/0x20 ? vprintk_emit.part.0+0x1 wake_up_klogd_work_func+0x60/0x60 blk_mq_alloc_request+0x2b7/0x6b0 ? __blk_mq_alloc_requests+0x1060/0x1060 ? __switch_to+0x5b7/0x1060 nvme_submit_user_cmd+0xa9/0x330 nvme_user_cmd.isra.0+0x240/0x3f0 ? force_sigsegv+0xe0/0xe0 ? nvme_user_cmd64+0x400/0x400 ? vfs_fileattr_set+0x9b0 cgroup_update_frozen_flag+0x24/0x1c0 ? cgroup_leave_frozen+0x204/0x330 ? nvme_ioctl+0x7c/0x2c0 blkdev_ioctl+0x1a8/0x4d0 ? blkdev_common_ioctl+0x193 fdget+0x54/0x380 __x64_sys_ioctl+0x129/0x190 do_syscall_64+0x5b/0x160 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x7f765f703b0b Code: ff ff f 49 c7 c4 ff ff ff ff 5b 5d 4c 89 e0 41 5c c3 66 0f 1f 84 00 00 00 00 00 f3 0f 1e fa b8 10 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d dd 52 0f 00 f7 d8 64 89 002b:00007ffe2cefe808 EFLAGS: 00000202 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 00007ffe2cefe860 RCX: 00007f765f703b0b RDX: 00007ffe2cef 00000000c0484e41 RDI: 0000000000000003 RBP: 0000000000000000 R08: 0000000000000003 R09: 0000000000000000 R10: 00007f765f611d50 R11: 0000000 R12: 0000000000000003 R13: 00000000c0484e41 R14: 0000000000000001 R15: 00007ffe2cefea60 </TASK>
CVE-2025-68255	In the Linux kernel, the following vulnerability has been resolved: staging: rtl8723bs: fix stack buffer overflow in OnAssocReq IE parsing The Supported Rates IE len incoming Association Request frame was used directly as the memcpy() length when copying into a fixed-size 16-byte stack buffer (supportRate). A malicious stati advertise an IE length larger than 16 bytes, causing a stack buffer overflow. Clamp ie_len to the buffer size before copying the Supported Rates IE, and correct the when merging Extended Supported Rates to prevent a second potential overflow. This prevents kernel stack corruption triggered by malformed association reques
CVE-2025-68078	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeNectar Salient Portfolio salient-portfolio allows Stored XS affects Salient Portfolio: from n/a through <= 1.8.2.
CVE-2025-68254	In the Linux kernel, the following vulnerability has been resolved: staging: rtl8723bs: fix out-of-bounds read in OnBeacon ESR IE parsing The Extended Supported R handling in OnBeacon accessed *(p + 1 + ielen) and *(p + 2 + ielen) without verifying that these offsets lie within the received frame buffer. A malformed beacon positioned at the end of the buffer could cause an out-of-bounds read, potentially triggering a kernel panic. Add a boundary check to ensure that the ESR IE body a subsequent bytes are within the limits of the frame before attempting to access them. This prevents OOB reads caused by malformed beacon frames.
CVE-2025-65075	WaveView client allows users to execute restricted set of predefined commands and scripts on the connected WaveStore Server. A malicious attacker with high-pri to read or delete files, with the permissions of dvr user, on the server using path traversal in the alog script. This issue was fixed in version 6.44.44
CVE-2025-68253	In the Linux kernel, the following vulnerability has been resolved: mm: don't spin in add_stack_record when gfp flags don't allow syzbot was able to find the followi add_stack_record_to_list mm/page_owner.c:182 [inline] inc_stack_record_count mm/page_owner.c:214 [inline] __set_page_owner+0x2c3/0x4a0 mm/page_owner.c: set_page_owner include/linux/page_owner.h:32 [inline] post_alloc_hook+0x240/0x2a0 mm/page_alloc.c:1851 prep_new_page mm/page_alloc.c:1859 [inline] get_page_from_freelist+0x21e4/0x22c0 mm/page_alloc.c:3858 alloc_pages_nolock_noprof+0x94/0x120 mm/page_alloc.c:7554 Don't spin in add_stack_record_to_l

	called from *_nolock() context.
CVE-2025-68281	In the Linux kernel, the following vulnerability has been resolved: ASoC: SDCA: bug fix while parsing mipi-sdca-control-cn-list "struct sdca_control" declares "values integer array. But the memory allocated to it is of char array. This causes crash for sdca_parse_function API. This patch addresses the issue by allocating correct da
CVE-2025-68082	Cross-Site Request Forgery (CSRF) vulnerability in SEMrush CY LTD Semrush Content Toolkit semrush-contentshake allows Cross Site Request Forgery.This issue af Content Toolkit: from n/a through <= 1.1.32.
CVE-2025-68252	In the Linux kernel, the following vulnerability has been resolved: misc: fastrpc: Fix dma_buf object leak in fastrpc_map_lookup In fastrpc_map_lookup, dma_buf_ge obtain a reference to the dma_buf for comparison purposes. However, this reference is never released when the function returns, leading to a dma_buf memory lea adding dma_buf_put before returning from the function, ensuring that the temporarily acquired reference is properly released regardless of whether a matching ma Rule: add
CVE-2025-68251	In the Linux kernel, the following vulnerability has been resolved: erofs: avoid infinite loops due to corrupted subpage compact indexes Robert reported an infinite by two crafted images. The root cause is that `clusterofs` can be larger than `lclustersize` for !NONHEAD `lclusters` in corrupted subpage compact indexes, e.g.: b lclustersize = 512 lcn = 6 clusterofs = 515 Move the corresponding check for full compress indexes to `z_erofs_load_lcluster_from_disk()` to also cover subpage co compress indexes. It also fixes the position of `m->type >= Z_EROFS_LCLUSTER_TYPE_MAX` check, since it should be placed right after `z_erofs_load_{compact,fu
CVE-2025-40347	In the Linux kernel, the following vulnerability has been resolved: net: enetc: fix the deadlock of enetc_mdio_lock After applying the workaround for err050089, the platform experiences RCU stalls on RT kernel. This issue is caused by the recursive acquisition of the read lock enetc_mdio_lock. Here list some of the call stacks id the enetc_poll path that may lead to a deadlock: enetc_poll -> enetc_lock_mdio -> enetc_clean_rx_ring OR napi_complete_done -> napi_gro_receive -> enetc_start enetc_lock_mdio -> enetc_map_tx_buffs -> enetc_unlock_mdio -> enetc_unlock_mdio After enetc_poll acquires the read lock, a higher-priority writer attempts to ac lock, causing preemption. The writer detects that a read lock is already held and is scheduled out. However, readers under enetc_poll cannot acquire the read lock because a writer is already waiting, leading to a thread hang. Currently, the deadlock is avoided by adjusting enetc_lock_mdio to prevent recursive lock acquisition
CVE-2025-68256	In the Linux kernel, the following vulnerability has been resolved: staging: rtl8723bs: fix out-of-bounds read in rtw_get_ie() parser The Information Element (IE) pars rtw_get_ie() trusted the length byte of each IE without validating that the IE body (len bytes after the 2-byte header) fits inside the remaining frame buffer. A malfo can advertise an IE length larger than the available data, causing the parser to increment its pointer beyond the buffer end. This results in out-of-bounds reads or, the pattern, an infinite loop. Fix by validating that (offset + 2 + len) does not exceed the limit before accepting the IE or advancing to the next element. This preve and ensures the parser terminates safely on malformed frames.
CVE-2025-40346	In the Linux kernel, the following vulnerability has been resolved: arch_topology: Fix incorrect error check in topology_parse_cpu_capacity() Fix incorrect use of PTR_ERR_OR_ZERO() in topology_parse_cpu_capacity() which causes the code to proceed with NULL clock pointers. The current logic uses !PTR_ERR_OR_ZERO(cpu_ evaluates to true for both valid pointers and NULL, leading to potential NULL pointer dereference in clk_get_rate(). Per include/linux/err.h documentation, PTR_ERR_ returns: "The error code within @ptr if it is an error pointer; 0 otherwise." This means PTR_ERR_OR_ZERO() returns 0 for both valid pointers AND NULL pointers. The !PTR_ERR_OR_ZERO(cpu_clk) evaluates to true (proceed) when cpu_clk is either valid or NULL, causing clk_get_rate(NULL) to be called when of_clk_get() returns NU with !IS_ERR_OR_NULL(cpu_clk) which only proceeds for valid pointers, preventing potential NULL pointer dereference in clk_get_rate().
CVE-2025-68257	In the Linux kernel, the following vulnerability has been resolved: comedi: check device's attached status in compat ioctls Syzbot identified an issue [1] that crashe seemingly due to unexistent callback dev->get_valid_routes(). By all means, this should not occur as said callback must always be set to get_zero_valid_routes() in __comedi_device_postconfig(). As the crash seems to appear exclusively in i386 kernels, at least, judging from [1] reports, the blame lies with compat versions of s handlers. Several of them are modified and do not use comedi_unlocked_ioctl(). While functionality of these ioctls essentially copy their original versions, they do n required sanity check for device's attached status. This, in turn, leads to a possibility of calling select IOCTLs on a device that has not been properly setup, even via COMEDI_DEVCONFIG. Doing so on unconfigured devices means that several crucial steps are missed, for instance, specifying dev->get_valid_routes() callback. Fix somewhat crudely by ensuring device's attached status before performing any ioctls, improving logic consistency between modern and compat functions. [1] Syzb BUG: kernel NULL pointer dereference, address: 0000000000000000 ... CR2: ffffffffffffffd6 CR3: 000000006c717000 CR4: 0000000000352ef0 Call Trace: <TASK> get_valid_routes drivers/comedi/comedi_fops.c:1322 [inline] parse_insn+0x78c/0x1970 drivers/comedi/comedi_fops.c:1401 do_insnlist_ioctl+0x272/0x700 drivers/comedi/comedi_fops.c:1594 compat_insnlist drivers/comedi/comedi_fops.c:3208 [inline] comedi_compat_ioctl+0x810/0x990 drivers/comedi/comedi_fops.c:3 __do_compat_sys_ioctl fs/ioctl.c:695 [inline] __se_compat_sys_ioctl fs/ioctl.c:638 [inline] __ia32_compat_sys_ioctl+0x242/0x370 fs/ioctl.c:638 do_syscall_32_irqs_on arch/x86/entry/syscall_32.c:83 [inline] ...
CVE-2025-68258	In the Linux kernel, the following vulnerability has been resolved: comedi: multiq3: sanitize config options in multiq3_attach() Syzbot identified an issue [1] in multi that induces a task timeout due to open() or COMEDI_DEVCONFIG ioctl operations, specifically, in the case of multiq3 driver. This problem arose when syzkaller ma weird configuration options used to specify the number of channels in encoder subdevice. If a particularly great number is passed to s->n_chan in multiq3_attach() >options[2], then multiple calls to multiq3_encoder_reset() at the end of driver-specific attach() method will be running for minutes, thus blocking tasks and affecte well. While this issue is most likely not too dangerous for real-life devices, it still makes sense to sanitize configuration inputs. Enable a sensible limit on the numbe chips (4 chips max, each with 2 channels) to stop this behaviour from manifesting. [1] Syzbot crash: INFO: task syz.2.19:6067 blocked for more than 143 seconds. <TASK> context_switch kernel/sched/core.c:5254 [inline] __schedule+0x17c4/0x4d60 kernel/sched/core.c:6862 __schedule_loop kernel/sched/core.c:6944 [inline] schedule+0x165/0x360 kernel/sched/core.c:6959 schedule_preempt_disabled+0x13/0x30 kernel/sched/core.c:7016 __mutex_lock_common kernel/locking/mutex.c __mutex_lock+0x7e6/0x1350 kernel/locking/mutex.c:760 comedi_open+0xc0/0x590 drivers/comedi/comedi_fops.c:2868 chrdev_open+0x4cc/0x5e0 fs/char_dev.c: do_dentry_open+0x953/0x13f0 fs/open.c:965 vfs_open+0x3b/0x340 fs/open.c:1097 ...
CVE-2025-68264	In the Linux kernel, the following vulnerability has been resolved: ext4: refresh inline data size before write operations The cached ei->i_inline_size can become sta the initial size check and when ext4_update_inline_data()/ext4_create_inline_data() use it. Although ext4_get_max_inline_size() reads the correct value at the time concurrent xattr operations can modify i_inline_size before ext4_write_lock_xattr() is acquired. This causes ext4_update_inline_data() and ext4_create_inline_data() stale capacity values, leading to a BUG_ON() crash in ext4_write_inline_data(): kernel BUG at fs/ext4/inline.c:1331! BUG_ON(pos + len > EXT4_I(inode)->i_inline_siz window: 1. ext4_get_max_inline_size() reads i_inline_size = 60 (correct) 2. Size check passes for 50-byte write 3. [Another thread adds xattr, i_inline_size changes t ext4_write_lock_xattr() acquires lock 5. ext4_update_inline_data() uses stale i_inline_size = 60 6. Attempts to write 50 bytes but only 40 bytes actually available 7. triggers Fix this by recalculating i_inline_size via ext4_find_inline_data_nolock() immediately after acquiring xattr_sem. This ensures ext4_update_inline_data() and ext4_create_inline_data() work with current values that are protected from concurrent modifications. This is similar to commit a54c4613dac1 ("ext4: fix race writin inline_data file while its xattrs are changing") which fixed i_inline_off staleness. This patch addresses the related i_inline_size staleness issue.
CVE-2025-68070	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vektor,Inc. VK Google Job Posting Manager vk-google-job-postin allows Stored XSS.This issue affects VK Google Job Posting Manager: from n/a through <= 1.2.21.
CVE-2025-68259	In the Linux kernel, the following vulnerability has been resolved: KVM: SVM: Don't skip unrelated instruction if INT3/INTO is replaced When re-injecting a soft interr INT3, INT0, or (select) INTn instruction, discard the exception and retry the instruction if the code stream is changed (e.g. by a different vCPU) between when the C the instruction and when KVM decodes the instruction to get the next RIP. As effectively predicted by commit 6ef88d6e36c2 ("KVM: SVM: Re-inject INT3/INTO inste the instruction"), failure to verify that the correct INTn instruction was decoded can effectively clobber guest state due to decoding the wrong instruction and thus wrong next RIP. The bug most often manifests as "Oops: int3" panics on static branch checks in Linux guests. Enabling or disabling a static branch in Linux uses the "text poke" code patching mechanism. To modify code while other CPUs may be executing that code, Linux (temporarily) replaces the first byte of the original instr int3 (opcode 0xcc), then patches in the new code stream except for the first byte, and finally replaces the int3 with the first byte of the new code stream. If a CPU i.e. executes the code while it's being modified, then the guest kernel must look up the RIP to determine how to handle the #BP, e.g. by emulating the new instruct is incorrect, then this lookup fails and the guest kernel panics. The bug reproduces almost instantly by hacking the guest kernel to repeatedly check a static branch

	running a drgn script[2] on the host to constantly swap out the memory containing the guest's TSS. [1]: https://gist.github.com/osandov/44d17c51c28c0ac998ea03 [2]: https://gist.github.com/osandov/10e45e45afa29b11e0c7209247afc00b
CVE-2025-68263	In the Linux kernel, the following vulnerability has been resolved: ksmbd: ipc: fix use-after-free in ipc_msg_send_request ipc_msg_send_request() waits for a generi using an ipc_msg_table_entry on the stack. The generic netlink handler (handle_generic_event()/handle_response()) fills entry->response under ipc_msg_table_lock ipc_msg_send_request() used to validate and free entry->response without holding the same lock. Under high concurrency this allows a race where handle_respons data into entry->response while ipc_msg_send_request() has just freed it, leading to a slab-use-after-free reported by KASAN in handle_generic_event(): BUG: KASA after-free in handle_generic_event+0x3c4/0x5f0 [ksmbd] Write of size 12 at addr ffff888198ee6e20 by task pool/109349 ... Freed by task: kvfree ipc_msg_send_req ksmbd_rpc_open -> ksmbd_session_rpc_open [ksmbd] Fix by: - Taking ipc_msg_table_lock in ipc_msg_send_request() while validating entry->response, freeing it w and removing the entry from ipc_msg_table. - Returning the final entry->response pointer to the caller only after the hash entry is removed under the lock. - Retur the error path, preserving the original API semantics. This makes all accesses to entry->response consistent with handle_response(), which already updates and fill response buffer under ipc_msg_table_lock, and closes the race that allowed the UAF.
CVE-2025-68262	In the Linux kernel, the following vulnerability has been resolved: crypto: zstd - fix double-free in per-CPU stream cleanup The crypto/zstd module has a double-free occurs when multiple tfms are allocated and freed. The issue happens because zstd_streams (per-CPU contexts) are freed in zstd_exit() during every tfm destructio being managed at the module level. When multiple tfms exist, each tfm exit attempts to free the same shared per-CPU streams, resulting in a double-free. This lea trace similar to: BUG: Bad page state in process kworker/u16:1 pfn:106fd93 page: refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x106fd93 f 0x17ffffc0000000(node=0|zone=2|lastcpupid=0x1fffff) page_type: 0xffffffff() raw: 0017ffffc0000000 dead000000000100 dead000000000122 0000000000000000 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 page dumped because: nonzero entire_mapcount Modules linked in: ... CPU: 3 UID: 0 Comm: kworker/u16:1 Kdump: loaded Tainted: G B Hardware name: ... Workqueue: btrfs-delalloc btrfs_work_helper Call Trace: <TASK> dump_stack_lvl+0x5d/0x80 bad_page+0x71/0xd0 free_unref_page_prepare+0x24e/0x490 free_unref_page+0x60/0x170 crypto_acomp_free_streams+0x5d/0xc0 crypto_acomp_exit_tfm+0x2 crypto_destroy_tfm+0x60/0xc0 ... Change the lifecycle management of zstd_streams to free the streams only once during module cleanup.
CVE-2025-68261	In the Linux kernel, the following vulnerability has been resolved: ext4: add i_data_sem protection in ext4_destroy_inline_data_nolock() Fix a race between inline da and block mapping. The function ext4_destroy_inline_data_nolock() changes the inode data layout by clearing EXT4_INODE_INLINE_DATA and setting EXT4_INODE_ the same time, another thread may execute ext4_map_blocks(), which tests EXT4_INODE_EXTENTS to decide whether to call ext4_ext_map_blocks() or ext4_ind_m Without i_data_sem protection, ext4_ind_map_blocks() may receive inode with EXT4_INODE_EXTENTS flag and triggering assert. kernel BUG at fs/ext4/indirect.c:54 (loop2): unmounting filesystem. invalid opcode: 0000 [#1] PREEMPT SMP KASAN NOPTI Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.12.0-1 0 0010:ext4_ind_map_blocks.cold+0x2b/0x5a fs/ext4/indirect.c:546 Call Trace: <TASK> ext4_map_blocks+0xb9b/0x16f0 fs/ext4/inode.c:681 _ext4_get_block+0x242 fs/ext4/inode.c:822 ext4_block_write_begin+0x48b/0x12c0 fs/ext4/inode.c:1124 ext4_write_begin+0x598/0xef0 fs/ext4/inode.c:1255 ext4_da_write_begin+0x21e/0 fs/ext4/inode.c:3000 generic_perform_write+0x259/0x5d0 mm/filemap.c:3846 ext4_buffered_write_iter+0x15b/0x470 fs/ext4/file.c:285 ext4_file_write_iter+0x8e0/ fs/ext4/file.c:679 call_write_iter include/linux/fs.h:2271 [inline] do_iter_readv_writev+0x212/0x3c0 fs/read_write.c:735 do_iter_write+0x186/0x710 fs/read_write.c:8 vfs_iter_write+0x70/0xa0 fs/read_write.c:902 iter_file_splice_write+0x73b/0xc90 fs/splice.c:685 do_splice_from fs/splice.c:763 [inline] direct_splice_actor+0x10f/0x fs/splice.c:950 splice_direct_to_actor+0x33a/0xa10 fs/splice.c:896 do_splice_direct+0x1a9/0x280 fs/splice.c:1002 do_sendfile+0xb13/0x12c0 fs/read_write.c:1255 __do_sys_sendfile64 fs/read_write.c:1323 [inline] __se_sys_sendfile64 fs/read_write.c:1309 [inline] __x64_sys_sendfile64+0x1cf/0x210 fs/read_write.c:1309 do_sysc arch/x86/entry/common.c:51 [inline] do_syscall_64+0x35/0x80 arch/x86/entry/common.c:81 entry_SYSCALL_64_after_hwframe+0x6e/0xd8
CVE-2025-68260	In the Linux kernel, the following vulnerability has been resolved: rust_binder: fix race condition on death_list Rust Binder contains the following unsafe operation: / `NodeDeath` is never inserted into the death list // of any node other than its owner, so it is either in this // death list or in no death list. unsafe { node_inner.death_list.remove(self) }; This operation is unsafe because when touching the prev/next pointers of a list element, we have to ensure that no other thre touching them in parallel. If the node is present in the list that `remove` is called on, then that is fine because we have exclusive access to that list. If the node is n then it's also ok. But if it's present in a different list that may be accessed in parallel, then that may be a data race on the prev/next pointers. And unfortunately tha what is happening here. In Node::release, we: 1. Take the lock. 2. Move all items to a local list on the stack. 3. Drop the lock. 4. Iterate the local list on the stack. Co threads using the unsafe remove method on the original list, this leads to memory corruption of the prev/next pointers. This leads to crashes like this one: Unable t kernel paging request at virtual address 000bb9841bcac70e Mem abort info: ESR = 0x0000000096000044 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, ISS = 0x00000044, ISS2 = 0x00000000 CM = 0, WnR = 1, TnD = 0, TagAccess = 0 GCS = 0, DirtyBit = 0, Xs = 0 [000bb9841bcac70e] address between user and kernel address ranges Internal error: Oops: 0000000096000044 [#1] PREEMPT SMP google- 538c004.gcdd: context saved(CPU:1) item - log_kevents is disabled Modules linked in: ... rust_binder CPU: 1 UID: 0 PID: 2092 Comm: kworker/1:178 Tainted: G S W android16-5-g98debd5df505-4k #1 f94a6367396c5488d635708e43ee0c888d230b0b Tainted: [S]=CPU_OUT_OF_SPEC, [W]=WARN, [O]=OOT_MODULE, [E]=UNSIG Hardware name: MUSTANG PVT 1.0 based on LGA (DT) Workqueue: events _RNvXs6_NtCsdfZWD8DztAw_6kernel9workqueueINtNtNtB7_4sync3arc3ArcNtNtCs8QPsHWIn21X_16rust_binder_main7process7ProcessEINtB5_15WorkItemPointerK [rust_binder] pstate: 23400005 (nzCv daif +PAN -UAO +TCO +DIT -SSBS BTYPE=--) pc : _RNvXs3_NtCs8QPsHWIn21X_16rust_binder_main7processNtB5_7ProcessNtNtCsdfZWD8DztAw_6kernel9workqueue8WorkItem3run+0x450/0x11f8 [rust_binder] lr : _RNvXs3_NtCs8QPsHWIn21X_16rust_binder_main7processNtB5_7ProcessNtNtCsdfZWD8DztAw_6kernel9workqueue8WorkItem3run+0x464/0x11f8 [rust_binder] sp ffffffc09b433ac0 x29: ffffffc09b433d30 x28: ffffff8821690000 x27: ffffffd40cbaa448 x26: ffffff8821690000 x25: 00000000ffffffff x24: ffffff88d0376578 x23: 000000 x22: ffffffc09b433c78 x21: ffffff88e8f9bf40 x20: ffffff88e8f9bf40 x19: ffffff882692b000 x18: ffffffd40f10bf00 x17: 00000000c006287d x16: 00000000c006287d x15 00000000000003b0 x14: 0000000000000100 x13: 000000201cb79ae0 x12: fffffffffffffff0 x11: 0000000000000000 x10: 0000000000000001 x9 : 00000000000000 b80bb9841bcac706 x7 : 0000000000000001 x6 : ffffffffebee63f30 x5 : 0000000000000000 x4 : 0000000000000001 x3 : 0000000000000000 x2 : 00000000000040 ffffff88216900c0 x0 : ffffff88e8f9bf00 Call trace: _RNvXs3_NtCs8QPsHWIn21X_16rust_binder_main7processNtB5_7ProcessNtNtCsdfZWD8DztAw_6kernel9workqueue8WorkItem3run+0x450/0x11f8 [rust_binder bbc172b53665bbc815363b22e97e3f7e3fe971fc] process_scheduled_works+0x1c4/0x45c worker_thread+0x32c/0x3e8 kthread+0x11c/0x1c8 ret_from_fork+0x10/ 94218d85 b4000155 a94026a8 d10102a0 (f9000509) ---[end trace 0000000000000000]--- Thus, modify Node::release to pop items directly off the original list.
CVE-2025-40348	In the Linux kernel, the following vulnerability has been resolved: slab: Avoid race on slab->obj_exts in alloc_slab_obj_exts If two competing threads enter alloc_sla and one of them fails to allocate the object extension vector, it might override the valid slab->obj_exts allocated by the other thread with OBJEXTS_ALLOC_FAIL. Th the thread that lost this race and expects a valid pointer to dereference a NULL pointer later on. Update slab->obj_exts atomically using cmpxchg() to avoid slab-> overrides by racing threads. Thanks for Vlastimil and Suren's help with debugging.
CVE-2025-40349	In the Linux kernel, the following vulnerability has been resolved: hfs: validate record offset in hfsplus_bmap_alloc hfsplus_bmap_alloc can trigger a crash if a recor length is larger than node_size [15.264282] BUG: KASAN: slab-out-of-bounds in hfsplus_bmap_alloc+0x887/0x8b0 [15.265192] Read of size 8 at addr ffff8881085 test/183 [15.265949] [15.266163] CPU: 0 UID: 0 PID: 183 Comm: test Not tainted 6.17.0-rc2-gc17b750b3ad9 #14 PREEMPT(voluntary) [15.266165] Hardware na Ubuntu 24.04 PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [15.266167] Call Trace: [15.266168] <TASK> [15.266169] dump_stack_lvl+0x5 15.266173] print_report+0xd0/0x660 [15.266181] kasan_report+0xce/0x100 [15.266185] hfsplus_bmap_alloc+0x887/0x8b0 [15.266208] hfs_btree_inc_height.isra.0+0xd5/0x7c0 [15.266217] hfsplus_brec_insert+0x870/0xb00 [15.266222] __hfsplus_ext_write_extent+0x428/0x570 [15.266225] __hfsplus_ext_cache_extent+0x5e/0x910 [15.266227] hfsplus_ext_read_extent+0x1b2/0x200 [15.266233] hfsplus_file_extend+0x5a7/0x1000 [15.266237] hfsplus_get_block+0x12b/0x8c0 [15.266238] __block_write_begin_int+0x36b/0x12c0 [15.266251] block_write_begin+0x77/0x110 [15.266252] cont_write_begin- [15.266259] hfsplus_write_begin+0x51/0x100 [15.266262] cont_write_begin+0x272/0x720 [15.266270] hfsplus_write_begin+0x51/0x100 [15.266274] generic_perform_write+0x321/0x750 [15.266285] generic_file_write_iter+0xc3/0x310 [15.266289] __kernel_write_iter+0x2fd/0x800 [15.266296] dump_user_range+0x2ea/0x910 [15.266301] elf_core_dump+0x2a94/0x2ed0 [15.266320] vfs_coredump+0x1d85/0x45e0 [15.266349] get_signal+0x12e3/0x19 15.266357] arch_do_signal_or_restart+0x89/0x580 [15.266362] irqentry_exit_to_user_mode+0xab/0x110 [15.266364] asm_exc_page_fault+0x26/0x30 [15.2663 0033:0x41bd35 [15.266367] Code: bc d1 f3 0f 7f 27 f3 0f 7f 6f 10 f3 0f 7f 77 20 f3 0f 7f 7f 30 49 83 c0 0f 49 29 d0 48 8d 7c 17 31 e9 9f 0b 00 00 66 0f ef c0 <f3> 6f 56 10 66 0f 74 c1 66 0f d7 d0 49 83 f8f [15.266369] RSP: 002b:00007ffc9e62d078 EFLAGS: 00010283 [15.266371] RAX: 00007ffc9e62d100 RBX: 0000000000 0000000000000000 [15.266372] RDX: 00000000000000e0 RSI: 0000000000000000 RDI: 00007ffc9e62d100 [15.266373] RBP: 0000400000000040 R08: 000000 R09: 0000000000000000 [15.266374] R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 [15.266375] R13: 0000000000000000 R14: 0000000000000000 R15: 0000400000000000 [15.266376] </TASK> When calling hfsplus_bmap_alloc to allocate a free node, this function first retrieves the bitm

	header node and map node using node->page together with the offset and length from hfs_brec_lenoff ``` len = hfs_brec_lenoff(node, 2, &off16); off = off16; off + >page_offset; pagep = node->page + (off >> PAGE_SHIFT); data = kmap_local_page(*pagep); ``` However, if the retrieved offset or length is invalid(i.e. exceeds the code may end up accessing pages outside the allocated range for this node. This patch adds proper validation of both offset and length before use, preventing page access. Move is_bnode_offset_valid and check_and_correct_requested_length to hfsplus_fs.h, as they may be required by other functions.
CVE-2025-40350	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: RX, Fix generating skb from non-linear xdp_buff for striding RQ XDP programs can cha layout of an xdp_buff through bpf_xdp_adjust_tail() and bpf_xdp_adjust_head(). Therefore, the driver cannot assume the size of the linear data area nor fragments. mlx5 by generating skb according to xdp_buff after XDP programs run. Currently, when handling multi-buf XDP, the mlx5 driver assumes the layout of an xdp_buff unchanged. That is, the linear data area continues to be empty and fragments remain the same. This may cause the driver to generate erroneous skb or triggering warning. When an XDP program added linear data through bpf_xdp_adjust_head(), the linear data will be ignored as mlx5e_build_linear_skb() builds an skb without and then pull data from fragments to fill the linear data area. When an XDP program has shrunk the non-linear data through bpf_xdp_adjust_tail(), the delta passed __pskb_pull_tail() may exceed the actual nonlinear data size and trigger the BUG_ON in it. To fix the issue, first record the original number of fragments. If the num fragments changes after the XDP program runs, rewind the end fragment pointer by the difference and recalculate the truesize. Then, build the skb with the linear matching the xdp_buff. Finally, only pull data in if there is non-linear data and fill the linear part up to 256 bytes.
CVE-2025-68250	In the Linux kernel, the following vulnerability has been resolved: hung_task: fix warnings caused by unaligned lock pointers The blocker tracking mechanism assu pointers are at least 4-byte aligned to use their lower bits for type encoding. However, as reported by Eero Tamminen, some architectures like m68k only guarante alignment of 32-bit values. This breaks the assumption and causes two related WARN_ON_ONCE checks to trigger. To fix this, the runtime checks are adjusted to si any lock that is not 4-byte aligned, effectively disabling the feature in such cases and avoiding the related warnings. Thanks to Geert Uytterhoeven for bisecting!
CVE-2025-68084	Missing Authorization vulnerability in Nitesh Ultimate Auction ultimate-auction allows Exploiting Incorrectly Configured Access Control Security Levels.This issue aff Auction : from n/a through <= 4.3.2.
CVE-2025-10450	Exposure of Private Personal Information to an Unauthorized Actor vulnerability in RTI Connext Professional (Core Libraries) allows Sniffing Network Traffic.This issu Connext Professional: from 7.4.0 before 7.*, from 7.2.0 before 7.3.1.
CVE-2025-68243	In the Linux kernel, the following vulnerability has been resolved: NFS: Check the TLS certificate fields in nfs_match_client() If the TLS security policy is of type RPC_XPRTSEC_TLS_X509, then the cert_serial and privkey_serial fields need to match as well since they define the client's identity, as presented to the server.
CVE-2025-65593	nopCommerce 4.90.0 is vulnerable to Cross Site Request Forgery (CSRF) via the Schedule Tasks functionality.
CVE-2025-68239	In the Linux kernel, the following vulnerability has been resolved: binfmt_misc: restore write access before closing files opened by open_exec() bm_register_write() executable file using open_exec(), which internally calls do_open_execat() and denies write access on the file to avoid modification while it is being executed. Howe error occurs, bm_register_write() closes the file using filp_close() directly. This does not restore the write permission, which may cause subsequent write operations file to fail. Fix this by calling exe_file_allow_write_access() before filp_close() to restore the write permission properly.
CVE-2025-65589	nopCommerce 4.90.0 is vulnerable to Cross Site Scripting (XSS) via the Attributes functionality.
CVE-2025-68240	In the Linux kernel, the following vulnerability has been resolved: nilfs2: avoid having an active sc_timer before freeing sci Because kthread_stop did not stop sc_ta and returned -EINTR, the sc_timer was not properly closed, ultimately causing the problem [1] reported by syzbot when freeing sci due to the sc_timer not being cl the thread sc_task main function nilfs_segctor_thread() returns 0 when it succeeds, when the return value of kthread_stop() is not 0 in nilfs_segctor_destroy(), we b has not properly closed sc_timer. We use timer_shutdown_sync() to sync wait for sc_timer to shutdown, and set the value of sc_task to NULL under the protection o sc_state_lock, so as to avoid the issue caused by sc_timer not being properly shutdowned. [1] ODEBUG: free active (active state 0) object: 00000000dacb411a obje timer_list hint: nilfs_construction_timeout Call trace: nilfs_segctor_destroy fs/nilfs2/segment.c:2811 [inline] nilfs_detach_log_writer+0x668/0x8cc fs/nilfs2/segment. nilfs_put_super+0x4c/0x12c fs/nilfs2/super.c:509
CVE-2025-62864	Ampere AmpereOne AC03 devices before 3.5.9.3, AmpereOne AC04 devices before 4.4.5.2, and AmpereOne M devices before 5.4.5.1 allow an incorrectly formed S UEFI-MM MMCommunicate service that could result in an out-of-bounds write within the UEFI-MM Secure Partition context.
CVE-2025-62863	Ampere AmpereOne AC03 devices before 3.5.9.3, AmpereOne AC04 devices before 4.4.5.2, and AmpereOne M devices before 5.4.5.1 allow an incorrectly formed S UEFI-MM PCIe driver that could result in an out-of-bounds write within PCIe driver's S-EL0 address space.
CVE-2025-68238	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: cadence: fix DMA device NULL pointer dereference The DMA device pointer `dma_ being dereferenced before ensuring that `cdns_ctrl->dmac` is properly initialized. Move the assignment of `dma_dev` after successfully acquiring the DMA channe the pointer is valid before use.
CVE-2025-68237	In the Linux kernel, the following vulnerability has been resolved: mtdchar: fix integer overflow in read/write ioctls The "req.start" and "req.len" variables are u64 v come from the user at the start of the function. We mask away the high 32 bits of "req.len" so that's capped at U32_MAX but the "req.start" variable can go up to U which means that the addition can still integer overflow. Use check_add_overflow() to fix this bug.
CVE-2025-52196	Server-Side Request Forgery (SSRF) vulnerability in Ctera Portal 8.1.x (8.1.1417.24) allows remote attackers to induce the server to make arbitrary HTTP requests v HTML file containing an iframe.
CVE-2025-68142	PyMdown Extensions is a set of extensions for the `Python-Markdown` markdown project. Versions prior to 10.16.1 have a ReDOS bug found within the figure capti (`pymdownx.blocks.caption`). In systems that take unchecked user content, this could cause long hanges when processing the data if a malicious payload was cra issue is patched in Release 10.16.1. As a workaround, those who process unknown user content without timeouts or other safeguards in place to prevent really larg content being aimed at systems may avoid the use of `pymdownx.blocks.caption` until they're able to upgrade.
CVE-2025-68241	In the Linux kernel, the following vulnerability has been resolved: ipv4: route: Prevent rt_bind_exception() from rebinding stale fnhe The sit driver's packet transmis calls: sit_tunnel_xmit() -> update_or_create_fnhe(), which lead to fnhe_remove_oldest() being called to delete entries exceeding FNHE_RECLAIM_DEPTH+random. T window is between fnhe_remove_oldest() selecting fnheX for deletion and the subsequent kfree_rcu(). During this time, the concurrent path's __mkroute_output() - find_exception() can fetch the soon-to-be-deleted fnheX, and rt_bind_exception() then binds it with a new dst using a dst_hold(). When the original fnheX is freed vi reference remains permanently leaked. CPU 0 CPU 1 __mkroute_output() find_exception() [fnheX] update_or_create_fnhe() fnhe_remove_oldest() [fnheX] rt_bind_ex [bind dst] RCU callback [fnheX freed, dst leak] This issue manifests as a device reference count leak and a warning in dmesg when unregistering the net device: unregister_netdevice: waiting for sitX to become free. Usage count = N Ido Schimmel provided the simple test validation method [1]. The fix clears 'oldest->fnhe_d calling fnhe_flush_routes(). Since rt_bind_exception() checks this field, setting it to zero prevents the stale fnhe from being reused and bound to a new dst just befo [1] ip netns add ns1 ip -n ns1 link set dev lo up ip -n ns1 address add 192.0.2.1/32 dev lo ip -n ns1 link add name dummy1 up type dummy ip -n ns1 route add 192

	dummy1 ip -n ns1 link add name gretap1 up arp off type gretap \ local 192.0.2.1 remote 192.0.2.2 ip -n ns1 route add 198.51.0.0/16 dev gretap1 taskset -c 0 ip ne mausezahn gretap1 \ -A 198.51.100.1 -B 198.51.0.0/16 -t udp -p 1000 -c 0 -q & taskset -c 2 ip netns exec ns1 mausezahn gretap1 \ -A 198.51.100.1 -B 198.51.0.0/ 1000 -c 0 -q & sleep 10 ip netns pids ns1 | xargs kill ip netns del ns1
CVE-2025-68242	In the Linux kernel, the following vulnerability has been resolved: NFS: Fix LTP test failures when timestamps are delegated The utimes01 and utime06 tests fail wh timestamps are enabled, specifically in subtests that modify the atime and mtime fields using the 'nobody' user ID. The problem can be reproduced as follow: # ec (rw,no_root_squash,sync)" >> /etc/exports # export -ra # mount -o rw,nfsvers=4.2 127.0.0.1:/media /tmpdir # cd /opt/ltp # ./runltp -d /tmpdir -s utimes01 # ./runl s utime06 This issue occurs because nfs_setattr does not verify the inode's UID against the caller's fsuid when delegated timestamps are permitted for the inode. T adds the UID check and if it does not match then the request is sent to the server for permission checking.
CVE-2025-68150	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.2 and 9.1.1-alpha.1, the Instagram au adapter allows clients to specify a custom API URL via the `apiURL` parameter in `authData`. This enables SSRF attacks and possibly authentication bypass if malic endpoints return fake responses to validate unauthorized users. This is fixed in versions 8.6.2 and 9.1.1-alpha.1 by hardcoding the Instagram Graph API URL `https://graph.instagram.com` and ignoring client-provided `apiURL` values. No known workarounds are available.
CVE-2025-65074	WaveView client allows users to execute restricted set of predefined commands and scripts on the connected WaveStore Server. A malicious attacker with high-pri to execute arbitrary OS commands on the server using path traversal in the showerr script. This issue was fixed in version 6.44.44
CVE-2025-65318	When using the attachment interaction functionality, Canary Mail 5.1.40 and below saves documents to a file system without a Mark-of-the-Web tag, which allows a bypass the built-in file protection mechanisms of both Windows OS and third-party software.
CVE-2025-65592	nopCommerce 4.90.0 is vulnerable to Cross Site Scripting (XSS) in the product management functionality. Malicious payloads inserted into the "Product Name" and Description" fields are stored in the backend database and executed automatically whenever a user views the affected pages.
CVE-2025-68244	In the Linux kernel, the following vulnerability has been resolved: drm/i915: Avoid lock inversion when pinning to GGTT on CHV/BXT+VTD On completion of i915_vr a synchronous variant of dma_fence_work_commit() is called. When pinning a VMA to GGTT address space on a Cherry View family processor, or on a Broxton gene with VTD enabled, i.e., when stop_machine() is then called from intel_ggtt_bind_vma(), that can potentially lead to lock inversion among reservation_ww and cpu_h [86.861179] == [86.861193] WARNING: possible circular locking dependenc [86.861209] 6.15.0-rc5-CI_DRM_16515-gca0305cadc2d+ #1 Tainted: G U [86.861226] -- [86.861238] i915_module_loa/1432 i acquire lock: [86.861252] ffffffff83489090 (cpu_hotplug_lock){++++}-{0:0}, at: stop_machine+0x1c/0x50 [86.861290] but task is already holding lock: [86.8613(ffffc90002e0b4c8 (reservation_ww_class_mutex){+.+.}-{3:3}, at: i915_vma_pin.constprop.0+0x39/0x1d0 [i915] [86.862233] which lock already depends on the n [86.862251] the existing dependency chain (in reverse order) is: [86.862265] -> #5 (reservation_ww_class_mutex){+.+.}-{3:3}: [86.862292] dma_resv_lockdep+ [86.862315] do_one_initcall+0x60/0x3f0 [86.862334] kernel_init_freeable+0x3cd/0x680 [86.862353] kernel_init+0x1b/0x200 [86.862369] ret_from_fork+0x47/0x [86.862383] ret_from_fork_asm+0x1a/0x30 [86.862399] -> #4 (reservation_ww_class_acquire){+.+.}-{0:0}: [86.862425] dma_resv_lockdep+0x178/0x390 [86.86 do_one_initcall+0x60/0x3f0 [86.862454] kernel_init_freeable+0x3cd/0x680 [86.862470] kernel_init+0x1b/0x200 [86.862482] ret_from_fork+0x47/0x70 [86.86249 ret_from_fork_asm+0x1a/0x30 [86.862509] -> #3 (&mm->mmap_lock){++++}-{3:3}: [86.862531] down_read_killable+0x46/0x1e0 [86.862546] lock_mm_and_find_vma+0xa2/0x280 [86.862561] do_user_addr_fault+0x266/0x8e0 [86.862578] exc_page_fault+0x8a/0x2f0 [86.862593] asm_exc_page_fault+0x [86.862607] filldir64+0xeb/0x180 [86.862620] kernfs_fop_readdir+0x118/0x480 [86.862635] iterate_dir+0xcf/0x2b0 [86.862648] __x64_sys_getdents64+0x84/0x [86.862661] x64_sys_call+0x1058/0x2660 [86.862675] do_syscall_64+0x91/0xe90 [86.862689] entry_SYSCALL_64_after_hwframe+0x76/0x7e [86.862703] -> #2 >kernfs_rwsem){++++}-{3:3}: [86.862725] down_write+0x3e/0xf0 [86.862738] kernfs_add_one+0x30/0x3c0 [86.862751] kernfs_create_dir_ns+0x53/0xb0 [86.8 internal_create_group+0x134/0x4c0 [86.862779] sysfs_create_group+0x13/0x20 [86.862792] topology_add_dev+0x1d/0x30 [86.862806] cpuhp_invoke_callback+ [86.862822] cpuhp_issue_call+0xbf/0x1f0 [86.862836] __cpuhp_setup_state_cpuslocked+0x111/0x320 [86.862852] __cpuhp_setup_state+0xb0/0x220 [86.862866 topology_sysfs_init+0x30/0x50 [86.862879] do_one_initcall+0x60/0x3f0 [86.862893] kernel_init_freeable+0x3cd/0x680 [86.862908] kernel_init+0x1b/0x200 [86.8 ret_from_fork+0x47/0x70 [86.862934] ret_from_fork_asm+0x1a/0x30 [86.862947] -> #1 (cpuhp_state_mutex){+.+.}-{3:3}: [86.862969] __mutex_lock+0xaa/0xe [86.862982] mutex_lock_nested+0x1b/0x30 [86.862995] __cpuhp_setup_state_cpuslocked+0x67/0x320 [86.863012] __cpuhp_setup_state+0xb0/0x220 [86.86302 page_alloc_init_cpuhp+0x2d/0x60 [86.863041] mm_core_init+0x22/0x2d0 [86.863054] start_kernel+0x576/0xbd0 [86.863068] x86_64_start_reservations+0x18/0 [86.863084] x86_64_start_kernel+0xbf/0x110 [86.863098] common_startup_64+0x13e/0x141 [86.863114] -> #0 (cpu_hotplug_lock){++++}-{0:0}: [86.863135] __lock_acquire+0x16 ---truncated---
CVE-2025-68245	In the Linux kernel, the following vulnerability has been resolved: net: netpoll: fix incorrect refcount handling causing incorrect cleanup commit efa95b01da18 ("ne after free") incorrectly ignored the refcount and prematurely set dev->npinfo to NULL during netpoll cleanup, leading to improper behavior and memory leaks. Sce lack of proper cleanup: 1) A netpoll is associated with a NIC (e.g., eth0) and netdev->npinfo is allocated, and refcnt = 1 - Keep in mind that npinfo is shared among instances. In this case, there is just one. 2) Another netpoll is also associated with the same NIC and npinfo->refcnt += 1. - Now dev->npinfo->refcnt = 2; - There i npinfo associated to the netdev. 3) When the first netpolls goes to clean up: - The first cleanup succeeds and clears np->dev->npinfo, ignoring refcnt. - It basically `RCU_INIT_POINTER(np->dev->npinfo, NULL);` - Set dev->npinfo = NULL, without proper cleanup - No ->ndo_netpoll_cleanup() is either called 4) Now the second t clean up - The second cleanup fails because np->dev->npinfo is already NULL. * In this case, ops->ndo_netpoll_cleanup() was never called, and the skb pool is not well (for the second netpoll instance) - This leaks npinfo and skbpool skbs, which is clearly reported by kmemleak. Revert commit efa95b01da18 ("netpoll: fix use a adds clarifying comments emphasizing that npinfo cleanup should only happen once the refcount reaches zero, ensuring stable and correct netpoll behavior.
CVE-2025-68246	In the Linux kernel, the following vulnerability has been resolved: ksmbd: close accepted socket when per-IP limit rejects connection When the per-IP connection lir exceeded in ksmbd_kthread_fn(), the code sets ret = -EAGAIN and continues the accept loop without closing the just-accepted socket. That leaks one socket per re attempt from a single IP and enables a trivial remote DoS. Release client_sk before continuing. This bug was found with ZeroPath.
CVE-2025-68247	In the Linux kernel, the following vulnerability has been resolved: posix-timers: Plug potential memory leak in do_timer_create() When posix timer creation is set to given timer ID and the access to the user space value faults, the function terminates without freeing the already allocated posix timer structure. Move the allocatio user space access to cure that. [tglx: Massaged change log]
CVE-2025-40352	In the Linux kernel, the following vulnerability has been resolved: platform/mellanox: mlxbf-pmc: add sysfs_attr_init() to count_clock init The lock-related debug log (CONFIG_LOCK_STAT) in the kernel is noting the following warning when the BlueField-3 SOC is booted: BUG: key ffff00008a3402a8 has not been registered! --------]---------- DEBUG_LOCKS_WARN_ON(1) WARNING: CPU: 4 PID: 592 at kernel/locking/lockdep.c:4801 lockdep_init_map_type+0x1d4/0x2a0 <snip> Call trace: lockdep_init_map_type+0x1d4/0x2a0 __kernfs_create_file+0x84/0x140 sysfs_add_file_mode_ns+0xcc/0x1cc internal_create_group+0x110/0x3d4 internal_create_groups.part.0+0x54/0xcc sysfs_create_groups+0x24/0x40 device_add+0x6e8/0x93c device_register+0x28/0x40 __hwmon_device_register+0x4b0 devm_hwmon_device_register_with_groups+0x7c/0xe0 mlxbf_pmc_probe+0x1e8/0x3e0 [mlxbf_pmc] platform_probe+0x70/0x110 The mlxbf_pmc driver must call sysfs_attr_init() during the initialization of the "count_clock" data structure to avoid this warning.
CVE-2025-14553	Exposure of password hashes through an unauthenticated API response in TP-Link Tapo C210 V.1.8 app on iOS and Android, allowing attackers to brute force the p local network. Issue can be mitigated through mobile application updates. Device firmware remains unchanged.
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: vmw_balloon: indicate success when effectively deflating during migration When migrating a ball first deflate the old page to then inflate the new page. However, if inflating the new page succeeded, we effectively deflated the old page, reducing the balloon size the migration actually worked: similar to migrating+ immediately deflating the new page. The old page will be freed back to the buddy. Right now, the core will lea be marked as isolated (as we returned an error). When later trying to putback that page, we will run into the WARN_ON_ONCE() in balloon_page_putback(). That ha changed in commit 3544c4faccb8 ("mm/balloon_compaction: stop using __ClearPageMovable()"); before that change, we would have tolerated that way of handling

68248	let's just return 0 in that case, making the core effectively just clear the "isolated" flag + freeing it back to the buddy as if the migration succeeded. Note that the r also get freed when the core puts the last reference. Note that this also makes it all be more consistent: we will no longer unisolate the page in the balloon driver w it marked as being isolated in migration core. This was found by code inspection.
CVE-2025-68249	In the Linux kernel, the following vulnerability has been resolved: most: usb: hdm_probe: Fix calling put_device() before device initialization The early error path in can jump to err_free_mdev before &mdev->dev has been initialized with device_initialize(). Calling put_device(&mdev->dev) there triggers a device core WARN an invoking kref_put(&kobj->kref, kobject_release) on an uninitialized kobject. In this path the private struct was only kmalloc'ed and the intended release is effective anyway, so free it directly instead of calling put_device() on an uninitialized device. This removes the WARNING and fixes the pre-initialization error path.
CVE-2025-65076	WaveView client allows users to execute restricted set of predefined commands and scripts on the connected WaveStore Server. A malicious attacker with high-pri to read or delete any file on the server using path traversal in the ilog script. This script is being run with root privileges. This issue was fixed in version 6.44.44
CVE-2025-14432	In limited scenarios, sensitive data might be written to the log file if an admin uses Microsoft Teams Admin Center (TAC) to make device configuration changes. The file is visible only to users with admin credentials. This is limited to Microsoft TAC and does not affect configuration changes made using the provisioning server or WebUI.
CVE-2025-40351	In the Linux kernel, the following vulnerability has been resolved: hfsplus: fix KMSAN uninit-value issue in hfsplus_delete_cat() The syzbot reported issue in hfsplus_ 70.682285][T9333] ===== [70.682943][T9333] BUG: KMSAN: uninit-value in hfsplus_subfolders_dec+0x1d7/0x220 [70.683640][T9333] hfsplus_subfolders_dec+0x1d7/0x220 [70.684141][T9333] hfsplus_delete_cat+0x105d/0x12b0 [70.6 T9333] hfsplus_rmdir+0x13d/0x310 [70.685048][T9333] vfs_rmdir+0x5ba/0x810 [70.685447][T9333] do_rmdir+0x964/0xea0 [70.685833][T9333] __x64_sys_rmdir+0x71/0xb0 [70.686260][T9333] x64_sys_call+0xcd8/0x3cf0 [70.686695][T9333] do_syscall_64+0xd9/0x1d0 [70.687119][T9333] entry_SYSCALL_64_after_hwframe+0x77/0x7f [70.687646][T9333] [70.687856][T9333] Uninit was stored to memory at: [70.688311][T9333] hfsplus_subfolders_inc+0x1c2/0x1d0 [70.688779][T9333] hfsplus_create_cat+0x148e/0x1800 [70.689231][T9333] hfsplus_mknod+0x27f/0x600 [70.689730][T hfsplus_mkdir+0x5a/0x70 [70.690146][T9333] vfs_mkdir+0x483/0x7a0 [70.690545][T9333] do_mkdirat+0x3f2/0xd30 [70.690944][T9333] __x64_sys_mkdir+0 70.691380][T9333] x64_sys_call+0x2f89/0x3cf0 [70.691816][T9333] do_syscall_64+0xd9/0x1d0 [70.692229][T9333] entry_SYSCALL_64_after_hwframe+0x77/ 70.692773][T9333] [70.692990][T9333] Uninit was stored to memory at: [70.693469][T9333] hfsplus_subfolders_inc+0x1c2/0x1d0 [70.693960][T9333] hfsplus_create_cat+0x148e/0x1800 [70.694438][T9333] hfsplus_fill_super+0x21c1/0x2700 [70.694911][T9333] mount_bdev+0x37b/0x530 [70.695320][T9333 hfsplus_mount+0x4d/0x60 [70.695729][T9333] legacy_get_tree+0x113/0x2c0 [70.696167][T9333] vfs_get_tree+0xb3/0x5c0 [70.696588][T9333] do_new_mount+0x73e/0x1630 [70.697013][T9333] path_mount+0x6e3/0x1eb0 [70.697425][T9333] __se_sys_mount+0x733/0x830 [70.697857][T9333] __x64_sys_mount+0xe4/0x150 [70.698269][T9333] x64_sys_call+0x2691/0x3cf0 [70.698704][T9333] do_syscall_64+0xd9/0x1d0 [70.699117][T9333] entry_SYSCALL_64_after_hwframe+0x77/0x7f [70.699730][T9333] [70.699946][T9333] Uninit was created at: [70.700378][T9333] __alloc_pages_noprof+0x714 70.700843][T9333] alloc_pages_mpol_noprof+0x2a2/0x9b0 [70.701331][T9333] alloc_pages_noprof+0xf8/0x1f0 [70.701774][T9333] allocate_slab+0x30e/0x13 70.702194][T9333] ___slab_alloc+0x1049/0x33a0 [70.702635][T9333] kmem_cache_alloc_lru_noprof+0x5ce/0xb20 [70.703153][T9333] hfsplus_alloc_inode+0x 70.703598][T9333] alloc_inode+0x82/0x490 [70.703984][T9333] iget_locked+0x22e/0x1320 [70.704428][T9333] hfsplus_iget+0x5c/0xba0 [70.704827][T933 hfsplus_btree_open+0x135/0x1dd0 [70.705291][T9333] hfsplus_fill_super+0x1132/0x2700 [70.705776][T9333] mount_bdev+0x37b/0x530 [70.706171][T9333 hfsplus_mount+0x4d/0x60 [70.706579][T9333] legacy_get_tree+0x113/0x2c0 [70.707019][T9333] vfs_get_tree+0xb3/0x5c0 [70.707444][T9333] do_new_mount+0x73e/0x1630 [70.707865][T9333] path_mount+0x6e3/0x1eb0 [70.708270][T9333] __se_sys_mount+0x733/0x830 [70.708711][T9333] __x64_sys_mount+0xe4/0x150 [70.709158][T9333] x64_sys_call+0x2691/0x3cf0 [70.709630][T9333] do_syscall_64+0xd9/0x1d0 [70.710053][T9333] entry_SYSCALL_64_after_hwframe+0x77/0x7f [70.710611][T9333] [70.710842][T9333] CPU: 3 UID: 0 PID: 9333 Comm: repro Not tainted 6.12.0-rc6-dirty #17 [T9333] Hardware name: QEMU Ubuntu 24.04 PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [70.712490][T9333] ===== [70.713085][T9333] Disabling lock debugging due to kernel taint [70.71 Kernel panic - not syncing: kmsan.panic set ... [70.714159][T9333] ---truncated---
CVE-2025-0852	Rejected reason: Voluntarily withdrawn
CVE-2025-40353	In the Linux kernel, the following vulnerability has been resolved: arm64: mte: Do not warn if the page is already tagged in copy_highpage() The arm64 copy_highp assumes that the destination page is newly allocated and not MTE-tagged (PG_mte_tagged unset) and warns accordingly. However, following commit 060913999d migrate: support poisoned recover from migrate folio"), folio_mc_copy() is called before __folio_migrate_mapping(). If the latter fails (-EAGAIN), the copy will be don same destination page. Since copy_highpage() already set the PG_mte_tagged flag, this second copy will warn. Replace the WARN_ON_ONCE(page already tagged) copy_highpage() with a comment.
CVE-2025-68319	In the Linux kernel, the following vulnerability has been resolved: netconsole: Acquire su_mutex before navigating configs hierarchy There is a race between opera iterate over the userdata cg_children list and concurrent add/remove of userdata items through configfs. The update_userdata() function iterates over the nt- >userdata_group.cg_children list, and count_extradata_entries() also iterates over this same list to count nodes. Quoting from Documentation/filesystems/configfs. subsystem can navigate the cg_children list and the ci_parent pointer > to see the tree created by the subsystem. This can race with configfs' > management of th so configfs uses the subsystem mutex to > protect modifications. Whenever a subsystem wants to navigate the > hierarchy, it must do so under the protection of > mutex. Without proper locking, if a userdata item is added or removed concurrently while these functions are iterating, the list can be accessed in an inconsister example, the list_for_each() loop can reach a node that is being removed from the list by list_del_init() which sets the nodes' .next pointer to point to itself, so the l end (or reach the WARN_ON_ONCE in update_userdata()). Fix this by holding the configfs subsystem mutex (su_mutex) during all operations that iterate over cg_c includes: - userdatum_value_store() which calls update_userdata() to iterate over cg_children - All sysdata_*_enabled_store() functions which call count_extradata_ iterate over cg_children The su_mutex must be acquired before dynamic_netconsole_mutex to avoid potential lock ordering issues, as configfs operations may alre su_mutex when calling into our code.
CVE-2025-68220	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: ti: netcp: Standardize knav_dma_open_channel to return NULL on error Make knav_dma_open_channel consistently return NULL on error instead of ERR_PTR. Currently the header include/linux/soc/ti/knav_dma.h returns NULL when the driver but the driver implementation does not even return NULL or ERR_PTR on failure, causing inconsistency in the users. This results in a crash in netcp_free_navigator_ followed (trimmed): Unhandled fault: alignment exception (0x221) at 0xffffffff2 [ffffffff2] *pgd=80000800207003, *pmd=82ffda003, *pte=00000000 Internal error: : ARM Modules linked in: CPU: 0 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.17.0-rc7 #1 NONE Hardware name: Keystone PC is at knav_dma_close_channel+0x30/ netcp_free_navigator_resources+0x2c/0x28c [... TRIM...] Call trace: knav_dma_close_channel from netcp_free_navigator_resources+0x2c/0x28c netcp_free_naviga from netcp_ndo_open+0x430/0x46c netcp_ndo_open from __dev_open+0x114/0x29c __dev_open from __dev_change_flags+0x190/0x208 __dev_change_flags from netif_change_flags+0x1c/0x58 netif_change_flags from dev_change_flags+0x38/0xa0 dev_change_flags from ip_auto_config+0x2c4/0x11f0 ip_auto_config from do_one_initcall+0x58/0x200 do_one_initcall from kernel_init_freeable+0x1cc/0x238 kernel_init_freeable from kernel_init+0x1c/0x12c kernel_init from ret_from_fork [... TRIM...] Standardize the error handling by making the function return NULL on all error conditions. The API is used in just the netcp_core.c so the impact is limite change, in effect reverts commit 5b6cb43b4d62 ("net: ethernet: ti: netcp_core: return error while dma channel open issue"), but provides a less error prone implen
CVE-2025-68308	In the Linux kernel, the following vulnerability has been resolved: can: kvaser_usb: leaf: Fix potential infinite loop in command parsers The `kvaser_usb_leaf_wait_c `kvaser_usb_leaf_read_bulk_callback` functions contain logic to zero-length commands. These commands are used to align data to the USB endpoint's wMaxPacke boundary. The driver attempts to skip these placeholders by aligning the buffer position `pos` to the next packet boundary using `round_up()` function. However, i command is found exactly on a packet boundary (i.e., `pos` is a multiple of wMaxPacketSize, including 0), `round_up` function will return the unchanged value of ` prevents `pos` to be increased, causing an infinite loop in the parsing logic. This patch fixes this in the function by using `pos + 1` instead. This ensures that even a boundary, the calculation is based on `pos + 1`, forcing `round_up()` to always return the next aligned boundary.

CVE-2025-68309	In the Linux kernel, the following vulnerability has been resolved: PCI/AER: Fix NULL pointer access by aer_info The kzalloc(GFP_KERNEL) may return NULL, so all ac aer_info->xxx will result in kernel panic. Fix it.
CVE-2025-68310	In the Linux kernel, the following vulnerability has been resolved: s390/pci: Avoid deadlock between PCI error recovery and mlx5 crdump Do not block PCI config ac through pci_cfg_access_lock() when executing the s390 variant of PCI error recovery: Acquire just device_lock() instead of pci_dev_lock() as powerpc's EEH and ger processing do. During error recovery testing a pair of tasks was reported to be hung: mlx5_core 0000:00:00.1: mlx5_health_try_recover:338:(pid 5553): health reco aborted, PCI reads still not working INFO: task kmcheck:72 blocked for more than 122 seconds. Not tainted 5.14.0-570.12.1.bringup7.el9.s390x #1 "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. task:kmcheck state:D stack:0 pid:72 tgid:72 ppid:2 flags:0x00000000 Call Trace: [<0000000652 __schedule+0x2a0/0x590 [<000000065256f356>] schedule+0x36/0xe0 [<000000065256f572>] schedule_preempt_disabled+0x22/0x30 [<0000000652570a94> __mutex_lock.constprop.0+0x484/0x8a8 [<000003ff800673a4>] mlx5_unload_one+0x34/0x58 [mlx5_core] [<000003ff8006745c>] mlx5_pci_err_detected+0x94/ [mlx5_core] [<0000000652556c5a>] zpci_event_attempt_error_recovery+0xf2/0x398 [<0000000651b9184a>] __zpci_event_error+0x23a/0x2c0 INFO: task kworker/u1664:6:1514 blocked for more than 122 seconds. Not tainted 5.14.0-570.12.1.bringup7.el9.s390x #1 "echo 0 > /proc/sys/kernel/hung_task_timeout_secs message. task:kworker/u1664:6 state:D stack:0 pid:1514 tgid:1514 ppid:2 flags:0x00000000 Workqueue: mlx5_health0000:00:00.0 mlx5_fw_fatal_reporter_err_wo Call Trace: [<000000065256f030>] __schedule+0x2a0/0x590 [<000000065256f356>] schedule+0x36/0xe0 [<0000000652172e28>] pci_wait_cfg+0x80/0xe8 [<0000000652172f94>] pci_cfg_access_lock+0x74/0x88 [<000003ff800916b6>] mlx5_vsc_gw_lock+0x36/0x178 [mlx5_core] [<000003ff80098824>] mlx5_crdump_collect+0x34/0x1c8 [mlx5_core] [<000003ff80074b62>] mlx5_fw_fatal_reporter_dump+0x6a/0xe8 [mlx5_core] [<0000000652512242>] devlink_health_do_dump.part.0+0x82/0x168 [<0000000652513212>] devlink_health_report+0x19a/0x230 [<000003ff80075a12>] mlx5_fw_fatal_reporter_err_work+0xba/0x1b0 [mlx5_core] No kernel log of the exact same error with an upstream kernel is available - but the very same deadlock be constructed there, too: - task: kmcheck mlx5_unload_one() tries to acquire devlink lock while the PCI error recovery code has set pdev->block_cfg_access by wa pci_cfg_access_lock() - task: kworker mlx5_crdump_collect() tries to set block_cfg_access through pci_cfg_access_lock() while devlink_health_report() had acquired lock. A similar deadlock situation can be reproduced by requesting a crdump with > devlink health dump show pci/<BDF> reporter fw_fatal while PCI error recover on the same <BDF> physical function by mlx5_core's pci_error_handlers. On s390 this can be injected with > zpcictl --reset-fw <BDF> Tests with this patch failed t that second deadlock situation, the devlink command is rejected with "kernel answers: Permission denied" - and we get a kernel log message of: mlx5_core 1ed0:0 mlx5_crdump_collect:50:(pid 254382): crdump: failed to lock vsc gw err -5 because the config read of VSC_SEMAPHORE is rejected by the underlying hardware. Tw attempts to address this issue have been discussed and ultimately rejected [see link], with the primary argument that s390's implementation of PCI error recovery restrictions that neither powerpc's EEH nor PCI AER handling need. Tests show that PCI error recovery on s390 is running to completion even without blocking acce config space.
CVE-2025-68311	In the Linux kernel, the following vulnerability has been resolved: tty: serial: ip22zilog: Use platform device for probing After commit 84a9582fd203 ("serial: core: S serial controllers to enable runtime PM") serial drivers need to provide a device in struct uart_port.dev otherwise an oops happens. To fix this issue for ip22zilog dri driver to a platform driver and setup the serial device in sgi-ip22 code.
CVE-2025-68312	In the Linux kernel, the following vulnerability has been resolved: usbnet: Prevents free active kevent The root cause of this issue are: 1. When probing the usbnet executing usbnet_link_change(dev, 0, 0); put the kevent work in global workqueue. However, the kevent has not yet been scheduled when the usbnet device is unr Therefore, executing free_netdev() results in the "free active object (kevent)" error reported here. 2. Another factor is that when calling usbnet_disconnect()->unregister_netdev(), if the usbnet device is up, ndo_stop() is executed to cancel the kevent. However, because the device is not up, ndo_stop() is not executed. T this problem is to cancel the kevent before executing free_netdev().
CVE-2025-68313	In the Linux kernel, the following vulnerability has been resolved: x86/CPU/AMD: Add RDSEED fix for Zen5 There's an issue with RDSEED's 16-bit and 32-bit register variants on Zen5 which return a random value of 0 "at a rate inconsistent with randomness while incorrectly signaling success (CF=1)". Search the web for AMD-SE more detail. Add a fix glue which checks microcode revisions. [bp: Add microcode revisions checking, rewrite.]
CVE-2025-68221	In the Linux kernel, the following vulnerability has been resolved: mptcp: fix address removal logic in mptcp_pm_nl_rm_addr Fix inverted WARN_ON_ONCE condition prevented normal address removal counter updates. The current code only executes decrement logic when the counter is already 0 (abnormal state), while normal (counter > 0) are ignored.
CVE-2025-68314	In the Linux kernel, the following vulnerability has been resolved: drm/msm: make sure last_fence is always updated Update last_fence in the vm-bind path instead managed path. last_fence is used to wait for work to finish in vm_bind contexts but not used for kernel managed contexts. This fixes a bug where last_fence is not context close leading to faults as resources are freed while in use. Patchwork: https://patchwork.freedesktop.org/patch/680080/
CVE-2025-68222	In the Linux kernel, the following vulnerability has been resolved: pinctrl: s32cc: fix uninitialized memory in s32_pinctrl_desc s32_pinctrl_desc is allocated with devr but not all of its fields are initialized. Notably, num_custom_params is used in pinconf_generic_parse_dt_config(), resulting in intermittent allocation errors, such as splat when probing i2c-imx: WARNING: CPU: 0 PID: 176 at mm/page_alloc.c:4795 __alloc_pages_noprof+0x290/0x300 [...] Hardware name: NXP S32G3 Reference D (S32G-VNP-RDB3) (DT) [...] Call trace: __alloc_pages_noprof+0x290/0x300 (P) ___kmalloc_large_node+0x84/0x168 __kmalloc_large_node_noprof+0x34/0x120 __kmalloc_noprof+0x2ac/0x378 pinconf_generic_parse_dt_config+0x68/0x1a0 s32_dt_node_to_map+0x104/0x248 dt_to_map_one_config+0x154/0x1d8 pinctrl_dt_to_map+0x12c/0x280 create_pinctrl+0x6c/0x270 pinctrl_get+0xc0/0x170 devm_pinctrl_get+0x50/0xa0 pinctrl_bind_pins+0x60/0x2a0 really_probe+0x6 __platform_driver_register+0x2c/0x40 i2c_adap_imx_init+0x28/0xff8 [i2c_imx] [...] This results in later parse failures that can cause issues in dependent drivers: s3 pinctrl 4009c240.pinctrl: /soc@0/pinctrl@4009c240/i2c0-pins/i2c0-grp0: could not parse node property s32g-siul2-pinctrl 4009c240.pinctrl: /soc@0/pinctrl@4009c2 pins/i2c0-grp0: could not parse node property [...] pca953x 0-0022: failed writing register: -6 i2c i2c-0: IMX I2C adapter registered s32g-siul2-pinctrl 4009c240.pinc /soc@0/pinctrl@4009c240/i2c2-pins/i2c2-grp0: could not parse node property s32g-siul2-pinctrl 4009c240.pinctrl: /soc@0/pinctrl@4009c240/i2c2-pins/i2c2-grp0: c node property i2c i2c-1: IMX I2C adapter registered s32g-siul2-pinctrl 4009c240.pinctrl: /soc@0/pinctrl@4009c240/i2c4-pins/i2c4-grp0: could not parse node prope pinctrl 4009c240.pinctrl: /soc@0/pinctrl@4009c240/i2c4-pins/i2c4-grp0: could not parse node property i2c i2c-2: IMX I2C adapter registered Fix this by initializing s32_pinctrl_desc with devm_kzalloc() instead of devm_kmalloc() in s32_pinctrl_probe(), which sets the previously uninitialized fields to zero.
CVE-2025-65834	Meltytech Shotcut 25.10.31 is vulnerable to Buffer Overflow. A memory access violation occurs when processing MLT project files with manipulated width and heigh By setting these values to extremely large numbers, the application attempts to allocate excessive memory during image processing, triggering a buffer overflow i mlt_image_fill_white function.
CVE-2025-68316	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Fix invalid probe error return value After DME Link Startup, the error return value i MIPI UniPro GenericErrorCode which can be 0 (SUCCESS) or 1 (FAILURE). Upon failure during driver probe, the error code 1 is propagated back to the driver probe f must return a negative value to indicate an error, but 1 is not negative, so the probe is considered to be successful even though it failed. Subsequently, removing t results in an oops because it is not in a valid state. This happens because none of the callers of ufshcd_init() expect a non-negative error code. Fix the return value documentation to match actual usage.
CVE-2025-68317	In the Linux kernel, the following vulnerability has been resolved: io_uring/zctx: check chained notif contexts Send zc only links ubuf_info for requests coming from context. There are some ambiguous syz reports, so let's check the assumption on notification completion.
CVE-2025-68318	In the Linux kernel, the following vulnerability has been resolved: clk: thead: th1520-ap: set all AXI clocks to CLK_IS_CRITICAL The AXI crossbar of TH1520 has no pr handling, which means gating AXI clocks can easily lead to bus timeout and thus system hang. Set all AXI clock gates to CLK_IS_CRITICAL. All these clock gates are default on system reset. In addition, convert all current CLK_IGNORE_UNUSED usage to CLK_IS_CRITICAL to prevent unwanted clock gating.
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: bpf: account for current allocated stack depth in widen_imprecise_scalars() The usage pattern for widen_imprecise_scalars() looks as follows: prev_st = find_prev_entry(env, ...); queued_st = push_stack(...); widen_imprecise_scalars(env, prev_st, queued_st); Whe an ancestor of the queued_st in the explored states tree. This ancestor is not guaranteed to have same allocated stack depth as queued_st. E.g. in the following ca

68208	for i in 1..2: foo(i) // same callsite, differnt param def foo(i): if i == 1: use 128 bytes of stack iterator based loop Here, for a second 'foo' call prev_st->allocated_stac while queued_st->allocated_stack is much smaller. widen_imprecise_scalars() needs to take this into account and avoid accessing bpf_verifier_state->frame[*]->st bounds.
CVE-2025-40354	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: increase max link count and fix link->enc NULL pointer access [why] 1.) dc->links[MAX_LINKS] array size smaller than actual requested. max_connector + max_dpia + 4 virtual = 14. increase from 12 to 14. 2.) hw_init() access null LINK_EN display_endpoint. (cherry picked from commit d7f5a61e1b04ed87b008c8d327649d184dc5bb45)
CVE-2025-68207	In the Linux kernel, the following vulnerability has been resolved: drm/xe/guc: Synchronize Dead CT worker with unbind Cancel and wait for any Dead CT worker to before continuing with device unbinding. Else the worker will end up using resources freed by the undind operation. (cherry picked from commit 492671339114e376aaa38626d637a2751cdef263)
CVE-2025-68206	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_ct: add seqadj extension for natted connections Sequence adjustment may be requi traffic with PASV/EPSV modes. due to need to re-write packet payload (IP, port) on the ftp control connection. This can require changes to the TCP length and expe ack_seq. The easiest way to reproduce this issue is with PASV mode. Example ruleset: table inet ftp_nat { ct helper ftp_helper { type "ftp" protocol tcp l3proto inet prerouting { type filter hook prerouting priority 0; policy accept; tcp dport 21 ct state new ct helper set "ftp_helper" } } table ip nat { chain prerouting { type nat h prerouting priority -100; policy accept; tcp dport 21 dnat ip prefix to ip daddr map { 192.168.100.1 : 192.168.13.2/32 } } chain postrouting { type nat hook postrou 100 ; policy accept; tcp sport 21 snat ip prefix to ip saddr map { 192.168.13.2 : 192.168.100.1/32 } } } Note that the ftp helper gets assigned *after* the dnat setu (nat after helper assign) is handled by an existing check in nf_nat_setup_info() and will not show the problem. Topoloy: +------------------+ +----------------------- 192.168.13.2 | <-> | NAT: 192.168.13.3, 192.168.100.1 | +------------------+ +----------------------+ | +----------------------+ | Client: 192.168.100.2 | +---------- changes do not work as expected in this case: Connected to 192.168.100.1. [..] ftp> epsv EPSV/EPRT on IPv4 off. ftp> ls 227 Entering passive mode (192,168,100, 421 Service not available, remote server has closed connection. Kernel logs: Missing nfct_seqadj_ext_add() setup call WARNING: CPU: 1 PID: 0 at net/netfilter/nf_conntrack_seqadj.c:41 [..] __nf_nat_mangle_tcp_packet+0x100/0x160 [nf_nat] nf_nat_ftp+0x142/0x280 [nf_nat_ftp] help+0x4d1/0x880 [nf_conntra nf_confirm+0x122/0x2e0 [nf_conntrack] nf_hook_slow+0x3c/0xb0 .. Fix this by adding the required extension when a conntrack helper is assigned to a connection binding.
CVE-2025-68205	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda/hdmi: Fix breakage at probing nvhdmi-mcp driver After restructuring and splitting the driver code, each HDMI codec driver contains the own build_controls and build_pcms ops. A copy-n-paste error put the wrong entries for nvhdmi-mcp driver; both b and build_pcms are swapped. Unfortunately both callbacks have the very same form, and the compiler didn't complain it, either. This resulted in a NULL dereferenc the PCM instance hasn't been initialized at calling the build_controls callback. Fix it by passing the proper entries.
CVE-2025-68204	In the Linux kernel, the following vulnerability has been resolved: pmdomain: arm: scmi: Fix genpd leak on provider registration failure If of_genpd_add_provider_o during probe, the previously created generic power domains are not removed, leading to a memory leak and potential kernel crash later in genpd_debug_add(). Ad handling to unwind the initialized domains before returning from probe to ensure all resources are correctly released on failure. Example crash trace observed with Unable to handle kernel paging request at virtual address ffffffffffffffc70 | CPU: 1 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.18.0-rc1 #405 PREEMPT | Hardware r LTD ARM Juno Development Platform/ARM Juno Development Platform | pstate: 00000005 (nzcv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) | pc : genpd_debug_add | lr : genpd_debug_init+0x74/0x98 | Call trace: | genpd_debug_add+0x2c/0x160 (P) | genpd_debug_init+0x74/0x98 | do_one_initcall+0xd0/0x2d8 | do_initcall_level | do_initcalls+0x60/0xa8 | do_basic_setup+0x28/0x40 | kernel_init_freeable+0xe8/0x170 | kernel_init+0x2c/0x140 | ret_from_fork+0x10/0x20
CVE-2025-68203	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix lock warning in amdgpu_userq_fence_driver_process Fix a potential deadlock ca inconsistent spinlock usage between interrupt and process contexts in the userq fence driver. The issue occurs when amdgpu_userq_fence_driver_process() is calle Interrupt context: gfx_v11_0_eop_irq() -> amdgpu_userq_fence_driver_process() - Process context: amdgpu_eviction_fence_suspend_worker() -> amdgpu_userq_fence_driver_force_completion() -> amdgpu_userq_fence_driver_process() In interrupt context, the spinlock was acquired without disabling interrup in {IN-HARDIRQ-W} state. When the same lock is acquired in process context, the kernel detects inconsistent locking since the process context acquisition would e interrupts while holding a lock previously acquired in interrupt context. Kernel log shows: [4039.310790] inconsistent {IN-HARDIRQ-W} -> {HARDIRQ-ON-W} usag 4039.310804] kworker/7:2/409 [HC0[0]:SC0[0]:HE1:SE1] takes: [4039.310818] ffff9284e1bed000 (&fence_drv->fence_list_lock){?...}-{3:3}, [4039.310993] {IN-H state was registered at: [4039.311004] lock_acquire+0xc6/0x300 [4039.311018] _raw_spin_lock+0x39/0x80 [4039.311031] amdgpu_userq_fence_driver_process.part.0+0x30/0x180 [amdgpu] [4039.311146] amdgpu_userq_fence_driver_process+0x17/0x30 [amdgpu] [4039.311257] gfx_v11_0_eop_irq+0x132/0x170 [amdgpu] Fix by using spin_lock_irqsave()/spin_unlock_irqrestore() to properly manage interrupt state regardless of calling conte picked from commit ded3ad780cf97a04927773c4600823b84f7f3cc2)
CVE-2025-68202	In the Linux kernel, the following vulnerability has been resolved: sched_ext: Fix unsafe locking in the scx_dump_state() For built with CONFIG_PREEMPT_RT=y kerr dump_lock will be converted sleepable spinlock and not disable-irq, so the following scenarios occur: inconsistent {IN-HARDIRQ-W} -> {HARDIRQ-ON-W} usage. irq [HC0[0]:SC0[0]:HE1:SE1] takes: (&rq->__lock){?...}-{2:2}, at: raw_spin_rq_lock_nested+0x2b/0x40 {IN-HARDIRQ-W} state was registered at: lock_acquire+0x1e1/ _raw_spin_lock_nested+0x42/0x80 raw_spin_rq_lock_nested+0x2b/0x40 sched_tick+0xae/0x7b0 update_process_times+0x14c/0x1b0 tick_periodic+0x62/0x1f0 tick_handle_periodic+0x48/0xf0 timer_interrupt+0x55/0x80 __handle_irq_event_percpu+0x20a/0x5c0 handle_irq_event_percpu+0x18/0xc0 handle_irq_event+0xb handle_level_irq+0x220/0x460 __common_interrupt+0xa2/0x1e0 common_interrupt+0xb0/0xd0 asm_common_interrupt+0x2b/0x40 _raw_spin_unlock_irqrestore+ __setup_irq+0xc34/0x1a30 request_threaded_irq+0x214/0x2f0 hpet_time_init+0x3e/0x60 x86_late_time_init+0x5b/0xb0 start_kernel+0x308/0x410 x86_64_start_reservations+0x1c/0x30 x86_64_start_kernel+0x96/0xa0 common_startup_64+0x13e/0x148 other info that might help us debug this: Possible unsaf scenario: CPU0 ---- lock(&rq->__lock); <Interrupt> lock(&rq->__lock); *** DEADLOCK *** stack backtrace: CPU: 0 UID: 0 PID: 27 Comm: irq_work/0 Call Trace: <TAS dump_stack_lvl+0x8c/0xd0 dump_stack+0x14/0x20 print_usage_bug+0x42e/0x690 mark_lock.part.44+0x867/0xa70 ? __pfx_mark_lock.part.44+0x10/0x10 ? string_nocheck+0x19c/0x310 ? number+0x739/0x9f0 ? __pfx_string_nocheck+0x10/0x10 ? __pfx_check_pointer+0x10/0x10 ? kvm_sched_clock_read+0x15/0x30 ? sched_clock_noinstr+0xd/0x20 ? local_clock_noinstr+0x1c/0xe0 __lock_acquire+0xc4b/0x62b0 ? __pfx_format_decode+0x10/0x10 ? __pfx_string+0x10/0x10 ? __pfx___lock_acquire+0x10/0x10 ? __pfx_vsnprintf+0x10/0x10 lock_acquire+0x1e1/0x510 ? raw_spin_rq_lock_nested+0x2b/0x40 ? __pfx_lock_acquire+0x10/0x10 dump_line+0x12e/0x270 ? raw_spin_rq_lock_nested+0x20/0x40 _raw_spin_lock_nested+0x42/0x80 ? raw_spin_rq_lock_nested+0x2b/0x40 raw_spin_rq_lock_neste scx_dump_state+0x3b3/0x1270 ? finish_task_switch+0x27e/0x840 scx_ops_error_irq_workfn+0x67/0x80 irq_work_single+0x113/0x260 irq_work_run_list.part.3+0 run_irq_workd+0x6b/0x90 ? __pfx_run_irq_workd+0x10/0x10 smpboot_thread_fn+0x529/0x870 ? __pfx_smpboot_thread_fn+0x10/0x10 kthread+0x305/0x3f0 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x40/0x70 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> This commit therefore use rq_lock_irqsav to replace rq_lock/unlock() in the scx_dump_state().
CVE-2025-68201	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: remove two invalid BUG_ON()s Those can be triggered trivially by userspace.
CVE-2025-68200	In the Linux kernel, the following vulnerability has been resolved: bpf: Add bpf_prog_run_data_pointers() syzbot found that cls_bpf_classify() is able to change tc_sk >drop_reason triggering a warning in sk_skb_reason_drop(). WARNING: CPU: 0 PID: 5965 at net/core/skbuff.c:1192 __sk_skb_reason_drop net/core/skbuff.c:1189 [ir WARNING: CPU: 0 PID: 5965 at net/core/skbuff.c:1192 sk_skb_reason_drop+0x76/0x170 net/core/skbuff.c:1214 struct tc_skb_cb has been added in commit ec624fe ("net/sched: Extend qdisc control block with tc control block"), which added a wrong interaction with db58ba459202 ("bpf: wire in data and data_end for cls_act_bp drop_reason was added later. Add bpf_prog_run_data_pointers() helper to save/restore the net_sched storage colliding with BPF data_meta/data_end.
	In the Linux kernel, the following vulnerability has been resolved: codetag: debug: handle existing CODETAG_EMPTY in mark_objexts_empty for slabobj_ext When alloc_slab_obj_exts() fails and then later succeeds in allocating a slab extension vector, it calls handle_failed_objexts_alloc() to mark all objects in the vector as emp all objects in this slab (slabA) will have their extensions set to CODETAG_EMPTY. Later on if this slabA is used to allocate a slabobj_ext vector for another slab (slabl with the slabB->obj_exts pointing to a slabobj_ext vector that itself has a non-NULL slabobj_ext equal to CODETAG_EMPTY. When slabB gets freed, free_slab_obj_ex to free slabB->obj_exts vector. free_slab_obj_exts() calls mark_objexts_empty(slabB->obj_exts) which will generate a warning because it expects slabobj_ext vecto NULL obj_ext, not CODETAG_EMPTY. Modify mark_objexts_empty() to skip the warning and setting the obj_ext value if it's already set to CODETAG_EMPTY. To quick

CVE-2025-68199	WARN, I modified the code from WARN_ON(slab_exts[offs].ref.ct) to BUG_ON(slab_exts[offs].ref.ct == 1); We then obtained this message: [21630.898561] ---------- [21630.898596] kernel BUG at mm/slub.c:2050! [21630.898611] Internal error: Oops - BUG: 00000000f2000800 [#1] SMP [21630.900372] Modules linked i isofs vfio_iommu_type1 vhost_vsock vfio vhost_net vmw_vsock_virtio_transport_common vhost tap vhost_iotlb iommufd vsock binfmt_misc nfsv3 nfs_acl nfs lockd g rds dns_resolver tun brd overlay ntfs3 exfat btrfs blake2b_generic xor xor_neon raid6_pq loop sctp ip6_udp_tunnel udp_tunnel nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 n nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject nft_ct nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 nf_tables rfkill ip_set sunrpc vfat fat jo sch_fq_codel nfnetlink virtio_gpu sr_mod cdrom drm_client_lib virtio_dma_buf drm_shmem_helper drm_kms_helper drm ghash_ce backlight virtio_net virtio_blk virti net_failover virtio_console failover virtio_mmio dm_mirror dm_region_hash dm_log dm_multipath dm_mod fuse i2c_dev virtio_pci virtio_pci_legacy_dev virtio_pci_m virtio virtio_ring autofs4 aes_neon_bs aes_ce_blk [last unloaded: hwpoison_inject] [21630.909177] CPU: 3 UID: 0 PID: 3787 Comm: kylin-process-m Kdump: loaded G W 6.18.0-rc1+ #74 PREEMPT(voluntary) [21630.910495] Tainted: [W]=WARN [21630.910867] Hardware name: QEMU KVM Virtual Machine, BIOS unk [21630.911625] pstate: 80400005 (Nzcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [21630.912392] pc : __free_slab+0x228/0x250 [21630.912868] lr : __free_slab+0x18c/0x250[21630.913334] sp : ffff8000a02f73e0 [21630.913830] x29: ffff8000a02f73e0 x28: ffffffdffc43fc800 x27: ffff0000c0011c40 [21630.91467 ffff0000c000cac0 x25: ffff00010fe5e5f0 x24: ffff000102199b40 [21630.915469] x23: 0000000000000003 x22: 0000000000000003 x21: ffff0000c0011c40 [21630 ffffffdffc4086600 x19: ffffffdffc43fc800 x18: 0000000000000000 [21630.917048] x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 [2163 x14: 0000000000000000 x13: 0000000000000000 x12: ffff70001405ee66 [21630.918640] x11: 1ffff0001405ee65 x10: ffff70001405ee65 x9 : ffff800080a295dc [21630.919442] x8 : ffff8000a02f7330 x7 : 0000000000000000 x6 : 0000000000003000 [21630.920232] x5 : 0000000024924925 x4 : 0000000000000001 x3 : 0000000000000007 [21630.921021] x2 : 0000000000001b40 x1 : 000000000000001f x0 : 0000000000000001 [21630.921810] Call trace: [21630.922130] __free_slab+0x228/0x250 (P) [21630.922669] free_slab+0x38/0x118 [21630.923079] free_to_partial_list+0x1d4/0x340 [21630.923591] __slab_free+0x24c/0x34 [21630.924024] ___cache_free+0xf0/0x110 [21630.924468] qlist_free_all+0x78/0x130 [21630.924922] kasan_quarantine_reduce+0x11 ---truncated---
CVE-2025-68198	In the Linux kernel, the following vulnerability has been resolved: crash: fix crashkernel resource shrink When crashkernel is configured with a high reservation, shr value below the low crashkernel reservation causes two issues: 1. Invalid crashkernel resource objects 2. Kernel crash if crashkernel shrinking is done twice For exa crashkernel=200M,high, the kernel reserves 200MB of high memory and some default low memory (say 256MB). The reservation appears as: cat /proc/iomem | gre af000000-beffffff : Crash kernel 433000000-43f7fffff : Crash kernel If crashkernel is then shrunk to 50MB (echo 52428800 > /sys/kernel/kexec_crash_size), /proc/io shows 256MB reserved: af000000-beffffff : Crash kernel Instead, it should show 50MB: af000000-b21fffff : Crash kernel Further shrinking crashkernel to 40MB caus crash with the following trace (x86): BUG: kernel NULL pointer dereference, address: 0000000000000038 PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI <snip Trace: <TASK> ? __die_body.cold+0x19/0x27 ? page_fault_oops+0x15a/0x2f0 ? search_module_extables+0x19/0x60 ? search_bpf_extables+0x5f/0x80 ? exc_page_fault+0x7e/0x180 ? asm_exc_page_fault+0x26/0x30 ? __release_resource+0xd/0xb0 release_resource+0x26/0x40 __crash_shrink_memory+0xe5/0x110 crash_shrink_memory+0x12a/0x190 kexec_crash_size_store+0x41/0x80 kernfs_fop_write_iter+0x141/0x1f0 vfs_write+0x294/0x460 ksys_write+0x6d/0xf0 <snip.. happens because __crash_shrink_memory()/kernel/crash_core.c incorrectly updates the crashk_res resource object even when crashk_low_res should be updated. F ensuring the correct crashkernel resource object is updated when shrinking crashkernel memory.
CVE-2025-68197	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Fix null pointer dereference in bnxt_bs_trace_check_wrap() With older FW, we may get t ASYNC_EVENT_CMPL_EVENT_ID_DBG_BUF_PRODUCER for FW trace data type that has not been initialized. This will result in a crash in bnxt_bs_trace_type_wrap(). A check for a valid magic_byte pointer before proceeding.
CVE-2025-68196	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Cache streams targeting link when performing LT automation [WHY] Last LT au update can cause crash by referencing current_state and calling into dc_update_planes_and_stream which may clobber current_state. [HOW] Cache relevant strear and iterate through them instead of relying on the current_state.
CVE-2025-68195	In the Linux kernel, the following vulnerability has been resolved: x86/CPU/AMD: Add missing terminator for zen5_rdseed_microcode Running x86_match_min_micr on a Zen5 CPU trips up KASAN for an out of bounds access.
CVE-2025-68194	In the Linux kernel, the following vulnerability has been resolved: media: imon: make send_packet() more robust syzbot is reporting that imon has three problems hung tasks due to forever holding device lock [1]. First problem is that when usb_rx_callback_intf0() once got -EPROTO error after ictx->dev_present_intf0 became usb_rx_callback_intf0() resubmits urb after printk(), and resubmitted urb causes usb_rx_callback_intf0() to again get -EPROTO error. This results in printk() flooding Alan Stern commented [2] that In theory it's okay to resubmit _if_ the driver has a robust error-recovery scheme (such as giving up after some fixed limit on the nu or after some fixed time has elapsed, perhaps with a time delay to prevent a flood of errors). Most drivers don't bother to do this; they simply give up right away. T them more vulnerable to short-term noise interference during USB transfers, but in reality such interference is quite rare. There's nothing really wrong with giving u but imon has a poor error-recovery scheme which just retries forever; this behavior should be fixed. Since I'm not sure whether it is safe for imon users to give up u code, this patch takes care of only union of error codes chosen from modules in drivers/media/rc/ directory which handle -EPROTO error (i.e. ir_toy, mceusb and igo Second problem is that when usb_rx_callback_intf0() once got -EPROTO error before ictx->dev_present_intf0 becomes true, usb_rx_callback_intf0() always resubmi commit 8791d63af0cf ("[media] imon: don't wedge hardware after early callbacks"). Move the ictx->dev_present_intf0 test introduced by commit 6f6b90c9231a (" don't parse scancodes until intf configured") to immediately before imon_incoming_packet(), or the first problem explained above happens without printk() flooding task). Third problem is that when usb_rx_callback_intf0() is not called for some reason (e.g. flaky hardware; the reproducer for this problem sometimes prevents usb_rx_callback_intf0() from being called), wait_for_completion_interruptible() in send_packet() never returns (i.e. hung task). As a workaround for such situation, c send_packet() to wait for completion with timeout of 10 seconds.
CVE-2025-68307	In the Linux kernel, the following vulnerability has been resolved: can: gs_usb: gs_usb_xmit_callback(): fix handling of failed transmitted URBs The driver lacks the failed transfers of URBs. This reduces the number of available URBs per error by 1. This leads to reduced performance and ultimately to a complete stop of the tran the sending of a bulk URB fails do proper cleanup: - increase netdev stats - mark the echo_sbk as free - free the driver's context and do accounting - wake the send
CVE-2025-68219	In the Linux kernel, the following vulnerability has been resolved: cifs: fix memory leak in smb3_fs_context_parse_param error path Add proper cleanup of ctx->sou >source to the cifs_parse_mount_err error handler. This ensures that memory allocated for the source strings is correctly freed on all error paths, matching the cle performed in the success path by smb3_cleanup_fs_context_contents(). Pointers are also set to NULL after freeing to prevent potential double-free issues. This cha memory leak originally detected by syzbot. The leak occurred when processing Opt_source mount options if an error happened after ctx->source and fc->source w successfully allocated but before the function completed. The specific leak sequence was: 1. ctx->source = smb3_fs_context_fullpath(ctx, '/') allocates memory 2. f kstrdup(ctx->source, GFP_KERNEL) allocates more memory 3. A subsequent error jumps to cifs_parse_mount_err 4. The old error handler freed passwords but not t strings, causing the memory to leak. This issue was not addressed by commit e8c73eb7db0a ("cifs: client: fix memory leak in smb3_fs_context_parse_param"), whi leaks from repeated fsconfig() calls but not this error path. Patch updated with minor change suggested by kernel test robot
CVE-2025-68218	In the Linux kernel, the following vulnerability has been resolved: nvme-multipath: fix lockdep WARN due to partition scan work Blktests test cases nvme/014, 057 occasionally due to a lockdep WARN. As reported in the Closes tag URL, the WARN indicates that a deadlock can happen due to the dependency among disk->oper kblockd workqueue completion and partition_scan_work completion. To avoid the lockdep WARN and the potential deadlock, cut the dependency by running the partition_scan_work not by kblockd workqueue but by nvme_wq.
CVE-2025-68306	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btusb: mediatek: Fix kernel crash when releasing mtk iso interface When performing r encountering abnormal card drop issues that lead to a kernel crash, it is necessary to perform a null check before releasing resources to avoid attempting to releas pointer. <4>[29.158070] Hardware name: Google Quigon sku196612/196613 board (DT) <4>[29.158076] Workqueue: hci0 hci_cmd_sync_work [bluetooth] <4>[pstate: 20400009 (nzCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) <4>[29.158162] pc : klist_remove+0x90/0x158 <4>[29.158174] lr : klist_remove+0x88/0x1 29.158180] sp : ffffffc0846b3c00 <4>[29.158185] pmr_save: 000000e0 <4>[29.158188] x29: ffffffc0846b3c30 x28: ffffff80cd31f880 x27: ffffff80c1bdc058 <4>[x26: dead000000000100 x25: ffffffdbdc624ea3 x24: ffffff80c1bdc4c0 <4>[29.158209] x23: ffffffdbdc62a3e6 x22: ffffff80c6c07000 x21: ffffffdbdc829290 <4>[29 0000000000000000 x19: ffffff80cd3e0648 x18: 000000031ec97781 <4>[29.158229] x17: ffffff80c1bdc4a8 x16: ffffffdc10576548 x15: ffffff80c1180428 <4>[29. 0000000000000000 x13: 000000000000e380 x12: 0000000000000018 <4>[29.158248] x11: ffffff80c2a7fd10 x10: 0000000000000000 x9 : 0000000100000000 29.158257] x8 : 0000000000000000 x7 : 7f7f7f7f7f7f7f7f x6 : 2d7223ff6364626d <4>[29.158266] x5 : 0000008000000000 x4 : 0000000000000020 x3 : 2e7325(<4>[29.158275] x2 : ffffffdc11afeff8 x1 : 0000000000000000 x0 : ffffffdc11be4d0c <4>[29.158285] Call trace: <4>[29.158290] klist_remove+0x90/0x158 <4>

	device_release_driver_internal+0x20c/0x268 <4>[29.158308] device_release_driver+0x1c/0x30 <4>[29.158316] usb_driver_release_interface+0x70/0x88 <4>[btusb_mtk_release_iso_intf+0x68/0xd8 [btusb (HASH:e8b6 5)] <4>[29.158347] btusb_mtk_reset+0x5c/0x480 [btusb (HASH:e8b6 5)] <4>[29.158361] hci_cmd_sync_work+0x10c/0x188 [bluetooth (HASH:a4fa 6)] <4>[29.158430] process_scheduled_works+0x258/0x4e8 <4>[29.158441] worker_thread+0x300/0 29.158448] kthread+0x108/0x1d0 <4>[29.158455] ret_from_fork+0x10/0x20 <0>[29.158467] Code: 91343000 940139d1 f9400268 927ff914 (f9401297) <4>[[end trace 0000000000000000]--- <0>[29.167129] Kernel panic - not syncing: Oops: Fatal exception <2>[29.167144] SMP: stopping secondary CPUs <4>[29.1 ----[cut here]----------
CVE-2025-68292	In the Linux kernel, the following vulnerability has been resolved: mm/memfd: fix information leak in hugetlb folios When allocating hugetlb folios for memfd, three steps are missing: 1. Folios are not zeroed, leading to kernel memory disclosure to userspace 2. Folios are not marked uptodate before adding to page cache 3. hugetlb_fault_mutex is not taken before hugetlb_add_to_page_cache() The memfd allocation path bypasses the normal page fault handler (hugetlb_no_page) which handle all of these initialization steps. This is problematic especially for udmabuf use cases where folios are pinned and directly accessed by userspace via DMA. Fi the initialization pattern used in hugetlb_no_page(): - Zero the folio using folio_zero_user() which is optimized for huge pages - Mark it uptodate with folio_mark_upt hugetlb_fault_mutex before adding to page cache to prevent races The folio_zero_user() change also fixes a potential security issue where uninitialized kernel mem disclosed to userspace through read() or mmap() operations on the memfd.
CVE-2025-68290	In the Linux kernel, the following vulnerability has been resolved: most: usb: fix double free on late probe failure The MOST subsystem has a non-standard registrat which frees the interface on registration failures and on deregistration. This unsurprisingly leads to bugs in the MOST drivers, and a couple of recent changes turne underflow and use-after-free in the USB driver into several double free and a use-after-free on late probe failures.
CVE-2025-68289	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_eem: Fix memory leak in eem_unwrap The existing code did not handle the failure usb_ep_queue in the command path, potentially leading to memory leaks. Improve error handling to free all allocated resources on usb_ep_queue failure. This patc use goto logic for error handling, as the existing error handling is complex and not easily adaptable to auto-cleanup helpers. kmemleak results: unreferenced objec 0xffffff895a512300 (size 240): backtrace: slab_post_alloc_hook+0xbc/0x3a4 kmem_cache_alloc+0x1b4/0x358 skb_clone+0x90/0xd8 eem_unwrap+0x1cc/0x36c u object 0xffffff8a157f4000 (size 256): backtrace: slab_post_alloc_hook+0xbc/0x3a4 __kmem_cache_alloc_node+0x1b4/0x2dc kmalloc_trace+0x48/0x140 dwc3_gadget_ep_alloc_request+0x58/0x11c usb_ep_alloc_request+0x40/0xe4 eem_unwrap+0x204/0x36c unreferenced object 0xffffff8aadbaac00 (size 128): back slab_post_alloc_hook+0xbc/0x3a4 __kmem_cache_alloc_node+0x1b4/0x2dc __kmalloc+0x64/0x1a8 eem_unwrap+0x218/0x36c unreferenced object 0xffffff89ccef backtrace: slab_post_alloc_hook+0xbc/0x3a4 __kmem_cache_alloc_node+0x1b4/0x2dc kmalloc_trace+0x48/0x140 eem_unwrap+0x238/0x36c
CVE-2025-68288	In the Linux kernel, the following vulnerability has been resolved: usb: storage: Fix memory leak in USB bulk transport A kernel memory leak was identified by the ' test from Linux Test Project (LTP). The following bytes were mainly observed: 0x53425355. When USB storage devices incorrectly skip the data phase with status c extracts/validates the CSW from the sg buffer, but fails to clear it afterwards. This leaves status protocol data in srb's transfer buffer, such as the US_BULK_CS_SIGN signature observed here. Thus, this can lead to USB protocols leaks to user space through SCSI generic (/dev/sg*) interfaces, such as the one seen here when the L requested 512 KiB. Fix the leak by zeroing the CSW data in srb's transfer buffer immediately after the validation of devices that skip data phase. Note: Differently f 2018-1000204, which fixed a big leak by zero- ing pages at allocation time, this leak occurs after allocation, when USB protocol data is written to already-allocated
CVE-2025-68287	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: Fix race condition between concurrent dwc3_remove_requests() call paths This patch race condition caused by unsynchronized execution of multiple call paths invoking `dwc3_remove_requests()`, leading to premature freeing of USB requests and su crashes. Three distinct execution paths interact with `dwc3_remove_requests()`: Path 1: Triggered via `dwc3_gadget_reset_interrupt()` during USB reset handling. includes: - `dwc3_ep0_reset_state()` - `dwc3_ep0_stall_and_restart()` - `dwc3_ep0_out_start()` - `dwc3_remove_requests()` - `dwc3_gadget_del_and_unmap_reque Also initiated from `dwc3_gadget_reset_interrupt()`, but through `dwc3_stop_active_transfers()`. The call stack includes: - `dwc3_stop_active_transfers()` - `dwc3_remove_requests()` - `dwc3_gadget_del_and_unmap_request()` Path 3: Occurs independently during `adb root` execution, which triggers USB function unb operations. The sequence includes: - `gserial_disconnect()` - `usb_ep_disable()` - `dwc3_gadget_ep_disable()` - `dwc3_remove_requests()` with `-ESHUTDOWN` st operates asynchronously and lacks synchronization with Paths 1 and 2. When Path 3 completes, it disables endpoints and frees 'out' requests. If Paths 1 or 2 are st these requests, accessing freed memory leads to a crash due to use-after-free conditions. To fix this added check for request completion and skip processing if alre completed and added the request status for ep0 while queue.
CVE-2025-68293	In the Linux kernel, the following vulnerability has been resolved: mm/huge_memory: fix NULL pointer deference when splitting folio Commit c010d47f107f ("mm: t page to any lower order pages") introduced an early check on the folio's order via mapping->flags before proceeding with the split work. This check introduced a b shmem folios in the swap cache and truncated folios, the mapping pointer can be NULL. Accessing mapping->flags in this state leads directly to a NULL pointer der commit fixes the issue by moving the check for mapping != NULL before any attempt to access mapping->flags.
CVE-2025-68215	In the Linux kernel, the following vulnerability has been resolved: ice: fix PTP cleanup on driver removal in error path Improve the cleanup on releasing PTP resourc path. The error case might happen either at the driver probe and PTP feature initialization or on PTP restart (errors in reset handling, NVM update etc). In both case PTP cleanup (ice_ptp_cleanup_pf function) and 'ps_lock' mutex deinitialization were missed. Additionally, ptp clock was not unregistered in the latter case. Keep PTI 'uninitialized' on init to distinguish between error scenarios and to avoid resource release duplication at driver removal. The consequence of missing ice_ptp_cleanu the following call trace dumped when ice_adapter object is freed (port list is not empty, as it is required at this stage): [T93022] ----------[cut here]---------- [T93 WARNING: CPU: 10 PID: 93022 at ice/ice_adapter.c:67 ice_adapter_put+0xef/0x100 [ice] ... [T93022] RIP: 0010:ice_adapter_put+0xef/0x100 [ice] ... [T93022] Call T93022] <TASK> [T93022] ? ice_adapter_put+0xef/0x100 [ice 33d2647ad4f6d866d41eefff1806df37c68aef0c] [T93022] ? __warn.cold+0xb0/0x10e [T93022] ? ice_adapter_put+0xef/0x100 [ice 33d2647ad4f6d866d41eefff1806df37c68aef0c] [T93022] ? report_bug+0xd8/0x150 [T93022] ? handle_bug+0xe9/0x110 [T930 exc_invalid_op+0x17/0x70 [T93022] ? asm_exc_invalid_op+0x1a/0x20 [T93022] ? ice_adapter_put+0xef/0x100 [ice 33d2647ad4f6d866d41eefff1806df37c68aef0 pci_device_remove+0x42/0xb0 [T93022] device_release_driver_internal+0x19f/0x200 [T93022] driver_detach+0x48/0x90 [T93022] bus_remove_driver+0x70/0x pci_unregister_driver+0x42/0xb0 [T93022] ice_module_exit+0x10/0xdb0 [ice 33d2647ad4f6d866d41eefff1806df37c68aef0c] ... [T93022] ---[end trace 0000000 [T93022] ice: module unloaded
CVE-2025-68294	In the Linux kernel, the following vulnerability has been resolved: io_uring/net: ensure vectored buffer node import is tied to notification When support for vectored buffers was added, the import itself is using 'req' rather than the notification io_kiocb, sr->notif. For non-vectored imports, sr->notif is correctly used. This is import lifetime of the two may be different. Use the correct io_kiocb for the vectored buffer import.
CVE-2025-68286	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check NULL before accessing [WHAT] IGT kms_cursor_legacy's long-nonblockin cursor-atomic fails with NULL pointer dereference. This can be reproduced with both an eDP panel and a DP monitors connected. BUG: kernel NULL pointer derefer 0000000000000000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] SMP NOPTI CPU: PID: 2960 Comm: kms_cursor_lega Not tainted 6.16.0-99-custom #8 PREEMPT(voluntary) Hardware name: AMD ..... RIP: 0010:dc_stream_get_scanoutpos+0x34/([amdgpu] Code: 57 4d 89 c7 41 56 49 89 ce 41 55 49 89 d5 41 54 49 89 fc 53 48 83 ec 18 48 8b 87 a0 64 00 00 48 89 75 d0 48 c7 c6 e0 41 30 c2 <48> 8b 38 48 00 00 e8 8d d7 fd ff 31 c0 48 81 c3 e0 02 RSP: 0018:ffffd0f3c2bd7608 EFLAGS: 00010292 RAX: 0000000000000000 RBX: 0000000000000000 RCX: ffffd0f3c2bd76 ffffd0f3c2bd7664 RSI: ffffffffc23041e0 RDI: ffff8b32494b8000 RBP: ffffd0f3c2bd7648 R08: ffffd0f3c2bd766c R09: ffffd0f3c2bd7760 R10: ffffd0f3c2bd7820 R11: 0000000000000000 R12: ffff8b32494b8000 R13: ffffd0f3c2bd7664 R14: ffffd0f3c2bd7668 R15: ffffd0f3c2bd766c FS: 000071f631b68700(0000) GS:ffff8b399f1140(knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 00000001b8105000 CR4: 0000000000f50ef0 PKR Call Trace: <TASK> dm_crtc_get_scanoutpos+0xd7/0x180 [amdgpu] amdgpu_display_get_crtc_scanoutpos+0x86/0x1c0 [amdgpu] ? __pfx_amdgpu_crtc_get_scanout_position+0x10/0x10[amdgpu] amdgpu_crtc_get_scanout_position+0x27/0x50 [amdgpu] drm_crtc_vblank_helper_get_vblank_timestamp_internal+0xf7/0x400 drm_crtc_vblank_helper_get_vblank_timestamp+0x1c/0x30 drm_crtc_get_last_vbltimestamp+ drm_crtc_next_vblank_start+0x45/0xa0 drm_atomic_helper_wait_for_fences+0x81/0x1f0 ... (cherry picked from commit 621e55f1919640acab25383362b96e65f2b
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix memory leak in cifs_construct_tcon() When having a multiuser mount with domain and using cifscreds, cifs_set_cifscreds() will end up setting @ctx->domainname, so it needs to be freed before leaving cifs_construct_tcon(). This fixes the following reported by kmemleak: mount.cifs //srv/share /mnt -o domain=ZELDA,multiuser,... su - testuser cifscreds add -d ZELDA -u testuser ... ls /mnt/1 ... umount /mnt ech /sys/kernel/debug/kmemleak cat /sys/kernel/debug/kmemleak unreferenced object 0xffff8881203c3f08 (size 8): comm "ls", pid 5060, jiffies 4307222943 hex dump

68295	bytes): 5a 45 4c 44 41 00 cc cc ZELDA... backtrace (crc d109a8cf): __kmalloc_node_track_caller_noprof+0x572/0x710 kstrdup+0x3a/0x70 cifs_sb_tlink+0x1209/0x cifs_get_fattr+0xe1/0xf50 [cifs] cifs_get_inode_info+0xb5/0x240 [cifs] cifs_revalidate_dentry_attr+0x2d1/0x470 [cifs] cifs_getattr+0x28e/0x450 [cifs] vfs_getattr_nosec+0x126/0x180 vfs_statx+0xf6/0x220 do_statx+0xab/0x110 __x64_sys_statx+0xd5/0x130 do_syscall_64+0xbb/0x380 entry_SYSCALL_64_after_hwframe+0x77/0x7f
CVE-2025-68214	In the Linux kernel, the following vulnerability has been resolved: timers: Fix NULL function pointer race in timer_shutdown_sync() There is a race condition betwee timer_shutdown_sync() and timer expiration that can lead to hitting a WARN_ON in expire_timers(). The issue occurs when timer_shutdown_sync() clears the timer NULL while the timer is still running on another CPU. The race scenario looks like this: CPU0 CPU1 <SOFTIRQ> lock_timer_base() expire_timers() base->running_tim unlock_timer_base() [call_timer_fn enter] mod_timer() ... timer_shutdown_sync() lock_timer_base() // For now, will not detach the timer but only clear its function to (base->running_timer != timer) ret = detach_if_pending(timer, base, true); if (shutdown) timer->function = NULL; unlock_timer_base() [call_timer_fn exit] lock_tim base->running_timer = NULL; unlock_timer_base() ... // Now timer is pending while its function set to NULL. // next timer trigger <SOFTIRQ> expire_timers() WARN_ON_ONCE(!fn) // hit ... lock_timer_base() // Now timer will detach if (base->running_timer != timer) ret = detach_if_pending(timer, base, true); if (shutdown) >function = NULL; unlock_timer_base() The problem is that timer_shutdown_sync() clears the timer function regardless of whether the timer is currently running. T a pending timer with a NULL function pointer, which triggers the WARN_ON_ONCE(!fn) check in expire_timers(). Fix this by only clearing the timer function when ac detaching the timer. If the timer is running, leave the function pointer intact, which is safe because the timer will be properly detached when it finishes running.
CVE-2025-68213	In the Linux kernel, the following vulnerability has been resolved: idpf: fix possible vport_config NULL pointer deref in remove Attempting to remove the driver will in cases where the vport failed to initialize. Following trace is from an instance where the driver failed during an attempt to create a VF: [1661.543624] idpf 0000:8 Device HW Reset initiated [1722.923726] idpf 0000:84:00.7: Transaction timed-out (op:1 cookie:2900 vc_op:1 salt:29 timeout:60000ms) [1723.353263] BUG: ker pointer dereference, address: 0000000000000028 ... [1723.358472] RIP: 0010:idpf_remove+0x11c/0x200 [idpf] ... [1723.364973] Call Trace: [1723.365475] <TA 1723.365972] pci_device_remove+0x42/0xb0 [1723.366481] device_release_driver_internal+0x1a9/0x210 [1723.366987] pci_stop_bus_device+0x6d/0x90 [172 pci_stop_and_remove_bus_device+0x12/0x20 [1723.367971] pci_iov_remove_virtfn+0xbd/0x120 [1723.368309] sriov_disable+0x34/0xe0 [1723.368643] idpf_sriov_configure+0x58/0x140 [idpf] [1723.368982] sriov_numvfs_store+0xda/0x1c0 Avoid the NULL pointer dereference by adding NULL pointer check for vpo before freeing user_config.q_coalesce.
CVE-2025-68296	In the Linux kernel, the following vulnerability has been resolved: drm, fbcon, vga_switcheroo: Avoid race condition in fbcon setup Protect vga_switcheroo_client_fb console lock. Avoids OOB access in fbcon_remap_all(). Without holding the console lock the call races with switching outputs. VGA switcheroo calls fbcon_remap_al switching clients. The fbcon function uses struct fb_info.node, which is set by register_framebuffer(). As the fb-helper code currently sets up VGA switcheroo before the framebuffer, the value of node is -1 and therefore not a legal value. For example, fbcon uses the value within set_con2fb_map() [1] as an index into an array. M vga_switcheroo_client_fb_set() after register_framebuffer() can result in VGA switching that does not switch fbcon correctly. Therefore move vga_switcheroo_client_ fbcon_fb_registered(), which already holds the console lock. Fbdev calls fbcon_fb_registered() from within register_framebuffer(). Serializes the helper with VGA swi to fbcon_remap_all(). Although vga_switcheroo_client_fb_set() takes an instance of struct fb_info as parameter, it really only needs the contained fbcon state. Movi fbcon initialization is therefore cleaner than before. Only amdgpu, i915, nouveau and radeon support vga_switcheroo. For all other drivers, this change does nothin
CVE-2025-68297	In the Linux kernel, the following vulnerability has been resolved: ceph: fix crash in process_v2_sparse_read() for encrypted directories The crash in process_v2_spa fscrypt-encrypted directories has been reported. Issue takes place for Ceph msgr2 protocol in secure mode. It can be reproduced by the steps: sudo mount -t ceph /mnt/cephfs/ -o name=admin,fs=cephfs,ms_mode=secure (1) mkdir /mnt/cephfs/fscrypt-test-3 (2) cp area_decrypted.tar /mnt/cephfs/fscrypt-test-3 (3) fscrypt encr source=raw_key --key=./my.key /mnt/cephfs/fscrypt-test-3 (4) fscrypt lock /mnt/cephfs/fscrypt-test-3 (5) fscrypt unlock --key=my.key /mnt/cephfs/fscrypt-test-3 (6 /mnt/cephfs/fscrypt-test-3/area_decrypted.tar (7) Issue has been triggered [408.072247] ------------[cut here]------------ [408.072251] WARNING: CPU: 1 PID: 392 at net/ceph/messenger_v2.c:865 ceph_con_v2_try_read+0x4b39/0x72f0 [408.072267] Modules linked in: intel_rapl_msr intel_rapl_common intel_uncore_frequency_c intel_pmc_core pmt_telemetry pmt_discovery pmt_class intel_pmc_ssram_telemetry intel_vsec kvm_intel joydev kvm irqbypass polyval_clmulni ghash_clmulni_inte rapl input_leds psmouse serio_raw i2c_piix4 vga16fb bochs vgastate i2c_smbus floppy mac_hid qemu_fw_cfg pata_acpi sch_fq_codel rbd msr parport_pc ppdev lp p efi_pstore [408.072304] CPU: 1 UID: 0 PID: 392 Comm: kworker/1:3 Not tainted 6.17.0-rc7+ [408.072307] Hardware name: QEMU Standard PC (i440FX + PIIX, 19 1.17.0-5.fc42 04/01/2014 [408.072310] Workqueue: ceph-msgr ceph_con_workfn [408.072314] RIP: 0010:ceph_con_v2_try_read+0x4b39/0x72f0 [408.072317] C f0 d4 ae 50 31 d2 48 c7 c6 60 27 d5 ae 48 c7 c7 f8 8e 6f b0 68 60 38 d5 ae e8 00 47 61 fe 48 83 c4 18 e9 ac fc ff ff <0f> 0b e9 06 fe ff ff 4c 8b 9d 98 fd ff ff 0f 84 85 [408.072319] RSP: 0018:ffff88811c3e7a30 EFLAGS: 00010246 [408.072322] RAX: ffffed1024874c6f RBX: ffffea00042c2b40 RCX: 0000000000000f38 [408.07 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 [408.072325] RBP: ffff88811c3e7ca8 R08: 0000000000000000 R09: 00000000000000c8 [R10: 00000000000000c8 R11: 0000000000000000 R12: 00000000000000c8 [408.072327] R13: dfffffc0000000000 R14: ffff8881243a6030 R15: 0000000000000030 408.072329] FS: 0000000000000000(0000) GS:ffff88823eadf000(0000) knlGS:0000000000000000 [408.072331] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000800 408.072332] CR2: 000000c0003c6000 CR3: 000000010c106005 CR4: 0000000000772ef0 [408.072336] PKRU: 55555554 [408.072337] Call Trace: [408.072338] 408.072340] ? sched_clock_noinstr+0x9/0x10 [408.072344] ? __pfx_ceph_con_v2_try_read+0x10/0x10 [408.072347] ? _raw_spin_unlock+0xe/0x40 [408.072349 finish_task_switch.isra.0+0x15d/0x830 [408.072353] ? __kasan_check_write+0x14/0x30 [408.072357] ? mutex_lock+0x84/0xe0 [408.072359] ? __pfx_mutex_loc [408.072361] ceph_con_workfn+0x27e/0x10e0 [408.072364] ? metric_delayed_work+0x311/0x2c50 [408.072367] process_one_work+0x611/0xe20 [408.07237 __kasan_check_write+0x14/0x30 [408.072373] worker_thread+0x7e3/0x1580 [408.072375] ? __pfx__raw_spin_lock_irqsave+0x10/0x10 [408.072378] ? __pfx_worker_thread+0x10/0x10 [408.072381] kthread+0x381/0x7a0 [408.072383] ? __pfx__raw_spin_lock_irq+0x10/0x10 [408.072385] ? __pfx_kthread+0x10/ 408.072387] ? __kasan_check_write+0x14/0x30 [408.072389] ? recalc_sigpending+0x160/0x220 [408.072392] ? _raw_spin_unlock_irq+0xe/0x50 [408.072394] ? calculate_sigpending+0x78/0xb0 [408.072395] ? __pfx_kthread+0x10/0x10 [408.072397] ret_from_fork+0x2b6/0x380 [408.072400] ? __pfx_kthread+0x10/0x10 408.072402] ret_from_fork_asm+0x1a/0x30 [408.072406] </TASK> [408.072407] ---[end trace 0000000000000000]--- [408.072418] Oops: general protection f for non-canonical address 0xdffffc00000000 ---truncated---
CVE-2025-68298	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btusb: mediatek: Avoid btusb_mtk_claim_iso_intf() NULL deref In btusb_mtk_setup(), w `btmtk_data->isopkt_intf` to: usb_ifnum_to_if(data->udev, MTK_ISO_IFNUM) That function can return NULL in some cases. Even when it returns NULL, though, we s call btusb_mtk_claim_iso_intf(). As of commit e9087e828827 ("Bluetooth: btusb: mediatek: Add locks for usb_driver_claim_interface()"), calling btusb_mtk_claim_iso `btmtk_data->isopkt_intf` is NULL will cause a crash because we'll end up passing a bad pointer to device_lock(). Prior to that commit we'd pass the NULL pointer usb_driver_claim_interface() which would detect it and return an error, which was handled. Resolve the crash in btusb_mtk_claim_iso_intf() by adding a NULL check the function. This makes the code handle a NULL `btmtk_data->isopkt_intf` the same way it did before the problematic commit (just with a slight change to the err printed).
CVE-2025-50398	Mercury D196G d196gv1-cn-up_2020-01-09_11.21.44 is vulnerable to Buffer Overflow in the function sub_404CAEDC via the parameter fac_password.
CVE-2025-68299	In the Linux kernel, the following vulnerability has been resolved: afs: Fix delayed allocation of a cell's anonymous key The allocation of a cell's anonymous key is d background thread along with other cell setup such as doing a DNS upcall. In the reported bug, this is triggered by afs_parse_source() parsing the device name giv and calling afs_lookup_cell() with the name of the cell. The normal key lookup then tries to use the key description on the anonymous authentication key as the ref request_key() - but it may not yet be set and so an oops can happen. This has been made more likely to happen by the fix for dynamic lookup failure. Fix this by fir a reference name and attaching it to the afs_cell record when the record is created. It can share the memory allocation with the cell name (unfortunately it can't ju cell name by prepending it with "afs@" as the cell name already has a '.' prepended for other purposes). This reference name is then passed to request_key(). Secc anon key is now allocated on demand at the point a key is requested in afs_request_key() if it is not already allocated. A mutex is used to prevent multiple allocatic Thirdly, make afs_request_key_rcu() return NULL if the anonymous key isn't yet allocated (if we need it) and then the caller can return -ECHILD to drop out of RCU- afs_request_key() can be called. Note that the anonymous key is kind of necessary to make the key lookup cache work as that doesn't currently cache a negative l probably worth some investigation to see if NULL can be used instead.
CVE-2025-68300	In the Linux kernel, the following vulnerability has been resolved: fs/namespace: fix reference leak in grab_requested_mnt_ns lookup_mnt_ns() already takes a refe mnt_ns. grab_requested_mnt_ns() doesn't need to take an extra reference.

CVE-2025-68216	In the Linux kernel, the following vulnerability has been resolved: LoongArch: BPF: Disable trampoline for kernel module function trace The current LoongArch BPF implementation is incompatible with tracing functions in kernel modules. This causes several severe and user-visible problems: * The `bpf_selftests/module_attach consistently. * Kernel lockup when a BPF program is attached to a module function [1]. * Critical kernel modules like WireGuard experience traffic disruption when are traced with fentry [2]. Given the severity and the potential for other unknown side-effects, it is safest to disable the feature entirely for now. This patch prevent subsystem from allowing trampoline attachments to kernel module functions on LoongArch. This is a temporary mitigation until the core issues in the trampoline c module handling can be identified and fixed. [root@fedora bpf]# ./test_progs -a module_attach -v bpf_testmod.ko is already unloaded. Loading bpf_testmod.ko... S loaded bpf_testmod.ko. test_module_attach:PASS:skel_open 0 nsec test_module_attach:PASS:set_attach_target 0 nsec test_module_attach:PASS:set_attach_target_ nsec test_module_attach:PASS:skel_load 0 nsec libbpf: prog 'handle_fentry': failed to attach: -ENOTSUPP libbpf: prog 'handle_fentry': failed to auto-attach: -ENOTSU test_module_attach:FAIL:skel_attach skeleton attach failed: -524 Summary: 0/0 PASSED, 0 SKIPPED, 1 FAILED Successfully unloaded bpf_testmod.ko. [1]: https://lore.kernel.org/loongarch/CAK3+h2wDmpC-hP4u4pJY8T-yfKyk4yRzpu2LMO+C13FMT58oqQ@mail.gmail.com/ [2]: https://lore.kernel.org/loongarch/CAK3+h2wYcpc+OwdLDUBvg2rF9rvvyc5amfHT-KcFaK93uoELPg@mail.gmail.com/
CVE-2025-68217	In the Linux kernel, the following vulnerability has been resolved: Input: pegasus-notetaker - fix potential out-of-bounds access In the pegasus_notetaker driver, the pegasus_probe() function allocates the URB transfer buffer using the wMaxPacketSize value from the endpoint descriptor. An attacker can use a malicious USB des force the allocation of a very small buffer. Subsequently, if the device sends an interrupt packet with a specific pattern (e.g., where the first byte is 0x80 or 0x42), pegasus_parse_packet() function parses the packet without checking the allocated buffer size. This leads to an out-of-bounds memory access.
CVE-2025-68301	In the Linux kernel, the following vulnerability has been resolved: net: atlantic: fix fragment overflow handling in RX path The atlantic driver can receive packets wi MAX_SKB_FRAGS (17) fragments when handling large multi-descriptor packets. This causes an out-of-bounds write in skb_add_rx_frag_netmem() leading to kernel issue occurs because the driver doesn't check the total number of fragments before calling skb_add_rx_frag(). When a packet requires more than MAX_SKB_FRAGS the fragment index exceeds the array bounds. Fix by assuming there will be an extra frag if buff->len > AQ_CFG_RX_HDR_SIZE, then all fragments are accounted f reusing the existing check to prevent the overflow earlier in the code path. This crash occurred in production with an Aquantia AQC113 10G NIC. Stack trace from p environment: ``` RIP: 0010:skb_add_rx_frag_netmem+0x29/0xd0 Code: 90 f3 0f 1e fa 0f 1f 44 00 00 48 89 f8 41 89 ca 48 89 d7 48 63 ce 8b 90 c0 00 00 00 48 c1 ca 48 03 90 c8 00 00 00 <48> 89 7a 30 44 89 52 3c 44 89 42 38 40 f6 c7 01 75 74 48 89 fa 83 RSP: 0018:ffffa9bec02a8d50 EFLAGS: 00010287 RAX: ffff925b22e8 ffff925ad38d2700 RCX: ffffffffe0a0c8000 RDX: ffff9258ea95bac0 RSI: ffff925ae0a0c800 RDI: 0000000000037a40 RBP: 0000000000000024 R08: 000000000000000 0000000000000021 R10: 0000000000000848 R11: 0000000000000000 R12: ffffa9bec02a8e24 R13: ffff925ad8615570 R14: 0000000000000000 R15: ffff925b22e 0000000000000000(0000) GS:ffff925e47880000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffff9258ea95baf0 C 0000000166022004 CR4: 0000000000f72ef0 PKRU: 55555554 Call Trace: <IRQ> aq_ring_rx_clean+0x175/0xe60 [atlantic] ? aq_ring_rx_clean+0x14d/0xe60 [atlan aq_ring_tx_clean+0xdf/0x190 [atlantic] ? kmem_cache_free+0x348/0x450 ? aq_vec_poll+0x81/0x1d0 [atlantic] ? __napi_poll+0x28/0x1c0 ? net_rx_action+0x337/0 Changes in v4: - Add Fixes: tag to satisfy patch validation requirements. Changes in v3: - Fix by assuming there will be an extra frag if buff->len > AQ_CFG_RX_HDI all fragments are accounted for.
CVE-2025-68212	In the Linux kernel, the following vulnerability has been resolved: fs: Fix uninitialized 'offp' in statmount_string() In statmount_string(), most flags assign an output (offp) which is later updated with the string offset. However, the STATMOUNT_MNT_UIDMAP and STATMOUNT_MNT_GIDMAP cases directly set the struct fields inste offp. This leaves offp uninitialized, leading to a possible uninitialized dereference when *offp is updated. Fix it by assigning offp for UIDMAP and GIDMAP as well, ke code path consistent.
CVE-2025-68302	In the Linux kernel, the following vulnerability has been resolved: net: sxgbe: fix potential NULL dereference in sxgbe_rx() Currently, when skb is null, the driver pri and then dereferences skb on the next line. To fix this, let's add a 'break' after the error message to switch to sxgbe_rx_refill(), which is similar to the approach tak other drivers in this particular case, e.g. calxeda with xgmac_rx(). Found during a code review.
CVE-2025-68303	In the Linux kernel, the following vulnerability has been resolved: platform/x86: intel: punit_ipc: fix memory corruption This passes the address of the pointer "&pur when the intent was to pass the pointer itself "punit_ipcdev" (without the ampersand). This means that the: complete(&ipcdev->cmd_complete); in intel_punit_ioc(a wrong memory address corrupting it.
CVE-2025-68211	In the Linux kernel, the following vulnerability has been resolved: ksm: use range-walk function to jump over holes in scan_get_next_rmap_item Currently, scan_get_next_rmap_item() walks every page address in a VMA to locate mergeable pages. This becomes highly inefficient when scanning large virtual memory ar contain mostly unmapped regions, causing ksmd to use large amount of cpu without deduplicating much pages. This patch replaces the per-address lookup with a using walk_page_range(). The range walker allows KSM to skip over entire unmapped holes in a VMA, avoiding unnecessary lookups. This problem was previously c [1]. Consider the following test program which creates a 32 TiB mapping in the virtual address space but only populates a single page: #include <unistd.h> #inclu #include <sys/mman.h> /* 32 TiB */ const size_t size = 32ul * 1024 * 1024 * 1024 * 1024; int main() { char *area = mmap(NULL, size, PROT_READ | PROT_WRITE, MAP_NORESERVE | MAP_PRIVATE | MAP_ANON, -1, 0); if (area == MAP_FAILED) { perror("mmap() failed\n"); return -1; } /* Populate a single page such that we get */ *area = 0; /* Enable KSM. */ madvise(area, size, MADV_MERGEABLE); pause(); return 0; } $ ./ksm-sparse & $ echo 1 > /sys/kernel/mm/ksm/run Without this patc 100% of the cpu for a long time (more then 1 hour in my test machine) scanning all the 32 TiB virtual address space that contain only one mapped page. This mak essentially deadlocked not able to deduplicate anything of value. With this patch ksmd walks only the one mapped page and skips the rest of the 32 TiB virtual add making the scan fast using little cpu.
CVE-2025-68304	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_core: lookup hci_conn on RX path on protocol side The hdev lock/lookup/unlock/us the packet RX path doesn't ensure hci_conn* is not concurrently modified/deleted. This locking appears to be leftover from before conn_hash started using RCU co bf4c63252490b ("Bluetooth: convert conn hash to RCU") and not clear if it had purpose since then. Currently, there are code paths that delete hci_conn* from else the ordered hdev->workqueue where the RX work runs in. E.g. commit 5af1f84ed13a ("Bluetooth: hci_sync: Fix UAF on hci_abort_conn_sync") introduced some of t there probably were a few others before it. It's better to do the locking so that even if these run concurrently no UAF is possible. Move the lookup of hci_conn and a socket-specific conn to protocol recv handlers, and do them within a single critical section to cover hci_conn* usage and lookup. syzkaller has reported a crash that be this issue: [Task hdev->workqueue] [Task 2] hci_disconnect_all_sync l2cap_recv_acldata(hcon) hci_conn_get(hcon) hci_abort_conn_sync(hcon) hci_dev_lock hci_ hci_conn_del(hcon) v---------- hci_dev_unlock hci_conn_put(hcon) conn = hcon->l2cap_data (UAF)
CVE-2025-68305	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sock: Prevent race in socket write iter and sock bind There is a potential race cond sock bind and socket write iter. bind may free the same cmd via mgmt_pending before write iter sends the cmd, just as syzbot reported in UAF[1]. Here we use hci synchronize the two, thereby avoiding the UAF mentioned in [1]. [1] syzbot reported: BUG: KASAN: slab-use-after-free in mgmt_pending_remove+0x3b/0x210 net/bluetooth/mgmt_util.c:316 Read of size 8 at addr ffff888077164818 by task syz.0.17/5989 Call Trace: mgmt_pending_remove+0x3b/0x210 net/bluetooth/mgm set_link_security+0x5c2/0x710 net/bluetooth/mgmt.c:1918 hci_mgmt_cmd+0x9c9/0xef0 net/bluetooth/hci_sock.c:1719 hci_sock_sendmsg+0x6ca/0xef0 net/bluetooth/hci_sock.c:1839 sock_sendmsg_nosec net/socket.c:727 [inline] __sock_sendmsg+0x21c/0x270 net/socket.c:742 sock_write_iter+0x279/0x360 net/so Allocated by task 5989: mgmt_pending_add+0x35/0x140 net/bluetooth/mgmt_util.c:296 set_link_security+0x557/0x710 net/bluetooth/mgmt.c:1910 hci_mgmt_cmd+0x9c9/0xef0 net/bluetooth/hci_sock.c:1719 hci_sock_sendmsg+0x6ca/0xef0 net/bluetooth/hci_sock.c:1839 sock_sendmsg_nosec net/socket.c:727 __sock_sendmsg+0x21c/0x270 net/socket.c:742 sock_write_iter+0x279/0x360 net/socket.c:1195 Freed by task 5991: mgmt_pending_free net/bluetooth/mgmt_util mgmt_pending_foreach+0x30d/0x380 net/bluetooth/mgmt_util.c:257 mgmt_index_removed+0x112/0x2f0 net/bluetooth/mgmt.c:9477 hci_sock_bind+0xbe9/0x10 net/bluetooth/hci_sock.c:1314
CVE-2025-68210	In the Linux kernel, the following vulnerability has been resolved: erofs: avoid infinite loop due to incomplete zstd-compressed data Currently, the decompression l incorrectly spins if compressed data is truncated in crafted (deliberately corrupted) images.
CVE-	In the Linux kernel, the following vulnerability has been resolved: mlx5: Fix default values in create CQ Currently, CQs without a completion function are assigned t mlx5_add_cq_to_tasklet function by default. This is problematic since only user CQs created through the mlx5_ib driver are intended to use this function. Additiona that will use doorbells instead of polling for completions must call mlx5_cq_arm. However, the default CQ creation flow leaves a valid value in the CQ's arm_db field

2025-68209	to send interrupts to polling-only CQs in certain corner cases. These two factors would allow a polling-only kernel CQ to be triggered by an EQ interrupt and call a c function intended only for user CQs, causing a null pointer exception. Some areas in the driver have prevented this issue with one-off fixes but did not address the This patch fixes the described issue by adding defaults to the create CQ flow. It adds a default dummy completion function to protect against null pointer exceptior an invalid command sequence number by default in kernel CQs to prevent the FW from sending an interrupt to the CQ until it is armed. User CQs are responsible fo initialization values. Callers of mlx5_core_create_cq are responsible for changing the completion function and arming the CQ per their needs.
CVE-2025-68193	In the Linux kernel, the following vulnerability has been resolved: drm/xe/guc: Add devm release action to safely tear down CT When a buffer object (BO) is allocate XE_BO_FLAG_GGTT_INVALIDATE flag, the driver initiates TLB invalidation requests via the CTB mechanism while releasing the BO. However a premature release of can lead to system crashes, as observed in: Oops: Oops: 0000 [#1] SMP NOPTI RIP: 0010:h2g_write+0x2f3/0x7c0 [xe] Call Trace: guc_ct_send_locked+0x8b/0x670 xe_guc_ct_send_locked+0x19/0x60 [xe] send_tlb_invalidation+0xb4/0x460 [xe] xe_gt_tlb_invalidation_ggtt+0x15e/0x2e0 [xe] ggtt_invalidate_gt_tlb.part.0+0x16/0 ggtt_node_remove+0x110/0x140 [xe] xe_ggtt_node_remove+0x40/0xa0 [xe] xe_ggtt_remove_bo+0x87/0x250 [xe] Introduce a devm-managed release action duri xe_guc_ct_init() and xe_guc_ct_init_post_hwconfig() to ensure proper CTB disablement before resource deallocation, preventing the use-after-free scenario.
CVE-2025-68320	In the Linux kernel, the following vulnerability has been resolved: lan966x: Fix sleeping in atomic context The following warning was seen when we try to connect u the device. BUG: sleeping function called from invalid context at kernel/locking/mutex.c:575 in_atomic(): 1, irqs_disabled(): 0, non_block: 0, pid: 104, name: dropbe preempt_count: 1, expected: 0 INFO: lockdep is turned off. CPU: 0 UID: 0 PID: 104 Comm: dropbear Tainted: G W 6.18.0-rc2-00399-g6f1ab1b109b9-dirty #530 NON [W]=WARN Hardware name: Generic DT based system Call trace: unwind_backtrace from show_stack+0x10/0x14 show_stack from dump_stack_lvl+0x7c/0xac dur from __might_resched+0x16c/0x2b0 __might_resched from __mutex_lock+0x64/0xd34 __mutex_lock from mutex_lock_nested+0x1c/0x24 mutex_lock_nested from lan966x_stats_get+0x5c/0x558 lan966x_stats_get from dev_get_stats+0x40/0x43c dev_get_stats from dev_seq_printf_stats+0x3c/0x184 dev_seq_printf_stats from dev_seq_show+0x10/0x30 dev_seq_show from seq_read_iter+0x350/0x4ec seq_read_iter from seq_read+0xfc/0x194 seq_read from proc_reg_read+0xac/0x100 pr from vfs_read+0xb0/0x2b0 vfs_read from ksys_read+0x6c/0xec ksys_read from ret_fast_syscall+0x0/0x1c Exception stack(0xf0b11fa8 to 0xf0b11ff0) 1fa0: 00000 00000008 be9048d8 00001000 00000001 1fc0: 00000001 00001000 00000008 00000003 be905920 0000001e 00000000 00000001 1fe0: 0005404c be9048c0 00 b6ec2cd8 It seems that we are using a mutex in a atomic context which is wrong. Change the mutex with a spinlock.
CVE-2025-68321	In the Linux kernel, the following vulnerability has been resolved: page_pool: always add GFP_NOWARN for ATOMIC allocations Driver authors often forget to add G for page allocation from the datapath. This is annoying to users as OOMs are a fact of life, and we pretty much expect network Rx to hit page allocation failures du Make page pool add GFP_NOWARN for ATOMIC allocations by default.
CVE-2025-68183	In the Linux kernel, the following vulnerability has been resolved: ima: don't clear IMA_DIGSIG flag when setting or removing non-IMA xattr Currently when both IM in fix mode, the IMA signature will be reset to IMA hash if a program first stores IMA signature in security.ima and then writes/removes some other security xattr fo example, on Fedora, after booting the kernel with "ima_appraise=fix evm=fix ima_policy=appraise_tcb" and installing rpm-plugin-ima, installing/reinstalling a pack make good reference IMA signature generated. Instead IMA hash is generated, # getfattr -m - -d -e hex /usr/bin/bash # file: usr/bin/bash security.ima=0x0404... Th because when setting security.selinux, the IMA_DIGSIG flag that had been set early was cleared. As a result, IMA hash is generated when the file is closed. Similarly signature can be cleared on file close after removing security xattr like security.evm or setting/removing ACL. Prevent replacing the IMA file signature with a file ha preventing the IMA_DIGSIG flag from being reset. Here's a minimal C reproducer which sets security.selinux as the last step which can also replaced by removing s setting ACL, #include <stdio.h> #include <sys/xattr.h> #include <fcntl.h> #include <unistd.h> #include <string.h> #include <stdlib.h> int main() { const char* "/usr/sbin/test_binary"; const char* hex_string = "030204d33204490066306402304"; int length = strlen(hex_string); char* ima_attr_value; int fd; fd = open(file_pa O_WRONLY|O_CREAT|O_EXCL, 0644); if (fd == -1) { perror("Error opening file"); return 1; } ima_attr_value = (char*)malloc(length / 2); for (int i = 0, j = 0; i < leng j++) { sscanf(hex_string + i, "%2hhx", &ima_attr_value[j]); } if (fsetxattr(fd, "security.ima", ima_attr_value, length/2, 0) == -1) { perror("Error setting extended att close(fd); return 1; } const char* selinux_value= "system_u:object_r:bin_t:s0"; if (fsetxattr(fd, "security.selinux", selinux_value, strlen(selinux_value), 0) == -1) { pe setting extended attribute"); close(fd); return 1; } close(fd); return 0; }
CVE-2025-68181	In the Linux kernel, the following vulnerability has been resolved: drm/radeon: Remove calls to drm_put_dev() Since the allocation of the drivers main structure wa devm_drm_dev_alloc() drm_put_dev()'ing to trigger it to be free'd should be done by devres. However, drm_put_dev() is still in the probe error and device remove p the driver fails to probe warnings like the following are shown because devres is trying to drm_put_dev() after the driver already did it. [5.642230] radeon 0000:01 with driver radeon failed with error -22 [5.649605] ------------[cut here]------------ [5.649607] refcount_t: underflow; use-after-free. [5.649620] WARNING: CPU: 0 PI lib/refcount.c:28 refcount_warn_saturate+0xbe/0x110 (cherry picked from commit 3eb8c0b4c091da0a623ade0d3ee7aa4a93df1ea4)
CVE-2025-14765	Use after free in WebGPU in Google Chrome prior to 143.0.7499.147 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chr security severity: High)
CVE-2025-68180	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix NULL deref in debugfs odm_combine_segments When a connector is conne inactive (e.g., disabled by desktop environments), pipe_ctx->stream_res.tg will be destroyed. Then, reading odm_combine_segments causes kernel NULL pointer d BUG: kernel NULL pointer dereference, address: 0000000000000000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD Oops: Oops: 0000 [#1] SMP NOPTI CPU: 16 UID: 0 PID: 26474 Comm: cat Not tainted 6.17.0+ #2 PREEMPT(lazy) e6a17af9ee6db7c63e9d90dbe5b28ccab67520c6 H name: LENOVO 21Q4/LNVNB161216, BIOS PXCN25WW 03/27/2025 RIP: 0010:odm_combine_segments_show+0x93/0xf0 [amdgpu] Code: 41 83 b8 b0 00 00 00 01 ba a1 ff ff ff 48 c1 e0 0c 48 8d 8c 07 d8 02 00 00 48 85 c9 74 2d 48 8b bc 07 f0 08 00 00 <48> 8b 07 48 8b 80 08 02 00> RSP: 0018:ffffd1bf4b953c58 EFLAGS: 00 0000000000005000 RBX: ffff8e35976b02d0 RCX: ffff8e3aeed052d8 RDX: 00000000ffffffa1 RSI: ffff8e35a3120800 RDI: 0000000000000000 RBP: 00000000000000 ffff8e3580eb0000 R09: ffff8e35976b02d0 R10: ffffd1bf4b953c78 R11: 0000000000000000 R12: ffffd1bf4b953d08 R13: 0000000000040000 R14: 00000000000000 0000000000000001 FS: 00007f44d3f9f740(0000) GS:ffff8e3caa47f000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR 0000000000000000 CR3: 00000006485c2000 CR4: 0000000000f50ef0 PKRU: 55555554 Call Trace: <TASK> seq_read_iter+0x125/0x490 ? __alloc_frozen_pages_noprof+0x18f/0x350 seq_read+0x12c/0x170 full_proxy_read+0x51/0x80 vfs_read+0xbc/0x390 ? __handle_mm_fault+0xa46/0xef0 ? do_syscall_64+0x71/0x900 ksys_read+0x73/0xf0 do_syscall_64+0x71/0x900 ? count_memcg_events+0xc2/0x190 ? handle_mm_fault+0x1d7/0x2d0 ? do_user_addr_fault+0x21a/0x690 ? exc_page_fault+0x7e/0x1a0 entry_SYSCALL_64_after_hwframe+0x6c/0x74 RIP: 0033:0x7f44d4031687 Code: 48 89 fa 4c 89 df 00 8b 93 08 03 00 00 59 5e 48 83 f8 fc 74 1a 5b c3 0f 1f 84 00 00 00 00 00 48 8b 44 24 10 0f 05 <5b> c3 0f 1f 80 00 00 00 00> RSP: 002b:00007ffdb4b5f0b0 EFL 00000202 ORIG_RAX: 0000000000000000 RAX: ffffffffffffffda RBX: 00007f44d3f9f740 RCX: 00007f44d4031687 RDX: 0000000000040000 RSI: 00007f44d3f5e000 F 0000000000000003 RBP: 0000000000040000 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000202 R12: 00007 R13: 0000000000000003 R14: 0000000000000000 R15: 0000000000040000 </TASK> Modules linked in: tls tcp_diag inet_diag xt_mark ccm snd_hrtimer snd_seq_ snd_seq_midi snd_seq_oss snd_seq_midi_event snd_rawmidi snd_seq snd_seq_device x> snd_hda_codec_atihdmi snd_hda_codec_realtek_lib lenovo_wmi_helpers th snd_hda_codec_generic snd_hda_codec_hdmi snd_soc_core kvm snd_compress uvcvideo sn> platform_profile joydev amd_pmc mousedev mac_hid sch_fq_codel ui parport_pc ppdev lp parport nvme_fabrics loop nfnetlink ip_tables x_tables dm_cryp> CR2: 0000000000000000 ---[end trace 0000000000000000]--- RIP: 0010:odm_combine_segments_show+0x93/0xf0 [amdgpu] Code: 41 83 b8 b0 00 00 00 01 75 6e 48 98 ba a1 ff ff ff 48 c1 e0 0c 48 8d 8c 07 d8 02 00 00 48 85 c9 7 07 f0 08 00 00 <48> 8b 07 48 8b 80 08 02 00> RSP: 0018:ffffd1bf4b953c58 EFLAGS: 00010286 RAX: 0000000000005000 RBX: ffff8e35976b02d0 RCX: ffff8e3aee 00000000ffffffa1 RSI: ffff8e35a3120800 RDI: 0000000000000000 RBP: 0000000000000000 R08: ffff8e3580eb0000 R09: ffff8e35976b02d0 R10: ffffd1bf4b953c78 0000000000000000 R12: ffffd1bf4b953d08 R13: 0000000000040000 R14: 0000000000000001 R15: 0000000000000001 FS: 00007f44d3f9f740(0000) GS:ffff8e3caa47f000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 00000006485c2000 0 0000000000f50ef0 PKRU: 55555554 Fix this by checking pipe_ctx-> ---truncated---
CVE-2025-68179	In the Linux kernel, the following vulnerability has been resolved: s390: Disable ARCH_WANT_OPTIMIZE_HUGETLB_VMEMMAP As reported by Luiz Capitulino enablir s390 leads to reproducible crashes. The problem is that kernel page tables are modified without flushing corresponding TLB entries. Even if it looks like the empty implementation on s390 is the problem, it is actually a different problem: on s390 it is not allowed to replace an active/valid page table entry with another valid pa without the detour over an invalid entry. A direct replacement may lead to random crashes and/or data corruption. In order to invalidate an entry special instructio used (e.g. ipte or idte). Alternatively there are also special instructions available which allow to replace a valid entry with a different valid entry (e.g. crdte or cspg) the HVO code currently does not provide the hooks to allow for an implementation which is compliant with the s390 architecture requirements, disable ARCH_WANT_OPTIMIZE_HUGETLB_VMEMMAP again, which is basically a revert of the original patch which enabled it.

CVE-2025-14766	Out of bounds read and write in V8 in Google Chrome prior to 143.0.7499.147 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML p (Chromium security severity: High)
CVE-2025-62862	Ampere AmpereOne AC03 devices before 3.5.9.3, AmpereOne AC04 devices before 4.4.5.2, and AmpereOne M devices before 5.4.5.1 allow an incorrectly formed S UEFI-MM Boot Error Record Table driver that could result in (1) an out-of-bounds read which leaks Secure-EL0 information to a process running in Non-Secure state of-bounds write which corrupts Secure or Non-Secure memory, limited to memory mapped to UEFI-MM Secure Partition by the Secure Partition Manager.
CVE-2025-68130	tRPC allows users to build and consume fully typesafe APIs without schemas or code generation. Starting in version 10.27.0 and prior to versions 10.45.3 and 11.8. prototype pollution vulnerability exists in `@trpc/server`'s `formDataToObject` function, which is used by the Next.js App Router adapter. An attacker can pollute `Object.prototype` by submitting specially crafted FormData field names, potentially leading to authorization bypass, denial of service, or other security impacts. N vulnerability is only present when using `experimental_caller` / `experimental_nextAppDirCaller`. Versions 10.45.3 and 11.8.0 fix the issue.
CVE-2025-65319	When using the attachment interaction functionality, Blue Mail 1.140.103 and below saves documents to a file system without a Mark-of-the-Web tag, which allows bypass the built-in file protection mechanisms of both Windows OS and third-party software.
CVE-2025-68178	In the Linux kernel, the following vulnerability has been resolved: blk-cgroup: fix possible deadlock while configuring policy Following deadlock can be triggered eas lockdep: WARNING: possible circular locking dependency detected 6.17.0-rc3-00124-ga12c2658ced0 #1665 Not tainted ---------- che trying to acquire lock: ff1100011d9d0678 (&q->sysfs_lock){+.+.}-{4:4}, at: blk_unregister_queue+0x53/0x180 but task is already holding lock: ff1100011d9d00e >q_usage_counter(queue)#3){++++}-{0:0}, at: del_gendisk+0xba/0x110 which lock already depends on the new lock. the existing dependency chain (in reverse #2 (&q->q_usage_counter(queue)#3){++++}-{0:0}: blk_queue_enter+0x40b/0x470 blkg_conf_prep+0x7b/0x3c0 tg_set_limit+0x10a/0x3e0 cgroup_file_write+0x kernfs_fop_write_iter+0x189/0x280 vfs_write+0x256/0x490 ksys_write+0x83/0x190 __x64_sys_write+0x21/0x30 x64_sys_call+0x4608/0x4630 do_syscall_64+0xd entry_SYSCALL_64_after_hwframe+0x76/0x7e -> #1 (&q->rq_qos_mutex){+.+.}-{4:4}: __mutex_lock+0xd8/0xf50 mutex_lock_nested+0x2b/0x40 wbt_init+0x17e wbt_enable_default+0xe9/0x140 blk_register_queue+0x1da/0x2e0 __add_disk+0x38c/0x5d0 add_disk_fwnode+0x89/0x250 device_add_disk+0x18/0x30 virtblk_probe+0x13a3/0x1800 virtio_dev_probe+0x389/0x610 really_probe+0x136/0x620 __driver_probe_device+0xb3/0x230 driver_probe_device+0x2f/0xe0 __driver_attach+0x158/0x250 bus_for_each_dev+0xa9/0x130 driver_attach+0x26/0x40 bus_add_driver+0x178/0x3d0 driver_register+0x7d/0x1c0 __register_virtio_driver+0x2c/0x60 virtio_blk_init+0x6f/0xe0 do_one_initcall+0x94/0x540 kernel_init_freeable+0x56a/0x7b0 kernel_init+0x2b/0x270 ret_from_fork ret_from_fork_asm+0x1a/0x30 -> #0 (&q->sysfs_lock){+.+.}-{4:4}: __lock_acquire+0x1835/0x2940 lock_acquire+0xf9/0x450 __mutex_lock+0xd8/0xf50 mutex_lock_nested+0x2b/0x40 blk_unregister_queue+0x53/0x180 __del_gendisk+0x226/0x690 del_gendisk+0xba/0x110 sd_remove+0x49/0xb0 [sd_mod] device_remove+0x87/0xb0 device_release_driver_internal+0x11e/0x230 device_release_driver+0x1a/0x30 bus_remove_device+0x14d/0x220 device_del+0x1e1/(__scsi_remove_device+0x1ff/0x2f0 scsi_remove_device+0x37/0x60 sdev_store_delete+0x77/0x100 dev_attr_store+0x1f/0x40 sysfs_kf_write+0x65/0x90 kernfs_fop_write_iter+0x189/0x280 vfs_write+0x256/0x490 ksys_write+0x83/0x190 __x64_sys_write+0x21/0x30 x64_sys_call+0x4608/0x4630 do_syscall_64+0xd entry_SYSCALL_64_after_hwframe+0x76/0x7e other info that might help us debug this: Chain exists of: &q->sysfs_lock --> &q->rq_qos_mutex --> &q->q_usage_counter(queue)#3 Possible unsafe locking scenario: CPU0 CPU1 ---- ---- lock(&q->q_usage_counter(queue)#3); lock(&q->rq_qos_mutex); lock(&q->q_usage_counter(queue)#3); lock(&q->sysfs_lock); Root cause is that queue_usage_counter is grabbed with rq_qos_mutex held in blkg_conf_prep(), while queue freezed before rq_qos_mutex from other context. The blk_queue_enter() from blkg_conf_prep() is used to protect against policy deactivation, which is already prote blkcg_mutex, hence convert blk_queue_enter() to blkcg_mutex to fix this problem. Meanwhile, consider that blkcg_mutex is held after queue is freezed from policy also convert blkg_alloc() to use GFP_NOIO.
CVE-2025-68177	In the Linux kernel, the following vulnerability has been resolved: cpufreq/longhaul: handle NULL policy in longhaul_exit longhaul_exit() was calling cpufreq_cpu_ge checking for a NULL policy pointer. On some systems, this could lead to a NULL dereference and a kernel warning or panic. This patch adds a check using unlikely() early if the policy is NULL. Bugzilla: #219962
CVE-2025-68176	In the Linux kernel, the following vulnerability has been resolved: PCI: cadence: Check for the existence of cdns_pcie::ops before using it cdns_pcie::ops might not l by all the Cadence glue drivers. This is going to be true for the upcoming Sophgo platform which doesn't set the ops. Hence, add a check to prevent NULL pointer d [mani: reworded subject and description]
CVE-2025-68175	In the Linux kernel, the following vulnerability has been resolved: media: nxp: imx8-isi: Fix streaming cleanup on release The current implementation unconditional mxc_isi_video_cleanup_streaming() in mxc_isi_video_release(). This can lead to situations where any release call (like from a simple "v4l2-ctl -l") may release a curr streaming queue when called on such a device. This is reproducible on an i.MX8MP board by streaming from an ISI capture device using gstreamer: gst-launch-1.0 device=/dev/videoX ! \ video/x-raw,format=GRAY8,width=1280,height=800,framerate=1/120 ! \ fakesink While this stream is running, querying the caps of the sa provokes the error state: v4l2-ctl -l -d /dev/videoX This results in the following trace: [155.452152] ------------[cut here]------------ [155.452163] WARNING: CPU: 0 P drivers/media/platform/nxp/imx8-isi/imx8-isi-pipe.c:713 mxc_isi_pipe_irq_handler+0x19c/0x1b0 [imx8_isi] [157.004248] Modules linked in: cfg80211 rpmsg_ctrl rp rpmsg_tty virtio_rpmsg_bus rpmsg_ns rpmsg_core rfkill nft_ct nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 nf_tables mcp251x6 [157.053499] CPU: 0 UID: 0 PID: 17 python3 Not tainted 6.15.4-00114-g1f61ca5cad76 #1 PREEMPT [157.064369] Hardware name: imx8mp_board_01 (DT) [157.068205] pstate: 400000c5 (nZcv dall TCO -DIT -SSBS BTYPE=--) [157.075169] pc : mxc_isi_pipe_irq_handler+0x19c/0x1b0 [imx8_isi] [157.081195] lr : mxc_isi_pipe_irq_handler+0x38/0x1b0 [imx8_isi] 157.087126] sp : ffff800080003ee0 [157.090438] x29: ffff800080003ee0 x28: ffff0000c3688000 x27: 0000000000000000 [157.097580] x26: 0000000000000000 ffff0000c1e7ac00 x24: ffff800081b5ad50 [157.104723] x23: 00000000000000d1 x22: 0000000000000000 x21: ffff0000c25e4000 [157.111866] x20: 000000006 ffff80007a0608d0 x18: 0000000000000000 [157.119008] x17: ffff80006a4e3000 x16: ffff800080000000 x15: 0000000000000000 [157.126146] x14: 000000000 0000000000000000 x12: 0000000000000000 [157.133287] x11: 0000000000000040 x10: ffff0000c01445f0 x9 : ffff80007a053a38 [157.140425] x8 : ffff0000c04 0000000000000000 x6 : 0000000000000000 [157.147567] x5 : ffff0000c0400490 x4 : ffff80006a4e3000 x3 : ffff0000c25e4000 [157.154706] x2 : 000000000000 ffff8000825c0014 x0 : 0000000060000200 [157.161850] Call trace: [157.164296] mxc_isi_pipe_irq_handler+0x19c/0x1b0 [imx8_isi] (P) [157.170319] __handle_irq_event_percpu+0x58/0x218 [157.175029] handle_irq_event+0x54/0xb8 [157.178867] handle_fasteoi_irq+0xac/0x248 [157.182968] handle_irq_desc 157.186723] generic_handle_domain_irq+0x24/0x38 [157.191346] gic_handle_irq+0x54/0x120 [157.195098] call_on_irq_stack+0x24/0x30 [157.199027] do_interrupt_handler+0x88/0x98 [157.203212] el0_interrupt+0x44/0xc0 [157.206792] __el0_irq_handler_common+0x18/0x28 [157.211328] el0t_64_irq_handler 157.215429] el0t_64_irq+0x198/0x1a0 [157.219009] ---[end trace 0000000000000000]--- Address this issue by moving the streaming preparation and cleanup t .prepare_streaming() and .unprepare_streaming() operations. This also simplifies the driver by allowing direct usage of the vb2_ioctl_streamon() and vb2_ioctl_stre helpers, and removal of the manual cleanup from mxc_isi_video_release().
CVE-2025-68174	In the Linux kernel, the following vulnerability has been resolved: amd/amdkfd: enhance kfd process check in switch partition current switch partition only check if kfd_processes_table is empty. kfd_prcesses_table entry is deleted in kfd_process_notifier_release, but kfd_process tear down is in kfd_process_wq_release. consider processes: Process A (workqueue) -> kfd_process_wq_release -> Access kfd_node member Process B switch partition -> amdgpu_xcp_pre_partition_switch -> amdgpu_amdkfd_device_fini_sw -> kfd_node tear down. Process A and B may trigger a race as shown in dmesg log. This patch is to resolve the race by adding an a kfd_process counter kfd_processes_count, it increment as create kfd process, decrement as finish kfd_process_wq_release. v2: Put kfd_processes_count per kfd_de decrement to kfd_process_destroy_pdds and bug fix. (Philip Yang) [3966658.307702] divide error: 0000 [#1] SMP NOPTI [3966658.350818] i10nm_edac [3966658. 124 PID: 38435 Comm: kworker/124:0 Kdump: loaded Tainted [3966658.356890] Workqueue: kfd_process_wq kfd_process_wq_release [amdgpu] [3966658.36283 [3966658.366457] RIP: 0010:kfd_get_num_sdma_engines+0x17/0x40 [amdgpu] [3966658.366460] Code: 00 00 e9 ac 81 02 00 66 66 2e 0f 1f 84 00 00 00 00 00 9 00 48 8b 4f 08 48 8b b7 00 01 00 00 8b 81 58 26 03 00 99 <f7> be b8 01 00 00 80 b9 70 2e 00 00 00 74 0b 83 f8 02 ba 02 00 00 [3966658.380967] x86_pkg_tem [3966658.391529] RSP: 0018:ffffc900a0edfdd8 EFLAGS: 00010246 [3966658.391531] RAX: 0000000000000008 RBX: ffff8974e593b800 RCX: ffff888645900000 [3966658.391531] RDX: 0000000000000000 RSI: ffff888129154400 RDI: ffff888129151c00 [3966658.391532] RBP: ffff8883ad79d400 R08: 0000000000000000 R(ffff8890d2750af4 [3966658.391532] R10: 0000000000000018 R11: 0000000000000018 R12: 0000000000000000 [3966658.391533] R13: ffff8883ad79d400 R14: ffffe87ff662ba00 R15: ffff8974e593b800 [3966658.391533] FS: 0000000000000000(0000) GS:ffff88fe7f600000(0000) knlGS:0000000000000000 [3966658.39153 DS: 0000 ES: 0000 CR0: 0000000080050033 [3966658.391534] CR2: 0000000000d71000 CR3: 000000dd0e970004 CR4: 0000000002770ee0 [3966658.391535] D

	0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [3966658.391535] DR3: 0000000000000000 DR6: 00000000fffe07f0 DR7: 000000000000 [3966658.391536] PKRU: 55555554 [3966658.391536] Call Trace: [3966658.391674] deallocate_sdma_queue+0x38/0xa0 [amdgpu] [3966658.391762] process_termination_cpsch+0x1ed/0x480 [amdgpu] [3966658.399754] intel_powerclamp [3966658.402831] kfd_process_dequeue_from_all_devices+0x5b/0xc0 [a [3966658.402908] kfd_process_wq_release+0x1a/0x1a0 [amdgpu] [3966658.410516] coretemp [3966658.434016] process_one_work+0x1ad/0x380 [3966658.434 worker_thread+0x49/0x310 [3966658.438963] kvm_intel [3966658.446041] ? process_one_work+0x380/0x380 [3966658.446045] kthread+0x118/0x140 [396665 __kthread_bind_mask+0x60/0x60 [3966658.446050] ret_from_fork+0x1f/0x30 [3966658.446053] Modules linked in: kpatch_20765354(OEK) [3966658.455310] kv [3966658.464534] mptcp_diag xsk_diag raw_diag unix_diag af_packet_diag netlink_diag udp_diag act_pedit act_mirred act_vlan cls_flower kpatch_21951273(OEK) kpatch_18424469(OEK) kpatch_19749756(OEK) [3966658.473462] idxd_mdev [3966658.482306] kpatch_17971294(OEK) sch_ingress xt_conntrack amdgpu(OE) a amddrm_buddy(OE) amd_sched(OE) amdttm(OE) amdkcl(OE) intel_ifs iptable_mangle tcm_loop target_core_pscsi tcp_diag target_core_file inet_diag target_core_ib target_core_user target_core_mod coldpgs kpatch_18383292(OEK) ip6table_nat ip6table_filter ip6_tables ip_set_hash_ipportip ip_set_hash_ipportnet ip_set_hash_ip ip_set_bitmap_port xt_comment iptable_nat nf_nat iptable_filter ip_tables ip_set ip_vs_sh ip_vs_wrr ip_vs_rr ip_vs nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 sn_co i40e overlay binfmt_misc tun bonding(OE) aisqos(OE) aisqo ---truncated---
CVE-2025-68173	In the Linux kernel, the following vulnerability has been resolved: ftrace: Fix softlockup in ftrace_module_enable A soft lockup was observed when loading amdgpu module has a lot of tracable functions, multiple calls to kallsyms_lookup can spend too much time in RCU critical section and with disabled preemption, causing ke This is the same issue that was fixed in commit d0b24b4e91fc ("ftrace: Prevent RCU stall on PREEMPT_VOLUNTARY kernels") and commit 42ea22e754ba ("ftrace: A cond_resched() to ftrace_graph_set_hash()"). Fix it the same way by adding cond_resched() in ftrace_module_enable.
CVE-2025-68172	In the Linux kernel, the following vulnerability has been resolved: crypto: aspeed - fix double free caused by devm The clock obtained via devm_clk_get_enabled() i automatically managed by devres and will be disabled and freed on driver detach. Manually calling clk_disable_unprepare() in error path and remove function caus free. Remove the manual clock cleanup in both aspeed_acry_probe()'s error path and aspeed_acry_remove().
CVE-2025-68171	In the Linux kernel, the following vulnerability has been resolved: x86/fpu: Ensure XFD state on signal delivery Sean reported [1] the following splat when running K WARNING: CPU: 232 PID: 15391 at xfd_validate_state+0x65/0x70 Call Trace: <TASK> fpu__clear_user_states+0x9c/0x100 arch_do_signal_or_restart+0x142/0x210 exit_to_user_mode_loop+0x55/0x100 do_syscall_64+0x205/0x2c0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 Chao further identified [2] a reproducible scenari signal delivery: a non-AMX task is preempted by an AMX-enabled task which modifies the XFD MSR. When the non-AMX task resumes and reloads XSTATE with init warning is triggered due to a mismatch between fpstate::xfd and the CPU's current XFD state. fpu__clear_user_states() does not currently re-synchronize the XFD s such preemption. Invoke xfd_update_state() which detects and corrects the mismatch if there is a dynamic feature. This also benefits the sigreturn path, as fpu__re may call fpu__clear_user_states() when the sigframe is inaccessible. [dhansen: minor changelog munging]
CVE-2025-68170	In the Linux kernel, the following vulnerability has been resolved: drm/radeon: Do not kfree() devres managed rdev Since the allocation of the drivers main structu changed to devm_drm_dev_alloc() rdev is managed by devres and we shouldn't be calling kfree() on it. This fixes things exploding if the driver probe fails and devr the rdev after we already free'd it. (cherry picked from commit 16c0681617b8a045773d4d87b6140002fa75b03b)
CVE-2025-68169	In the Linux kernel, the following vulnerability has been resolved: netpoll: Fix deadlock in memory allocation under spinlock Fix a AA deadlock in refill_skbs() where allocation while holding skb_pool->lock can trigger a recursive lock acquisition attempt. The deadlock scenario occurs when the system is under severe memory pr refill_skbs() acquires skb_pool->lock (spinlock) 2. alloc_skb() is called while holding the lock 3. Memory allocator fails and calls slab_out_of_memory() 4. This trigger the OOM warning 5. The console output path calls netpoll_send_udp() 6. netpoll_send_udp() attempts to acquire the same skb_pool->lock 7. Deadlock: the lock is a the same CPU Call stack: refill_skbs() spin_lock_irqsave(&skb_pool->lock) <- lock acquired __alloc_skb() kmem_cache_alloc_node_noprof() slab_out_of_memory() pr console_flush_all() netpoll_send_udp() skb_dequeue() spin_lock_irqsave(&skb_pool->lock) <- deadlock attempt This bug was exposed by commit 248f6571fd4c51 (Optimize skb refilling on critical path") which removed refill_skbs() from the critical path (where nested printk was being deferred), letting nested printk being calle refill_skbs() Refactor refill_skbs() to never allocate memory while holding the spinlock. Another possible solution to fix this problem is protecting the refill_skbs() fro printks, basically calling printk_deferred_{enter,exit}() in refill_skbs(), then, any nested pr_warn() would be deferred. I prefer this approach, given I _think_ it might idea to move the alloc_skb() from GFP_ATOMIC to GFP_KERNEL in the future, so, having the alloc_skb() outside of the lock will be necessary step. There is a possibl issue when checking for the pool length, and queueing the new allocated skb, but, this is not an issue, given that an extra SKB in the pool is harmless and it will be used.
CVE-2025-68168	In the Linux kernel, the following vulnerability has been resolved: jfs: fix uninitialized waitqueue in transaction manager The transaction manager initialization in tx properly initializing TxBlock[0].waitor waitqueue, causing a crash when txEnd(0) is called on read-only filesystems. When a filesystem is mounted read-only, txBegi tid=0 to indicate no transaction. However, txEnd(0) still gets called and tries to access TxBlock[0].waitor via tid_to_tblock(0), but this waitqueue was never initialize the initialization loop started at index 1 instead of 0. This causes a 'non-static key' lockdep warning and system crash: INFO: trying to register non-static key in txE ensuring all transaction blocks including TxBlock[0] have their waitqueues properly initialized during txInit().
CVE-2025-68167	In the Linux kernel, the following vulnerability has been resolved: gpiolib: fix invalid pointer access in debugfs If the memory allocation in gpiolib_seq_start() fails, t field remains uninitialized and is later dereferenced without checking in gpiolib_seq_stop(). Initialize s->private to NULL before calling kzalloc() and check it before it.
CVE-2025-40363	In the Linux kernel, the following vulnerability has been resolved: net: ipv6: fix field-spanning memcpy warning in AH output Fix field-spanning memcpy warnings i and ah6_output_done() where extension headers are copied to/from IPv6 address fields, triggering fortify-string warnings about writes beyond the 16-byte address memcpy: detected field-spanning write (size 40) of single field "&top_iph->saddr" at net/ipv6/ah6.c:439 (size 16) WARNING: CPU: 0 PID: 8838 at net/ipv6/ah6.c:43 ah6_output+0xe7e/0x14e0 net/ipv6/ah6.c:439 The warnings are false positives as the extension headers are intentionally placed after the IPv6 header in memory. properly copying addresses and extension headers separately, and introduce helper functions to avoid code duplication.
CVE-2025-40362	In the Linux kernel, the following vulnerability has been resolved: ceph: fix multifs mds auth caps issue The mds auth caps check should also validate the fsname a associated caps. Not doing so would result in applying the mds auth caps of one fs on to the other fs in a multifs ceph cluster. The bug causes multiple issues w.r.t authentication, following is one such example. Steps to Reproduce (on vstart cluster): 1. Create two file systems in a cluster, say 'fsname1' and 'fsname2' 2. Autho permission to the user 'client.usr' on fs 'fsname1' $ceph fs authorize fsname1 client.usr / r 3. Authorize read and write permission to the same user 'client.usr' on fs $ceph fs authorize fsname2 client.usr / rw 4. Update the keyring $ceph auth get client.usr >> ./keyring With above permssions for the user 'client.usr', following is expectation. a. The 'client.usr' should be able to only read the contents and not allowed to create or delete files on file system 'fsname1'. b. The 'client.usr' should read/write on file system 'fsname2'. But, with this bug, the 'client.usr' is allowed to read/write on file system 'fsname1'. See below. 5. Mount the file system 'fsname user 'client.usr' $sudo bin/mount.ceph usr@.fsname1=/ /kmnt_fsname1_usr/ 6. Try creating a file on file system 'fsname1' with user 'client.usr'. This should fail but this bug. $touch /kmnt_fsname1_usr/file1 7. Mount the file system 'fsname1' with the user 'client.admin' and create a file. $sudo bin/mount.ceph admin@.fsname1 /kmnt_fsname1_admin $echo "data" > /kmnt_fsname1_admin/admin_file1 8. Try removing an existing file on file system 'fsname1' with the user 'client.usr'. This sh succeed but succeeds with the bug. $rm -f /kmnt_fsname1_usr/admin_file1 For more information, please take a look at the corresponding mds/fuse patch and tests looking into the tracker mentioned below. v2: Fix a possible null dereference in doutc v3: Don't store fsname from mdsmap, validate against ceph_mount_options's use it v4: Code refactor, better warning message and fix possible compiler warning [Slava.Dubeyko: "fsname check failed" -> "fsname mismatch"]
CVE-2025-40361	In the Linux kernel, the following vulnerability has been resolved: fs: ext4: change GFP_KERNEL to GFP_NOFS to avoid deadlock The parent function ext4_xattr_inode_lookup_create already uses GFP_NOFS for memory alloction, so the function ext4_xattr_inode_cache_find should use same gfp_flag.
CVE-2025-40360	In the Linux kernel, the following vulnerability has been resolved: drm/sysfb: Do not dereference NULL pointer in plane reset The plane state in __drm_gem_reset_shadow_plane() can be NULL. Do not deref that pointer, but forward NULL to the other plane-reset helpers. Clears plane->state to NULL. v2: - fix commit description (Javier)
	In the Linux kernel, the following vulnerability has been resolved: perf/x86/intel: Fix KASAN global-out-of-bounds warning When running "perf mem record" comma

CVE-2025-40359	the below KASAN global-out-of-bounds warning is seen. ==========...========== KASAN: global-out-of-bounds in cmt_latency_data+0x176/0x1b0 Read of size 4 at addr ffffffffb721d000 by task dtlb/9850 Call Trace: kasan_report+0xb8/0xf0 cmt_latency_data+0x176/0x1b0 setup_arch_pebs_sample_data+0xf49/0x2560 intel_pmu_drain_arch_pebs+0x577/0xb00 handle_pmi_common+0x6c4/0xc80 The i caused by below code in __grt_latency_data(). The code tries to access x86_hybrid_pmu structure which doesn't exist on non-hybrid platform like CWF. WARN_ON_ONCE(hybrid_pmu(event->pmu)->pmu_type == hybrid_big) So add is_hybrid() check before calling this WARN_ON_ONCE to fix the global-out-of-bounds
CVE-2025-40358	In the Linux kernel, the following vulnerability has been resolved: riscv: stacktrace: Disable KASAN checks for non-current tasks Unwinding the stack of a task other KASAN would report "BUG: KASAN: out-of-bounds in walk_stackframe+0x41c/0x460" There is a same issue on x86 and has been resolved by the commit 84936118 ("x86/unwind: Disable KASAN checks for non-current tasks") The solution could be applied to RISC-V too. This patch also can solve the issue: https://seclists.org/oss sec/2025/q4/23 [pjw@kernel.org: clean up checkpatch issues]
CVE-2025-40357	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix general protection fault in __smc_diag_dump The syzbot report a crash: Oops: genera fault, probably for non-canonical address 0xfbd5a5d5a0000003: 0000 [#1] SMP KASAN NOPTI KASAN: maybe wild-memory-access in range [0xdead4ead00000018 0xdead4ead0000001f] CPU: 1 UID: 0 PID: 6949 Comm: syz.0.335 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Compute Engine/Google Compute Google 08/18/2025 RIP: 0010:smc_diag_msg_common_fill net/smc/smc_diag.c:44 [inline] RIP: 0010:__smc_diag_dump.constprop.0+0x3ca/0x2550 net/smc/smc_dia Trace: <TASK> smc_diag_dump_proto+0x26d/0x420 net/smc/smc_diag.c:217 smc_diag_dump+0x27/0x90 net/smc/smc_diag.c:234 netlink_dump+0x539/0xd30 net/netlink/af_netlink.c:2327 __netlink_dump_start+0x6d6/0x990 net/netlink/af_netlink.c:2442 netlink_dump_start include/linux/netlink.h:341 [inline] smc_diag_handler_dump+0x1f9/0x240 net/smc/smc_diag.c:251 __sock_diag_cmd net/core/sock_diag.c:249 [inline] sock_diag_rcv_msg+0x438/0x790 net/core/sock netlink_rcv_skb+0x158/0x420 net/netlink/af_netlink.c:2552 netlink_unicast_kernel net/netlink/af_netlink.c:1320 [inline] netlink_unicast+0x5a7/0x870 net/netlink/af_netlink.c:1346 netlink_sendmsg+0x8d1/0xdd0 net/netlink/af_netlink.c:1896 sock_sendmsg_nosec net/socket.c:714 [inline] __sock_sendmsg net/sock [inline] ____sys_sendmsg+0xa95/0xc70 net/socket.c:2614 ___sys_sendmsg+0x134/0x1d0 net/socket.c:2668 __sys_sendmsg+0x16d/0x220 net/socket.c:2700 do_sy arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xcd/0x4e0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> The proce (CPU1) | (CPU2) ----------|---------- inet_create() | // init clcsock to NULL | sk = sk_alloc() | | // unexpectedly change clcsock | inet_init_cs add sk to hash table | smc_inet_init_sock() | smc_sk_init() | smc_hash_sk() | | // traverse the hash table | smc_diag_dump_proto | __smc_diag_dump() | // visit wrong smc_diag_msg_common_fill() // alloc clcsock | smc_create_clcsk | sock_create_kern | With CONFIG_DEBUG_LOCK_ALLOC=y, the smc->clcsock is unexpectedly chan inet_init_csk_locks(). The INET_PROTOSW_ICSK flag is no need by smc, just remove it. After removing the INET_PROTOSW_ICSK flag, this patch alse revert commit 6 ("net/smc: fix lacks of icsk_syn_mss with IPPROTO_SMC") to avoid casting smc_sock to inet_connection_sock.
CVE-2025-40356	In the Linux kernel, the following vulnerability has been resolved: spi: rockchip-sfc: Fix DMA-API usage Use DMA-API dma_map_single() call for getting the DMA add transfer buffer instead of hacking with virt_to_phys(). This fixes the following DMA-API debug warning: ------------[cut here]------------ DMA-API: rockchip-sfc fe300000 driver tries to sync DMA memory it has not allocated [device address=0x000000000cf70000] [size=288 bytes] WARNING: kernel/dma/debug.c:1106 at check_sync+0x1d8/0x690, CPU#2: systemd-udevd/151 Modules linked in: ... Hardware name: Hardkernel ODROID-M1 (DT) pstate: 604000c9 (nZCv daIF +PAN -UA SSBS BTYPE=--) pc : check_sync+0x1d8/0x690 lr : check_sync+0x1d8/0x690 .. Call trace: check_sync+0x1d8/0x690 (P) debug_dma_sync_single_for_cpu+0x84/0x __dma_sync_single_for_cpu+0x88/0x234 rockchip_sfc_exec_mem_op+0x4a0/0x798 [spi_rockchip_sfc] spi_mem_exec_op+0x408/0x498 spi_nor_read_data+0x170/ spi_nor_read_sfdp+0x74/0xe4 spi_nor_parse_sfdp+0x120/0x11f0 spi_nor_sfdp_init_params_deprecated+0x3c/0x8c spi_nor_scan+0x690/0xf88 spi_nor_probe+0xe spi_mem_probe+0x6c/0xa8 spi_probe+0x94/0xd4 really_probe+0xbc/0x298 ...
CVE-2025-40355	In the Linux kernel, the following vulnerability has been resolved: sysfs: check visibility before changing group attribute ownership Since commit 0c17270f9b92 ("n Implement is_visible for phys_(port_id, port_name, switch_id)"), __dev_change_net_namespace() can hit WARN_ON() when trying to change owner of a file that isn't the trace below: WARNING: CPU: 6 PID: 2938 at net/core/dev.c:12410 __dev_change_net_namespace+0xb89/0xc30 CPU: 6 UID: 0 PID: 2938 Comm: incusd Not tain mainline #1 PREEMPT(full) 4b783b4a638669fb644857f484487d17cb45ed1f Hardware name: Framework Laptop 13 (AMD Ryzen 7040Series)/FRANMDCP07, BIOS 0 02/19/2025 RIP: 0010:__dev_change_net_namespace+0xb89/0xc30 [...] Call Trace: <TASK> ? if6_seq_show+0x30/0x50 do_setlink.isra.0+0xc7/0x1270 ? __nla_validate_parse+0x5c/0xcc0 ? security_capable+0x94/0x1a0 rtnl_newlink+0x858/0xc20 ? update_curr+0x8e/0x1c0 ? update_entity_lag+0x71/0x80 ? sched_balance_newidle+0x358/0x450 ? psi_task_switch+0x113/0x2a0 ? __pfx_rtnl_newlink+0x10/0x10 rtnetlink_rcv_msg+0x346/0x3e0 ? sched_clock+0x10/0x30 __pfx_rtnetlink_rcv_msg+0x10/0x10 netlink_rcv_skb+0x59/0x110 netlink_unicast+0x285/0x3c0 ? __alloc_skb+0xdb/0x1a0 netlink_sendmsg+0x20d/0x430 ____sys_sendmsg+0x39f/0x3d0 ? import_iovec+0x2f/0x40 ___sys_sendmsg+0x99/0xe0 __sys_sendmsg+0x8a/0xf0 do_syscall_64+0x81/0x970 ? __sys_bind+0xe3/ syscall_exit_work+0x143/0x1b0 ? do_syscall_64+0x244/0x970 ? sock_alloc_file+0x63/0xc0 ? syscall_exit_work+0x143/0x1b0 ? do_syscall_64+0x244/0x970 ? alloc_fd+0x12e/0x190 ? put_unused_fd+0x2a/0x70 ? do_sys_openat2+0xa2/0xe0 ? syscall_exit_work+0x143/0x1b0 ? do_syscall_64+0x244/0x970 ? exc_page_fault+0x7e/0x1a0 entry_SYSCALL_64_after_hwframe+0x76/0x7e [...] </TASK> Fix this by checking is_visible() before trying to touch the attribute.
CVE-2025-68182	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: fix potential use after free in iwl_mld_remove_link() This code frees "link" by calling k rcu_head) and then it dereferences "link" to get the "link->fw_id". Save the "link->fw_id" first to avoid a potential use after free.
CVE-2025-68184	In the Linux kernel, the following vulnerability has been resolved: drm/mediatek: Disable AFBC support on Mediatek DRM driver Commit c410fa9b07c3 ("drm/media AFBC support to Mediatek DRM driver") added AFBC support to Mediatek DRM and enabled the 32x8/split/sparse modifier. However, this is currently broken on Me (Genio 700 EVK platform); tested using upstream Kernel and Mesa (v25.2.1), AFBC is used by default since Mesa v25.0. Kernel trace reports vblank timeouts consta render is garbled: ``` [CRTC:62:crtc-0] vblank wait timed out WARNING: CPU: 7 PID: 70 at drivers/gpu/drm/drm_atomic_helper.c:1835 drm_atomic_helper_wait_for_vblanks.part.0+0x24c/0x27c [...] Hardware name: MediaTek Genio-700 EVK (DT) Workqueue: events_unbound commit_work pstate: 6 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : drm_atomic_helper_wait_for_vblanks.part.0+0x24c/0x27c lr : drm_atomic_helper_wait_for_vblanks.part.0+0x : ffff80008337bca0 x29: ffff80008337bcd0 x28: 0000000000000061 x27: 0000000000000000 x26: 0000000000000001 x25: 0000000000000000 x24: ffff0000c9d 0000000000000001 x22: 0000000000000000 x21: ffff0000c66f2f80 x20: ffff0000c0d7d880 x19: 0000000000000000 x18: 000000000000000a x17: 00000004004 005000f2b5503510 x15: 0000000000000000 x14: 0000000000000000 x13: 74756f2064656d69 x12: 7420746961772006b x11: 0000000000000058 x10: 0000000 : ffff800082396a70 x8 : 0000000000057fa8 x7 : 0000000000000cce x6 : ffff8000823eea70 x5 : ffff0001fef5f408 x4 : ffff80017ccee000 x3 : ffff0000c12cb480 x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffff0000c12cb480 Call trace: drm_atomic_helper_wait_for_vblanks.part.0+0x24c/0x27c (P) drm_atomic_helper_commit_tail_rpm+0x64/0x80 commit_tail+0xa4/0x1a4 commit_work+0x14/0x20 process_one_work+0x150/0x290 worker_thread+0x2d0/0x3e kthread+0x12c/0x210 ret_from_fork+0x10/0x20 ---[end trace 0000000000000000]--- ``` Until this gets fixed upstream, disable AFBC support on this platform, as broken with upstream Mesa.
CVE-2025-68322	In the Linux kernel, the following vulnerability has been resolved: parisc: Avoid crash due to unaligned access in unwinder Guenter Roeck reported this kernel crash emulated B160L machine: Starting network: udhcpc: started, v1.36.1 Backtrace: [<104320d4>] unwind_once+0x1c/0x5c [<10434a00>] walk_stackframe.isra.0+0 [<10434a6c>] arch_stack_walk+0x28/0x38 [<104e5efc>] stack_trace_save+0x48/0x5c [<105d1bdc>] set_track_prepare+0x44/0x6c [<105d9c80>] ___slab_alloc+0xfc4/0x1024 [<105d9d38>] __slab_alloc.isra.0+0x58/0x90 [<105dc80c>] kmem_cache_alloc_noprof+0x2ac/0x4a0 [<105b8e54>] __anon_vma_prepare+0x60/0x280 [<105a823c>] __vmf_anon_prepare+0x68/0x94 [<105a8b34>] do_wp_page+0x8cc/0xf10 [<105aad88>] handle_mm_fault+0x [<10425568>] do_page_fault+0x110/0x440 [<10427938>] handle_interruption+0x184/0x748 [<11178398>] schedule+0x4c/0x190 BUG: spinlock recursion on C ifconfig/2420 lock: terminate_lock.2+0x0/0x1c, .magic: dead4ead, .owner: ifconfig/2420, .owner_cpu: 0 While creating the stack trace, the unwinder uses the stack guess the previous frame to read the previous stack pointer from memory. The crash happens, because the unwinder tries to read from unaligned memory and as the unalignment trap handler which then leads to the spinlock recursion and finally to a deadlock. Fix it by checking the alignment before accessing the memory.
CVE-2025-68185	In the Linux kernel, the following vulnerability has been resolved: nfs4_setup_readdir(): insufficient locking for ->d_parent->d_inode dereferencing Theoretically it's race, but I don't believe one can manage to hit it on real hardware; might become doable on a KVM, but it still won't be easy to attack. Anyway, it's easy to deal wi xdr_encode_hyper() is just a call of put_unaligned_be64(), we can put that under ->d_lock and be done with that.
	In the Linux kernel, the following vulnerability has been resolved: libceph: fix potential use-after-free in have_mon_and_osd_map() The wait loop in __ceph_open_se race with the client receiving a new monmap or osdmap shortly after the initial map is received. Both ceph_monc_handle_map() and handle_one_map() install a ne

CVE-2025-68285	immediately after freeing the old one kfree(monc->monmap); monc->monmap = monmap; ceph_osdmap_destroy(osdc->osdmap); osdc->osdmap = newmap; unc >monc.mutex and client->osdc.lock respectively, but because neither is taken in have_mon_and_osd_map() it's possible for client->monc.monmap->epoch and cli >osdc.osdmap->epoch arms in client->monc.monmap && client->monc.monmap->epoch && client->osdc.osdmap && client->osdc.osdmap->epoch; condition to an already freed map. This happens to be reproducible with generic/395 and generic/397 with KASAN enabled: BUG: KASAN: slab-use-after-free in have_mon_and_osd_map+0x56/0x70 Read of size 4 at addr ffff88811012d810 by task mount.ceph/13305 CPU: 2 UID: 0 PID: 13305 Comm: mount.ceph Not tainted build2+ #1266 ... Call Trace: <TASK> have_mon_and_osd_map+0x56/0x70 ceph_open_session+0x182/0x290 ceph_get_tree+0x333/0x680 vfs_get_tree+0x49/0x1 do_new_mount+0x1a3/0x2d0 path_mount+0x6dd/0x730 do_mount+0x99/0xe0 __do_sys_mount+0x141/0x180 do_syscall_64+0x9f/0x100 entry_SYSCALL_64_after_hwframe+0x76/0x7e </TASK> Allocated by task 13305: ceph_osdmap_alloc+0x16/0x130 ceph_osdc_init+0x27a/0x4c0 ceph_create_client+0x153/0x190 create_fs_client+0x50/0x2a0 ceph_get_tree+0xff/0x680 vfs_get_tree+0x49/0x180 do_new_mount+0x1a3/0x2d0 path_mount+0x do_mount+0x99/0xe0 __do_sys_mount+0x141/0x180 do_syscall_64+0x9f/0x100 entry_SYSCALL_64_after_hwframe+0x76/0x7e Freed by task 9475: kfree+0x212/(handle_one_map+0x23c/0x3b0 ceph_osdc_handle_map+0x3c9/0x590 mon_dispatch+0x655/0x6f0 ceph_con_process_message+0xc3/0xe0 ceph_con_v1_try_read+ ceph_con_workfn+0x2de/0x650 process_one_work+0x486/0x7c0 process_scheduled_works+0x73/0x90 worker_thread+0x1c8/0x2a0 kthread+0x2ec/0x300 ret_from_fork+0x24/0x40 ret_from_fork_asm+0x1a/0x30 Rewrite the wait loop to check the above condition directly with client->monc.mutex and client->osdc.loc appropriate. While at it, improve the timeout handling (previously mount_timeout could be exceeded in case wait_event_interruptible_timeout() slept more than on access client->auth_err under client->monc.mutex to match how it's set in finish_auth(). monmap_show() and osdmap_show() now take the respective lock before map as well.
CVE-2025-68284	In the Linux kernel, the following vulnerability has been resolved: libceph: prevent potential out-of-bounds writes in handle_auth_session_key() The len field origina untrusted network packets. Boundary checks have been added to prevent potential out-of-bounds writes when decrypting the connection secret or processing serv idryomov: changelog]
CVE-2025-68283	In the Linux kernel, the following vulnerability has been resolved: libceph: replace BUG_ON with bounds check for map->max_osd OSD indexes come from untruste packets. Boundary checks are added to validate these against map->max_osd. [idryomov: drop BUG_ON in ceph_get_primary_affinity(), minor cosmetic edits]
CVE-2025-68282	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: udc: fix use-after-free in usb_gadget_state_work A race condition during gadget tear lead to a use-after-free in usb_gadget_state_work(), as reported by KASAN: BUG: KASAN: invalid-access in sysfs_notify+0x2c/0xd0 Workqueue: events usb_gadget_ The fundamental race occurs because a concurrent event (e.g., an interrupt) can call usb_gadget_set_state() and schedule gadget->work at any time during the cl in usb_del_gadget(). Commit 399a45e5237c ("usb: gadget: core: flush gadget workqueue after device removal") attempted to fix this by moving flush_work() to aft device_del(). However, this does not fully solve the race, as a new work item can still be scheduled *after* flush_work() completes but before the gadget's memory leading to the same use-after-free. This patch fixes the race condition robustly by introducing a 'teardown' flag and a 'state_lock' spinlock to the usb_gadget struct. set during cleanup in usb_del_gadget() *before* calling flush_work() to prevent any new work from being scheduled once cleanup has commenced. The scheduling usb_gadget_set_state(), now checks this flag under the lock before queueing the work, thus safely closing the race window.
CVE-2025-68223	In the Linux kernel, the following vulnerability has been resolved: drm/radeon: delete radeon_fence_process in is_signaled, no deadlock Delete the attempt to prog queue when checking if fence is signaled. This avoids deadlock. dma-fence_ops::signaled can be called with the fence lock in unknown state. For radeon, the fence the wait queue lock. This can cause a self deadlock when signaled() tries to make forward progress on the wait queue. But advancing the queue is unneeded becau returning false from signaled() is perfectly acceptable. (cherry picked from commit 527ba26e50ec2ca2be9c7c82f3ad42998a75d0db)
CVE-2025-68192	In the Linux kernel, the following vulnerability has been resolved: net: usb: qmi_wwan: initialize MAC header offset in qmimux_rx_fixup Raw IP packets have no MA leaving skb->mac_header uninitialized. This can trigger kernel panics on ARM64 when xfrm or other subsystems access the offset due to strict alignment checks. I MAC header to prevent such crashes. This can trigger kernel panics on ARM when running IPsec over the qmimux0 interface. Example trace: Internal error: Oops: 000000009600004f [#1] SMP CPU: 0 UID: 0 PID: 0 Comm: swapper/0 Not tainted 6.12.34-gbe78e49cb433 #1 Hardware name: LS1028A RDB Board (DT) pstate: 60 daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : xfrm_input+0xde8/0x1318 lr : xfrm_input+0x61c/0x1318 sp : ffff800080003b20 Call trace: xfrm_input+0xde8/0x13 xfrm6_rcv+0x38/0x44 xfrm6_esp_rcv+0x48/0xa8 ip6_protocol_deliver_rcu+0x94/0x4b0 ip6_input_finish+0x44/0x70 ip6_input+0x44/0xc0 ipv6_rcv+0x6c/0x114 __netif_receive_skb_one_core+0x5c/0x8c __netif_receive_skb+0x18/0x60 process_backlog+0x78/0x17c __napi_poll+0x38/0x180 net_rx_action+0x168/0x2f0
CVE-2025-68224	In the Linux kernel, the following vulnerability has been resolved: scsi: core: Fix a regression triggered by scsi_host_busy() Commit 995412e23bb2 ("blk-mq: Replac with SRCU for tag iterators") introduced the following regression: Call trace: __srcu_read_lock+0x30/0x80 (P) blk_mq_tagset_busy_iter+0x44/0x300 scsi_host_busy ufshcd_print_host_state+0x34/0x1bc ufshcd_link_startup.constprop.0+0xe4/0x2e0 ufshcd_init+0x944/0xf80 ufshcd_pltfrm_init+0x504/0x820 ufs_rockchip_probe+ platform_probe+0x5c/0xa4 really_probe+0xc0/0x38c __driver_probe_device+0x7c/0x150 driver_probe_device+0x40/0x120 __driver_attach+0xc8/0x1e0 bus_for_each_dev+0x7c/0xdc driver_attach+0x24/0x30 bus_add_driver+0x110/0x230 driver_register+0x68/0x130 __platform_driver_register+0x20/0x2c ufs_rockchip_pltform_init+0x1c/0x28 do_one_initcall+0x60/0x1e0 kernel_init_freeable+0x248/0x2c4 kernel_init+0x20/0x140 ret_from_fork+0x10/0x20 Fix this reg making scsi_host_busy() check whether the SCSI host tag set has already been initialized. tag_set->ops is set by scsi_mq_setup_tags() just before blk_mq_alloc_tag called. This fix is based on the assumption that scsi_host_busy() and scsi_mq_setup_tags() calls are serialized. This is the case in the UFS driver.
CVE-2025-68225	In the Linux kernel, the following vulnerability has been resolved: lib/test_kho: check if KHO is enabled We must check whether KHO is enabled prior to issuing KHO otherwise KHO internal data structures are not initialized.
CVE-2025-68274	SIPGO is a library for writing SIP services in the GO language. Starting in version 0.3.0 and prior to version 1.0.0-alpha-1, a nil pointer dereference vulnerability is in library's `NewResponseFromRequest` function that affects all normal SIP operations. The vulnerability allows remote attackers to crash any SIP application by send malformed SIP request without a To header. The vulnerability occurs when SIP message parsing succeeds for a request missing the To header, but the response cr assumes the To header exists without proper nil checks. This affects routine operations like call setup, authentication, and message handling - not just error cases. vulnerability affects all SIP applications using the sipgo library, not just specific configurations or edge cases, as long as they make use of the `NewResponseFromR function. Version 1.0.0-alpha-1 contains a patch for the issue.
CVE-2025-50401	Mercury D196G d196gv1-cn-up_2020-01-09_11.21.44 is vulnerable to Buffer Overflow in the function sub_404CAEDC via the parameter password.
CVE-2025-68226	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix incomplete backport in cfids_invalidation_worker() The previous commit bdb596ce client: fix potential UAF in smb2_close_cached_fid()") was an incomplete backport and missed one kref_put() call in cfids_invalidation_worker() that should have be to close_cached_dir().
CVE-2025-68227	In the Linux kernel, the following vulnerability has been resolved: mptcp: Fix proto fallback detection with BPF The sockmap feature allows bpf syscall from userspa on bpf sockops, replacing the sk_prot of sockets during protocol stack processing with sockmap's custom read/write interfaces. ''' tcp_rcv_state_process() syn_recv_sock()/subflow_syn_recv_sock() tcp_init_transfer(BPF_SOCK_OPS_PASSIVE_ESTABLISHED_CB) bpf_skops_established <== sockops bpf_sock_map_update(bpf helper tcp_bpf_update_proto() <== update sk_prot ''' When the server has MPTCP enabled but the client sends a TCP SYN without MPTCP, subflow_syn_recv_so a fallback on the subflow, replacing the subflow sk's sk_prot with the native sk_prot. ''' subflow_syn_recv_sock() subflow_ulp_fallback() subflow_drop_ctx() mptcp_subflow_ops_undo_override() ''' Then, this subflow can be normally used by sockmap, which replaces the native sk_prot with sockmap's custom sk_prot. The when the user executes accept::mptcp_stream_accept::mptcp_fallback_tcp_ops(). Here, it uses sk->sk_prot to compare with the native sk_prot, but this is incorrect sockmap is used, as we may incorrectly set sk->sk_socket->ops. This fix uses the more generic sk_family for the comparison instead. Additionally, this also preven from occurring: result from ./scripts/decode_stacktrace.sh: ------------[cut here]------------ WARNING: CPU: 0 PID: 337 at net/mptcp/protocol.c:68 mptcp_stream_accep (net/mptcp/protocol.c:4005) Modules linked in: ... PKRU: 55555554 Call Trace: <TASK> do_accept (net/socket.c:1989) __sys_accept4 (net/socket.c:2028 net/socket __x64_sys_accept (net/socket.c:2067) x64_sys_call (arch/x86/entry/syscall_64.c:41) do_syscall_64 (arch/x86/entry/syscall_64.c:63 arch/x86/entry/syscall_64.c:94)

	entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) RIP: 0033:0x7f87ac92b83d ---[end trace 0000000000000000]---
CVE-2025-68228	In the Linux kernel, the following vulnerability has been resolved: drm/plane: Fix create_in_format_blob() return value create_in_format_blob() is either supposed to pointer or an error, but never NULL. The caller will dereference the blob when it is not an error, and thus will oops if NULL returned. Return proper error values in th cases.
CVE-2025-68229	In the Linux kernel, the following vulnerability has been resolved: scsi: target: tcm_loop: Fix segfault in tcm_loop_tpg_address_show() If the allocation of tl_hba->sh tcm_loop_driver_probe() and we attempt to dereference it in tcm_loop_tpg_address_show() we will get a segfault, see below for an example. So, check tl_hba->sh b dereferencing it. Unable to allocate struct scsi_host BUG: kernel NULL pointer dereference, address: 0000000000000194 #PF: supervisor read access in kernel mod error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 1 PID: 8356 Comm: tokio-runtime-w Not tainted 6.6.104.2-4.azl3 # name: Microsoft Corporation Virtual Machine/Virtual Machine, BIOS Hyper-V UEFI Release v4.1 09/28/2024 RIP: 0010:tcm_loop_tpg_address_show+0x2e/0x50 [tcm_ Trace: <TASK> configfs_read_iter+0x12d/0x1d0 [configfs] vfs_read+0x1b5/0x300 ksys_read+0x6f/0xf0 ...
CVE-2025-68230	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix gpu page fault after hibernation on PF passthrough On PF passthrough environm hibernate and then resume, coralgemm will cause gpu page fault. Mode1 reset happens during hibernate, but partition mode is not restored on resume, register mmCP_HYP_XCP_CTL and mmCP_PSP_XCP_CTL is not right after resume. When CP access the MQD BO, wrong stride size is used, this will cause out of bound acces BO, resulting page fault. The fix is to ensure gfx_v9_4_3_switch_compute_partition() is called when resume from a hibernation. KFD resume is called separately dur recovery or resume from suspend sequence. Hence it's not required to be called as part of partition switch. (cherry picked from commit 5d1b32cfe4a676fe552416cb5ae847b215463a1a)
CVE-2025-68231	In the Linux kernel, the following vulnerability has been resolved: mm/mempool: fix poisoning order>0 pages with HIGHMEM The kernel test has reported: BUG: un page fault for address: fffba000 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page *pde = 03171067 *pte = 00000000 Oops [#1] CPU: 0 UID: 0 PID: 1 Comm: swapper/0 Tainted: G T 6.18.0-rc2-00031-gec7f31b2a2d3 #1 NONE a1d066dfe789f54bc7645c7989957d2bdee593ca Tainted: [T]=RANDSTRUCT Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 EIP: memset (arch/x86/include/asm/string_3 arch/x86/lib/memcpy_32.c:17) Code: a5 8b 4d f4 83 e1 03 74 02 f3 a4 83 c4 04 5e 5f 5d 2e e9 73 41 01 00 90 90 90 3e 8d 74 26 00 55 89 e5 57 56 89 c6 89 d0 89 89 f0 5e 5f 5d 2e e9 53 41 01 00 cc cc cc 55 89 e5 53 57 56 EAX: 0000006b EBX: 00000015 ECX: 001fefff EDX: 0000006b ESI: fffb9000 EDI: fffba000 EBP: c611fbf c611fbe8 DS: 007b ES: 007b FS: 0000 GS: 0000 SS: 0068 EFLAGS: 00010287 CR0: 80050033 CR2: fffba000 CR3: 0316e000 CR4: 00040690 Call Trace: poison_elen (mm/mempool.c:83 mm/mempool.c:102) mempool_init_node (mm/mempool.c:142 mm/mempool.c:226) mempool_init_noprof (mm/mempool.c:250 (discriminator 1 mempool_alloc_pages (mm/mempool.c:640) bio_integrity_initfn (block/bio-integrity.c:483 (discriminator 8)) ? mempool_alloc_pages (mm/mempool.c:640) do_one_i (init/main.c:1283) Christoph found out this is due to the poisoning code not dealing properly with CONFIG_HIGHMEM because only the first page is mapped but the potentially high-order page is accessed. We could give up on HIGHMEM here, but it's straightforward to fix this with a loop that's mapping, poisoning or checking ar individual pages.
CVE-2025-68232	In the Linux kernel, the following vulnerability has been resolved: veth: more robust handing of race to avoid txq getting stuck Commit dc82a33297fc ("veth: apply backpressure on full ptr_ring to reduce TX drops") introduced a race condition that can lead to a permanently stalled TXQ. This was observed in production on ARM (Ampere Altra Max). The race occurs in veth_xmit(). The producer observes a full ptr_ring and stops the queue (netif_tx_stop_queue()). The subsequent conditional intended to re-wake the queue if the consumer had just emptied it (if (__ptr_ring_empty(...)) netif_tx_wake_queue()), can fail. This leads to a "lost wakeup" where th remains stopped (QUEUE_STATE_DRV_XOFF) and traffic halts. This failure is caused by an incorrect use of the __ptr_ring_empty() API from the producer side. As not comments, this check is not guaranteed to be correct if a consumer is operating on another CPU. The empty test is based on ptr_ring->consumer_head, making it r for the consumer. Using this check from the producer side is fundamentally racy. This patch fixes the race by adopting the more robust logic from an earlier versio patchset, which always flushed the peer: (1) In veth_xmit(), the racy conditional wake-up logic and its memory barrier are removed. Instead, after stopping the que unconditionally call __veth_xdp_flush(rq). This guarantees that the NAPI consumer is scheduled, making it solely responsible for re-waking the TXQ. This handles th veth_poll() consumes all packets and completes NAPI *before* veth_xmit() on the producer side has called netif_tx_stop_queue. The __veth_xdp_flush(rq) will obser rx_notify_masked is false and schedule NAPI. (2) On the consumer side, the logic for waking the peer TXQ is moved out of veth_xdp_rcv() and placed at the end of t function. This placement is part of fixing the race, as the netif_tx_queue_stopped() check must occur after rx_notify_masked is potentially set to false during NAPI c This handles the race where veth_poll() consumes all packets, but haven't finished (rx_notify_masked is still true). The producer veth_xmit() stops the TXQ and __veth_xdp_flush(rq) will observe rx_notify_masked is true, meaning not starting NAPI. Then veth_poll() change rx_notify_masked to false and stops NAPI. Before ex veth_poll() will observe TXQ is stopped and wake it up.
CVE-2025-68233	In the Linux kernel, the following vulnerability has been resolved: drm/tegra: Add call to put_pid() Add a call to put_pid() corresponding to get_task_pid(). host1x_memory_context_alloc() does not take ownership of the PID so we need to free it here to avoid leaking. [mperttunen@nvidia.com: reword commit message]
CVE-2025-68234	In the Linux kernel, the following vulnerability has been resolved: io_uring/cmd_net: fix wrong argument types for skb_queue_splice() If timestamp retriving needs t and the local list of SKB's already has entries, then it's spliced back into the socket queue. However, the arguments for the splice helper are transposed, causing ex wrong direction of splicing into the on-stack list. Fix that up.
CVE-2025-68235	In the Linux kernel, the following vulnerability has been resolved: nouveau/firmware: Add missing kfree() of nvkm_falcon_fw::boot nvkm_falcon_fw::boot is allocate frees it. This causes a kmemleak warning. Make sure this data is deallocated.
CVE-2025-68236	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: ufs-qcom: Fix UFS OCP issue during UFS power down (PC=3) According to UFS specificat power-off sequence for a UFS device includes: - Sending an SSU command with Power_Condition=3 and await a response. - Asserting RST_N low. - Turning off REF_ off VCC. - Turning off VCCQ/VCCQ2. As part of ufs shutdown, after the SSU command completion, asserting hardware reset (HWRST) triggers the device firmware to execute its reset routine. This routine initializes hardware blocks and takes a few milliseconds to complete. During this time, the ICCQ draws a large current. This la current may cause issues for the regulator which is supplying power to UFS, because the turn off request from UFS driver to the regulator framework will be immed followed by low power mode(LPM) request by regulator framework. This is done by framework because UFS which is the only client is requesting for disable. So if th in the process of shutting down while ICCQ exceeds LPM current thresholds, and LPM mode is activated in hardware during this state, it may trigger an overcurrent (OCP) fault in the regulator. To prevent this, a 10ms delay is added after asserting HWRST. This allows the reset operation to complete while power rails remain act high-power mode. Currently there is no way for Host to query whether the reset is completed or not and hence this the delay is based on experiments with Qualcor controllers across multiple UFS vendors.
CVE-2025-68191	In the Linux kernel, the following vulnerability has been resolved: udp_tunnel: use netdev_warn() instead of netdev_WARN() netdev_WARN() uses WARN/WARN_ON backtrace along with file and line information. In this case, udp_tunnel_nic_register() returning an error is just a failed operation, not a kernel bug. udp_tunnel_nic_r fail due to a memory allocation failure (kzalloc() or udp_tunnel_nic_alloc()). This is a normal runtime error and not a kernel bug. Replace netdev_WARN() with netde accordingly.
CVE-2025-68190	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/atom: Check kcalloc() for WS buffer in amdgpu_atom_execute_table_locked() kcallo When WS is non-zero and allocation fails, ectx.ws remains NULL while ectx.ws_size is set, leading to a potential NULL pointer dereference in atom_get_src_int() whe WS entries. Return -ENOMEM on allocation failure to avoid the NULL dereference.
	In the Linux kernel, the following vulnerability has been resolved: mptcp: Initialise rcv_mss before calling tcp_send_active_reset() in mptcp_do_fastclose(). syzbot re by-zero in __tcp_select_window() by MPTCP socket. [0] We had a similar issue for the bare TCP and fixed in commit 499350a5a6e7 ("tcp: initialize rcv_mss to TCP_M instead of 0"). Let's apply the same fix to mptcp_do_fastclose(). [0]: Oops: divide error: 0000 [#1] SMP KASAN PTI CPU: 0 UID: 0 PID: 6068 Comm: syz.0.17 Not tain #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/25/2025 RIP: 0010:__tcp_select_window+0x824/0x132 net/ipv4/tcp_output.c:3336 Code: ff ff ff 44 89 f1 d3 e0 89 c1 f7 d1 41 01 cc 41 21 c4 e9 a9 00 00 00 e8 ca 49 01 f8 e9 9c 00 00 00 e8 c0 49 01 f8 44 89 e0 99 <f7 29 d4 48 bb 00 00 00 00 00 fc ff df e9 80 00 00 00 RSP: 0018:ffffc90003017640 EFLAGS: 00010293 RAX: 0000000000000000 RBX: 0000000000000000 RCX: ffff88

CVE-2025-68291	RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffc90003017730 R08: ffff888033268143 R09: 1ffff1100664d028 R10: dfffc000 ffffed100664d029 R12: 0000000000000000 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 000055557faa0500(0000) GS:ffff888126135000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f64a1912ff8 CR3: 0000000072122000 C 00000000003526f0 Call Trace: <TASK> tcp_select_window net/ipv4/tcp_output.c:281 [inline] __tcp_transmit_skb+0xbc7/0x3aa0 net/ipv4/tcp_output.c:1568 tcp_tra net/ipv4/tcp_output.c:1649 [inline] tcp_send_active_reset+0x2d1/0x5b0 net/ipv4/tcp_output.c:3836 mptcp_do_fastclose+0x27e/0x380 net/mptcp/protocol.c:2793 mptcp_disconnect+0x238/0x710 net/mptcp/protocol.c:3253 mptcp_sendmsg_fastopen+0x2f8/0x580 net/mptcp/protocol.c:1776 mptcp_sendmsg+0x1774/0x1980 net/mptcp/protocol.c:1855 sock_sendmsg_nosec net/socket.c:727 [inline] __sock_sendmsg+0xe5/0x270 net/socket.c:742 __sys_sendto+0x3bd/0x520 net/socket.c: __do_sys_sendto net/socket.c:2251 [inline] __se_sys_sendto net/socket.c:2247 [inline] __x64_sys_sendto+0xde/0x100 net/socket.c:2247 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0xfa0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f66e99 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 d8 64 89 01 48 RSP: 002b:00007ffff9acedb8 EFLAGS: 00000246 ORIG_RAX: 000000000000002c RAX: ffffffffffffffda RBX: 00007f66e9be5fa0 RCX: 00007f66e998f74 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000003 RBP: 00007ffff9acee10 R08: 0000000000000000 R09: 0000000000000000 R10: 00000000 R11: 0000000000000246 R12: 0000000000000001 R13: 00007f66e9be5fa0 R14: 00007f66e9be5fa0 R15: 0000000000000006 </TASK>
CVE-2025-68189	In the Linux kernel, the following vulnerability has been resolved: drm/msm: Fix GEM free for imported dma-bufs Imported dma-bufs also have obj->resv != &obj-> should check both this condition in addition to flags for handling the _NO_SHARE case. Fixes this splat that was reported with IRIS video playback: ------------[cut her WARNING: CPU: 3 PID: 2040 at drivers/gpu/drm/msm/msm_gem.c:1127 msm_gem_free_object+0x1f8/0x264 [msm] CPU: 3 UID: 1000 PID: 2040 Comm: .gnome-sh tainted 6.17.0-rc7 #1 PREEMPT pstate: 81400005 (Nzcv daif +PAN -UAO -TCO +DIT -SSBS BTYPE=--) pc : msm_gem_free_object+0x1f8/0x264 [msm] lr : msm_gem_free_object+0x138/0x264 [msm] sp : ffff800092a1bb30 x29: ffff800092a1bb80 x28: ffff800092a1bce8 x27: ffffbc702dbdbe08 x26: 0000000000000008 0000000000000009 x24: 00000000000000a6 x23: ffff00083c72f850 x22: ffff00083c72f868 x21: ffff00087e69f200 x20: ffff00087e69f330 x19: ffff00084d157ae0 x 0000000000000000 x17: 0000000000000000 x16: ffffbc704bd46b80 x15: 0000ffffd0959540 x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000 ffffbc702e6cdb48 x10: 0000000000000000 x9 : 000000000000003f x8 : ffff800092a1ba90 x7 : 0000000000000000 x6 : 0000000000000020 x5 : ffffbc704bd46c4 fffffdffe102cf60 x3 : 0000000000400032 x2 : 0000000000020000 x1 : ffff00087e6978e8 x0 : ffff00087e6977e8 Call trace: msm_gem_free_object+0x1f8/0x264 [m drm_gem_object_free+0x1c/0x30 [drm] drm_gem_object_handle_put_unlocked+0x138/0x150 [drm] drm_gem_object_release_handle+0x5c/0xcc [drm] drm_gem_handle_delete+0x68/0xbc [drm] drm_gem_close_ioctl+0x34/0x40 [drm] drm_ioctl_kernel+0xc0/0x130 [drm] drm_ioctl+0x360/0x4e0 [drm] __arm64_sys_ioctl+0xac/0x104 invoke_syscall+0x48/0x104 el0_svc_common.constprop.0+0x40/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x34/0xec el0t_64_sync_handler+0xa0/0xe4 el0t_64_sync+0x198/0x19c ---[end trace 0000000000000000]--- ------------[cut here]------------ Patchwork: https://patchwork.freedesktop.org/patch/676273/
CVE-2025-67999	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Stefano Lissa Newsletter newsletter allows Blind SQL Injectio affects Newsletter: from n/a through <= 9.0.9.
CVE-2025-68188	In the Linux kernel, the following vulnerability has been resolved: tcp: use dst_dev_rcu() in tcp_fastopen_active_disable_ofo_check() Use RCU to avoid a pair of aton and a potential UAF on dst_dev()->flags.
CVE-2025-68187	In the Linux kernel, the following vulnerability has been resolved: net: mdio: Check regmap pointer returned by device_node_to_regmap() The call to device_node_t airoha_mdio_probe() can return an ERR_PTR() if regmap initialization fails. Currently, the driver stores the pointer without validation, which could lead to a crash if i dereferenced. Add an IS_ERR() check and return the corresponding error code to make the probe path more robust.
CVE-2025-68186	In the Linux kernel, the following vulnerability has been resolved: ring-buffer: Do not warn in ring_buffer_map_get_reader() when reader catches up The function ring_buffer_map_get_reader() is a bit more strict than the other get reader functions, and except for certain situations the rb_get_reader_page() should not return N does, it triggers a warning. This warning was triggering but after looking at why, it was because another acceptable situation was happening and it wasn't checked reader catches up to the writer and there's still data to be read on the reader page, then the rb_get_reader_page() will return NULL as there's no new page to get. I situation, the reader page should not be updated and no warning should trigger.
CVE-2025-68315	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to detect potential corrupted nid in free_nid_list As reported, on-disk footer.ino and foote same and out-of-range, let's add sanity check on f2fs_alloc_nid() to detect any potential corruption in free_nid_list.
CVE-2025-43506	A logic error was addressed with improved error handling. This issue is fixed in macOS Tahoe 26.1. iCloud Private Relay may not activate when more than one user at the same time.
CVE-2025-67989	Server-Side Request Forgery (SSRF) vulnerability in LMPixels Kerge kerge allows Server Side Request Forgery.This issue affects Kerge: from n/a through <= 4.1.3.
CVE-2023-53741	Screen SFT DAB 1.9.3 contains a weak session management vulnerability that allows attackers to bypass authentication controls by reusing IP address-bound sessi Attackers can exploit the vulnerable API by intercepting and reusing established sessions to remove user accounts without proper authorization.
CVE-2025-67693	Rejected reason: Not used
CVE-2025-67692	Rejected reason: Not used
CVE-2025-67691	Rejected reason: Not used
CVE-2025-67690	Rejected reason: Not used
CVE-2025-67689	Rejected reason: Not used
CVE-2025-67688	Rejected reason: Not used
CVE-	

2025-67687	Rejected reason: Not used
CVE-2025-67686	Rejected reason: Not used
CVE-2025-67719	Ibexa is a composable end-to-end DXP (Digital Experience Platform). Versions 5.0.0-beta1 through 5.0.3 do not have password validation. During the transition fror error was introduced into validation code which causes the validation of the previous password not to run as expected. This makes it possible for a logged in user t password in the back office without knowing the previous password. For example, if a user logs into their account and walks away without locking their workstation could access the unattended session and change the password, therefore locking the legitimate user out. This issue is fixed in version 5.0.4.
CVE-2025-67718	Form.io is a combined Form and API platform for Serverless applications. Versions 3.5.6 and below and 4.0.0-rc.1 through 4.4.2 contain a flaw in path handling whi an attacker to access protected API endpoints by sending a crafted request path. An unauthenticated or unauthorized request could retrieve data from endpoints t protected. This issue is fixed in versions 3.5.7 and 4.4.3.
CVE-2025-67717	ZITADEL is an open-source identity infrastructure tool. Versions 2.44.0 through 3.4.4 and 4.0.0-rc.1 through 4.7.1 disclose the total number of instance users to aut users, regardless of their specific permissions. While this does not leak individual user data or PII, disclosing the total user count via the totalResult field constitutes information disclosure vulnerability that may be sensitive in certain contexts. This issue is fixed in versions 3.4.5 and 4.7.2.
CVE-2025-67713	Miniflux 2 is an open source feed reader. Versions 2.2.14 and below treat redirect_url as safe when url.Parse(...).IsAbs() is false, enabling phishing flows after login. relative URLs like //ikotaslabs.com have an empty scheme and pass that check, allowing post-login redirects to attacker-controlled sites. This issue is fixed in versi
CVE-2025-67514	Rejected reason: Vulnerability is dependency-based.
CVE-2025-67512	Rejected reason: The vulnerability is dependency-based.
CVE-2025-67513	FreePBX Endpoint Manager is a module for managing telephony endpoints in FreePBX systems. Versions prior to 16.0.96 and 17.0.1 through 17.0.9 have a weak de password. By default, this is a 6 digit numeric value which can be brute forced. (This is the app_password parameter). Depending on local configuration, this passw the extension, voicemail, user manager, DPMA or EPM phone admin password. This issue is fixed in versions 16.0.96 and 17.0.10.
CVE-2025-13923	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2025-12731	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2025-66474	XWiki Rendering is a generic rendering system that converts textual input in a given syntax (wiki syntax, HTML, etc) into another syntax (XHTML, etc). Versions 16. below, 17.0.0-rc-1 through 17.4.2 and 17.5.0-rc-1 through 17.5.0 have insufficient protection against {{/html}} injection, which attackers can exploit through RCE. can edit their own profile or any other document can execute arbitrary script macros, including Groovy and Python macros, which enable remote code execution as unrestricted read and write access to all wiki contents. This issue is fixed in versions 16.10.10, 17.4.3 and 17.6.0-rc-1.
CVE-2025-66473	XWiki is an open-source wiki software platform. Versions 16.10.10 and below, 17.0.0-rc-1 through 17.4.3 and 17.5.0-rc-1 through 17.6.0 contain a REST API which d enforce any limits for the number of items that can be requested in a single request at the moment. Depending on the number of pages in the wiki and the memor configuration, this can lead to slowness and unavailability of the wiki. As an example, the /rest/wikis/xwiki/spaces resource returns all spaces on the wiki by default basically all pages. This issue is fixed in versions 17.4.4 and 16.10.11.
CVE-2025-66472	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Versions 6.2-milestone-1 through 16.10.9 and 17.0.0-rc-1 throu both XWiki Platform Flamingo Skin Resources and XWiki Platform Web Templates are vulnerable to a reflected XSS attack through a deletion confirmation message attacker-supplied script is executed when the victim clicks the "No" button. This issue is fixed in versions 16.10.10 and 17.4.2 of both XWiki Platform Flamingo Skin and XWiki Platform Web Templates.
CVE-2025-65291	Aqara Hub devices including Hub M2 4.3.6_0027, Hub M3 4.3.6_0025, Camera Hub G3 4.1.9_0027 fail to validate server certificates in TLS connections for discover CoAP gateway communications, enabling man-in-the-middle attacks on device control and monitoring.
CVE-2024-58285	Chyrp 2.5.2 contains a stored cross-site scripting vulnerability that allows authenticated users to inject malicious scripts into post titles. Attackers can craft payload field that will execute when the post is viewed by other users, potentially stealing session cookies or performing client-side attacks.
CVE-2024-58284	PopojiCMS 2.0.1 contains an authenticated remote command execution vulnerability that allows administrative users to inject malicious PHP code through the meta endpoint. Attackers can log in and modify the meta content to create a web shell that executes arbitrary system commands through a GET parameter.
CVE-2024-58282	Serendipity 2.5.0 contains a remote code execution vulnerability that allows authenticated administrators to upload malicious PHP files through the media upload f Attackers can exploit the file upload mechanism by creating a PHP shell with a command execution form that enables arbitrary system command execution on the
CVE-2024-58281	Dotclear 2.29 contains a remote code execution vulnerability that allows authenticated attackers to upload malicious PHP files through the media upload functiona can exploit the file upload process by crafting a PHP shell with a command execution form to gain system access through the uploaded file.
CVE-2024-58280	CMSimple 5.15 contains a remote command execution vulnerability that allows authenticated attackers to modify file extensions and upload malicious PHP files. At append ',php' to Extensions_userfiles and upload a shell script to the media directory to execute arbitrary code on the server.
CVE-2024-58279	appRain CMF 4.0.5 contains an authenticated remote code execution vulnerability that allows administrative users to upload malicious PHP files through the filema endpoint. Attackers can leverage authenticated access to generate a web shell with command execution capabilities by uploading a crafted PHP file to the site's up directory.
CVE-	

2023-53776	Screen SFT DAB 1.9.3 contains an authentication bypass vulnerability that allows attackers to exploit weak session management by reusing IP-bound session ident Attackers can issue unauthorized requests to the device management API by leveraging the session binding mechanism to perform critical operations on the transı
CVE-2023-53775	Screen SFT DAB 1.9.3 contains an authentication bypass vulnerability that allows attackers to change user passwords by exploiting weak session management con Attackers can reuse IP-bound session identifiers to issue unauthorized requests to the userManager API and modify user credentials without proper authentication.
CVE-2025-67694	Rejected reason: Not used
CVE-2025-64701	QND Premium/Advance/Standard Ver.11.0.9i and prior contains a privilege escalation vulnerability, which may allow a user who can log in to a Windows system wit product to gain administrator privileges. As a result, sensitive information may be accessed or altered, and arbitrary actions may be performed.
CVE-2024-8273	Authentication Bypass by Spoofing vulnerability in HYPR Server allows Identity Spoofing.This issue affects Server: before 10.1.
CVE-2024-58289	Microweber 2.0.15 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts into user profile fields. Attacker script payloads in the first name field that will execute when the profile is viewed by other users, potentially stealing session cookies and executing arbitrary JavaS
CVE-2024-58306	minaliC 2.0.0 contains a denial of service vulnerability that allows remote attackers to crash the web server by sending oversized GET requests. Attackers can send requests with excessive data to overwhelm the server and cause service interruption.
CVE-2024-58303	FoF Pretty Mail 1.1.2 contains a server-side template injection vulnerability that allows administrative users to inject malicious code into email templates. Attackers system commands by inserting crafted template expressions that trigger arbitrary code execution during email generation.
CVE-2024-58302	FoF Pretty Mail 1.1.2 contains a local file inclusion vulnerability that allows administrative users to include arbitrary server files in email templates. Attackers can ex template settings by inserting file inclusion payloads to read sensitive system files like /etc/passwd during email generation.
CVE-2024-58301	Purei CMS 1.0 contains a time-based blind SQL injection vulnerability that allows attackers to manipulate database queries through unfiltered user input parameter can exploit vulnerable endpoints like getAllParks.php and events-ajax.php by injecting crafted SQL payloads to potentially extract or modify database information.
CVE-2024-58300	Siklu MultiHaul TG series devices before version 2.0.0 contain an unauthenticated vulnerability that allows remote attackers to retrieve randomly generated creder network request. Attackers can send a specific hex-encoded command to port 12777 to obtain username and password, enabling direct SSH access to the device.
CVE-2024-58298	Compuware iStrobe Web 20.13 contains a pre-authentication remote code execution vulnerability that allows unauthenticated attackers to upload malicious JSP file path traversal in the file upload form. Attackers can exploit the 'fileName' parameter to upload a web shell and execute arbitrary commands by sending POST requ uploaded JSP endpoint.
CVE-2024-58297	PyroCMS v3.0.1 contains a stored cross-site scripting vulnerability in the admin redirects configuration that allows attackers to inject malicious scripts. Attackers ca payload in the 'Redirect From' field to execute arbitrary JavaScript when administrators view the redirects page.
CVE-2024-58296	CE Phoenix v3.0.1 contains a stored cross-site scripting vulnerability in the currencies administration panel that allows attackers to inject malicious scripts. Attacke XSS payloads in the title field to execute arbitrary JavaScript when administrators view the currencies page.
CVE-2024-58295	ElkArte Forum 1.1.9 contains a remote code execution vulnerability that allows authenticated administrators to upload malicious PHP files through the theme instal process. Attackers can upload a ZIP archive with a PHP file containing system commands, which can then be executed by accessing the uploaded file in the theme
CVE-2024-58293	Akaunting 3.1.8 contains a server-side template injection vulnerability that allows authenticated administrators to execute template expressions in multiple form ir Attackers can inject template payloads in items, taxes, transactions, and vendor name fields to perform arithmetic operations and string manipulations.
CVE-2024-58292	XMB Forum 1.9.12.06 contains a persistent cross-site scripting vulnerability that allows authenticated administrators to inject malicious JavaScript into templates a settings. Attackers can insert XSS payloads in footer templates and news ticker fields, enabling script execution for all forum users when pages are rendered.
CVE-2024-58291	Flatboard 3.2 contains a stored cross-site scripting vulnerability that allows authenticated administrators to inject malicious scripts in forum information fields. Atta insert JavaScript payloads that execute when other users view the forum, potentially stealing session cookies and executing client-side scripts.
CVE-2024-58290	Xhibiter NFT Marketplace 1.10.2 contains a SQL injection vulnerability in the collections endpoint that allows attackers to manipulate database queries through the parameter. Attackers can exploit boolean-based, time-based, and UNION-based SQL injection techniques to potentially extract or manipulate database information crafted payloads to the collections page.
CVE-2024-58288	Genexus Protection Server 9.7.2.10 contains an unquoted service path vulnerability in the protsrvservice Windows service configuration. Attackers can exploit the binary path to execute arbitrary code with elevated LocalSystem privileges by placing malicious executables in specific file system locations.
CVE-2025-65474	An arbitrary file rename vulnerability in the /admin/manager.php component of EasyImages 2.0 v2.8.6 and below allows attackers to execute arbitrary code via ren file to a SVG format.
CVE-2024-58287	reNgine 2.2.0 contains a command injection vulnerability in the nmap_cmd parameter of scan engine configuration that allows authenticated attackers to execute commands. Attackers can modify the nmap_cmd parameter with malicious base64-encoded payloads to achieve remote code execution during scan engine config
CVE-	

2024-58286	dizqueTV 1.5.3 contains a remote code execution vulnerability that allows attackers to inject arbitrary commands through the FFMPEG Executable Path settings. At modify the executable path with shell commands to read system files like /etc/passwd by exploiting improper input validation.
CVE-2025-66590	In AzeoTech DAQFactory release 20.7 (Build 2555), an Out-of-bounds Write vulnerability can be exploited by an attacker to cause the program to write data past th allocated memory buffer. This can lead to arbitrary code execution or a system crash.
CVE-2025-66589	In AzeoTech DAQFactory release 20.7 (Build 2555), an Out-of-bounds Read vulnerability can be exploited by an attacker to cause the program to read data past th allocated buffer. This could allow an attacker to disclose information or cause a system crash.
CVE-2025-66588	In AzeoTech DAQFactory release 20.7 (Build 2555), an Access of Uninitialized Pointer vulnerability can be exploited by an attacker which can lead to arbitrary code
CVE-2025-66587	In AzeoTech DAQFactory release 20.7 (Build 2555), the affected application is vulnerable to memory corruption while parsing specially crafted .ctl files. This could a attacker to execute code in the context of the current process.
CVE-2025-66586	In AzeoTech DAQFactory release 20.7 (Build 2555), an Access of Resource Using Incompatible Type vulnerability can be exploited to cause memory corruption whil specially crafted .ctl files. This could allow an attacker to execute code in the context of the current process.
CVE-2025-66585	In AzeoTech DAQFactory release 20.7 (Build 2555), a Use After Free vulnerability can be exploited to cause memory corruption while parsing specially crafted .ctl f could allow an attacker to execute code in the context of the current process.
CVE-2025-66584	In AzeoTech DAQFactory release 20.7 (Build 2555), a Stack-Based Buffer Overflow vulnerability can be exploited to cause memory corruption while parsing speciall files. This could allow an attacker to execute code in the context of the current process.
CVE-2025-12532	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this car been removed to prevent accidental usage.
CVE-2025-14281	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2025-13977. Reason: This candidate is a reservation duplicate of CVE-2025 Notes: All CVE users should reference CVE-2025-13977 instead of this candidate. All references and descriptions in this candidate have been removed to prevent a usage.
CVE-2025-14046	An improper neutralization of input vulnerability was identified in GitHub Enterprise Server that allowed user-supplied HTML to inject DOM elements with IDs that c server-initialized data islands. These collisions could overwrite or shadow critical application state objects used by certain Project views, leading to unintended serv requests or other unauthorized backend interactions. Successful exploitation requires an attacker to have access to the target GitHub Enterprise Server instance a privileged user to view crafted malicious content that includes conflicting HTML elements. This vulnerability affected all versions of GitHub Enterprise Server prior t 3.17.9, 3.16.12, 3.15.16, and 3.14.21.
CVE-2025-13912	Multiple constant-time implementations in wolfSSL before version 5.8.4 may be transformed into non-constant-time binary by LLVM optimizations, which can poten observable timing discrepancies and lead to information disclosure through timing side-channel attacks.
CVE-2025-65828	An unauthenticated attacker within proximity of the Meatmeet device can issue several commands over Bluetooth Low Energy (BLE) to these devices which would Denial of Service. These commands include: shutdown, restart, clear config. Clear config would disassociate the current device from its user and would require re-c to re-enable the device. As a result, the end user would be unable to receive updates from the Meatmeet base station which communicates with the cloud services device had been fixed or turned back on.
CVE-2023-53740	Screen SFT DAB 1.9.3 contains an authentication bypass vulnerability that allows attackers to change the admin password without providing the current credential can exploit the userManager.cgx endpoint by sending a crafted JSON request with a new MD5-hashed password to directly modify the admin account.
CVE-2024-58308	Quick.CMS 6.7 contains a SQL injection vulnerability that allows unauthenticated attackers to bypass login authentication by manipulating the login form. Attackers specific SQL payloads like ' or '1'='1 to gain unauthorized administrative access to the system.
CVE-2020-36902	UBICOD Medivision Digital Signage 1.5.1 contains an authorization bypass vulnerability that allows normal users to escalate privileges by manipulating the 'ft[grp]' Attackers can send a GET request to /html/user with 'ft[grp]' set to integer value '3' to gain super admin rights without authentication.
CVE-2025-34419	MailEnable versions prior to 10.54 contain an unsafe DLL loading vulnerability that can lead to local arbitrary code execution. The MailEnable administrative execut to load MEAISM.DLL from its installation directory without sufficient integrity validation or a secure search order. A local attacker with write access to that directory malicious MEAISM.DLL, which is then loaded when the executable starts, resulting in execution of attacker-controlled code with the privileges of the process.
CVE-2025-34418	MailEnable versions prior to 10.54 contain an unsafe DLL loading vulnerability that can lead to local arbitrary code execution. The MailEnable administrative execut to load MEAIMF.DLL from its installation directory without sufficient integrity validation or a secure search order. A local attacker with write access to that directory malicious MEAIMF.DLL, which is then loaded when the executable starts, resulting in execution of attacker-controlled code with the privileges of the process.
CVE-2025-34417	MailEnable versions prior to 10.54 contain an unsafe DLL loading vulnerability that can lead to local arbitrary code execution. The MailEnable administrative execut to load MEAISO.DLL from its installation directory without sufficient integrity validation or a secure search order. A local attacker with write access to that directory malicious MEAISO.DLL, which is then loaded when the executable starts, resulting in execution of attacker-controlled code with the privileges of the process.
CVE-2025-34416	MailEnable versions prior to 10.54 contain an unsafe DLL loading vulnerability that can lead to local arbitrary code execution. The MailEnable administrative execut to load MEAIPO.DLL from its installation directory without sufficient integrity validation or a secure search order. A local attacker with write access to that directory malicious MEAIPO.DLL, which is then loaded when the executable starts, resulting in execution of attacker-controlled code with the privileges of the process.
CVE-2025-34410	1Panel versions 1.10.33 - 2.0.15 contain a cross-site request forgery (CSRF) vulnerability in the Change Username functionality available from the settings panel (/settings/panel). The endpoint does not implement CSRF protections such as anti-CSRF tokens or Origin/Referer validation. An attacker can craft a malicious webp submits a username-change request; when a victim visits the page while authenticated, the browser includes valid session cookies and the request succeeds. This attacker to change the victim's 1Panel username without consent. After the change, the victim is logged out and unable to log in with the previous username, resu account lockout and denial of service.

CVE-2025-34395	Barracuda Service Center, as implemented in the RMM solution, in versions prior to 2025.1.1, exposes a .NET Remoting service in which an unauthenticated attack a method vulnerable to path traversal to read arbitrary files. This vulnerability can be escalated to remote code execution by retrieving the .NET machine keys.
CVE-2025-34394	Barracuda Service Center, as implemented in the RMM solution, in versions prior to 2025.1.1, exposes a .NET Remoting service that is insufficiently protected agair deserialization of arbitrary types. This can lead to remote code execution.
CVE-2025-34393	Barracuda Service Center, as implemented in the RMM solution, in versions prior to 2025.1.1, does not correctly verify the name of an attacker-controlled WSDL se to insecure reflection. This can result in remote code execution through either invocation of arbitrary methods or deserialization of untrusted types.
CVE-2025-34392	Barracuda Service Center, as implemented in the RMM solution, in versions prior to 2025.1.1, does not verify the URL defined in an attacker-controlled WSDL that i by the application. This can lead to arbitrary file write and remote code execution via webshell upload.
CVE-2025-8110	Improper Symbolic link handling in the PutContents API in Gogs allows Local Execution of Code.
CVE-2025-41358	Direct Object Reference Vulnerability (IDOR) in i2A's CronosWeb, in versions prior to 25.00.00.12, inclusive. This vulnerability could allow an authenticated attacker other users' documents by manipulating the ‘documentCode‘ parameter in '/CronosWeb/Modulos/Personas/DocumentosPersonales/AdjuntarDocumentosPersonas'.
CVE-2025-13953	Bypass vulnerability in the authentication method in the GTT Tax Information System application, related to the Active Directory (LDAP) login method. Authenticati performed through a local WebSocket, but the web application does not properly validate the authenticity or origin of the data received, allowing an attacker with a local machine or internal network to impersonate the legitimate WebSocket and inject manipulated information. Exploiting this vulnerability could allow an attacker authenticate as any user in the domain, without the need for valid credentials, compromising the confidentiality, integrity, and availability of the application and its
CVE-2025-7073	A local privilege escalation vulnerability in Bitdefender Total Security 27.0.46.231 allows low-privileged attackers to elevate privileges. The issue arises from bdservicehost.exe deleting files from a user-writable directory (C:\ProgramData\Atc\Feedback) without proper symbolic link validation, enabling arbitrary file deleti is chained with a file copy operation during network events and a filter driver bypass via DLL injection to achieve arbitrary file copy and code execution as elevated
CVE-2025-9315	An unauthenticated device registration vulnerability, caused by Improperly Controlled Modification of Dynamically-Determined Object Attributes, has been identifie MXsecurity Series. An unauthenticated remote attacker can exploit this vulnerability by sending a specially crafted JSON payload to the device's registration endpo /api/v1/devices/register, allowing the attacker to register unauthorized devices without authentication. Although exploiting this vulnerability has limited modificatio there is no impact to the confidentiality and availability of the affected device, as well as no loss of confidentiality, integrity, and availability within any subsequent
CVE-2025-13955	Predictable default Wi-Fi Password in Access Point functionality in EZCast Pro II version 1.17478.146 allows attackers in Wi-Fi range to gain access to the dongle by the default password from observable device identifiers
CVE-2025-13954	Hard-coded cryptographic keys in Admin UI of EZCast Pro II version 1.17478.146 allows attackers to bypass authorization checks and gain full access to the admin
CVE-2025-12952	A privilege escalation vulnerability exists in Google Cloud's Dialogflow CX. Dialogflow agent developers with Webhook editor permission are able to configure Webh Dialogflow service agent access token authentication. This allows the attacker to escalate their privileges from agent-level to project-level, granting them unauthor manage resources in services associated with the project, leading to unexpected costs and resource depletion for the producer project. A fix was applied on the se protect from this vulnerability in February 2025. No customer action is required.
CVE-2025-9571	A remote code execution (RCE) vulnerability exists in Google Cloud Data Fusion. A user with permissions to upload artifacts to a Data Fusion instance can execute within the core AppFabric component. This could allow the attacker to gain control over the Data Fusion instance, potentially leading to unauthorized access to sen modification of data pipelines, and exploration of the underlying infrastructure. The following CDAP versions include the necessary update to protect against this vu 6.10.6+ * 6.11.1+ Users must immediately upgrade to them, or greater ones, available at: https://github.com/cdapio/cdap-build/releases .
CVE-2025-67613	Rejected reason: Not used
CVE-2025-67612	Rejected reason: Not used
CVE-2025-67611	Rejected reason: Not used
CVE-2025-67610	Rejected reason: Not used
CVE-2025-67609	Rejected reason: Not used
CVE-2025-67608	Rejected reason: Not used
CVE-2025-67607	Rejected reason: Not used
CVE-2025-67606	Rejected reason: Not used

CVE-2025-67605	Rejected reason: Not used
CVE-2025-67503	Rejected reason: This CVE is a duplicate of another CVE.
CVE-2025-67501	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. Versions 3.5.4 and below contain an SQL Injection vulnerability i /html/matPat/editar_categoria.php endpoint. The application fails to properly validate and sanitize user inputs in the id_categoria parameter, which allows attackers malicious SQL payloads for direct execution. This issue is fixed in version 3.5.5.
CVE-2025-34420	MailEnable versions prior to 10.54 contain an unsafe DLL loading vulnerability that can lead to local arbitrary code execution. The MailEnable administrative execut to load MEAIAM.DLL from its installation directory without sufficient integrity validation or a secure search order. A local attacker with write access to that directory malicious MEAIAM.DLL, which is then loaded on execution, resulting in attacker-controlled code running with the privileges of the process.
CVE-2025-34421	MailEnable versions prior to 10.54 contain an unsafe DLL loading vulnerability that can lead to local arbitrary code execution. The MailEnable administrative execut to load MEAISP.DLL from its installation directory without sufficient integrity validation or a secure search order. A local attacker with write access to that directory malicious MEAISP.DLL, which is then loaded on execution, resulting in attacker-controlled code running with the privileges of the process.
CVE-2025-34422	MailEnable versions prior to 10.54 contain an unsafe DLL loading vulnerability that can lead to local arbitrary code execution. The MailEnable administrative execut to load MEAIPC.DLL from its installation directory without sufficient integrity validation or a secure search order. A local attacker with write access to that directory malicious MEAIPC.DLL, which is then loaded on execution, resulting in attacker-controlled code running with the privileges of the process.
CVE-2020-36885	Sony IPELA Network Camera 1.82.01 contains a stack buffer overflow vulnerability in the ftpclient.cgi endpoint that allows remote attackers to execute arbitrary co can exploit the vulnerability by sending a crafted POST request with oversized data to the FTP client functionality, potentially causing remote code execution or de
CVE-2020-36901	UBICOD Medivision Digital Signage 1.5.1 contains a cross-site request forgery vulnerability that allows attackers to create administrative user accounts without pro validation. Attackers can craft a malicious web page that submits a form to the /query/user/itSet endpoint to add a new admin user with elevated privileges.
CVE-2020-36900	All-Dynamics Digital Signage System 2.0.2 contains a cross-site request forgery vulnerability that allows attackers to create administrative users without proper re validation. Attackers can craft a malicious web page that automatically submits forms to create a new user with global administrative privileges when a logged-in u page.
CVE-2020-36899	QiHang Media Web Digital Signage 3.0.9 contains an unauthenticated file disclosure vulnerability that allows remote attackers to access sensitive files through unv 'filename' and 'path' parameters. Attackers can exploit the QH.aspx endpoint to read arbitrary files and directory contents without authentication by manipulating getAll actions.
CVE-2020-36898	QiHang Media Web Digital Signage 3.0.9 contains an unauthenticated file deletion vulnerability in the QH.aspx endpoint that allows remote attackers to delete files authentication. Attackers can exploit the 'data' parameter by sending a POST request with file paths to delete arbitrary files with web server permissions using dire traversal sequences.
CVE-2020-36897	QiHang Media Web Digital Signage 3.0.9 contains an unauthenticated remote code execution vulnerability in the QH.aspx file that allows attackers to upload malic scripts. Attackers can exploit the file upload functionality by using the 'remotePath' and 'fileToUpload' parameters to write and execute arbitrary system commands server.
CVE-2020-36896	QiHang Media Web Digital Signage 3.0.9 contains a cleartext credentials vulnerability that allows unauthenticated attackers to access administrative login informat an unprotected XML file. Attackers can retrieve hardcoded admin credentials by requesting the '/xml/User/User.xml' file, enabling direct authentication bypass.
CVE-2020-36895	EIBIZ i-Media Server Digital Signage 3.8.0 contains an unauthenticated configuration disclosure vulnerability that allows remote attackers to access sensitive config via direct object reference. Attackers can retrieve the SiteConfig.properties file through an HTTP GET request, exposing administrative credentials, database conne and system configuration information.
CVE-2020-36894	Eibiz i-Media Server Digital Signage 3.8.0 contains an authentication bypass vulnerability that allows unauthenticated attackers to create admin users through AMF object manipulation. Attackers can send crafted serialized objects to the /messagebroker/amf endpoint to create administrative users without authentication, bypa controls.
CVE-2020-36893	Eibiz i-Media Server Digital Signage 3.8.0 contains a directory traversal vulnerability that allows unauthenticated remote attackers to access files outside the serve directory. Attackers can exploit the 'oldfile' GET parameter to view sensitive configuration files like web.xml and system files such as win.ini.
CVE-2020-36892	Eibiz i-Media Server Digital Signage 3.8.0 contains an unauthenticated privilege escalation vulnerability in the updateUser object that allows attackers to modify us Attackers can exploit the /messagebroker/amf endpoint to elevate privileges and take over user accounts by manipulating role settings without authentication.
CVE-2020-36888	SpinetiX Fusion Digital Signage 3.4.8 contains a username enumeration vulnerability in its login script that allows attackers to identify valid user accounts. Attacke crafted login requests with different usernames to distinguish between existing and non-existing accounts by analyzing the server's error responses.
CVE-2020-36887	SpinetiX Fusion Digital Signage 3.4.8 contains an unauthenticated information disclosure vulnerability in the database backup directory. Attackers can access the /content/files/backups/ endpoint to download sensitive backup files containing user credentials and system information.
CVE-2020-36886	SpinetiX Fusion Digital Signage 3.4.8 contains a cross-site request forgery vulnerability that allows attackers to create administrative user accounts without proper validation. Attackers can craft a malicious web page that automatically submits a form to create a new admin user with full system privileges when a logged-in use page.
CVE-2020-36884	BrightSign Digital Signage Diagnostic Web Server 8.2.26 and less contains an unauthenticated server-side request forgery vulnerability in the 'url' GET parameter Download Speed Test service. Attackers can specify external domains to bypass firewalls and perform network enumeration by forcing the application to make arb requests to internal network hosts.
CVE-2025-34423	MailEnable versions prior to 10.54 contain an unsafe DLL loading vulnerability that can lead to local arbitrary code execution. The MailEnable administrative execut to load MEAIAU.DLL from its installation directory without sufficient integrity validation or a secure search order. A local attacker with write access to that directory malicious MEAIAU.DLL, which is then loaded on execution, resulting in attacker-controlled code running with the privileges of the process.

CVE-2020-36883	SpinetiX Fusion Digital Signage 3.4.8 and lower contains an authenticated path traversal vulnerability that allows attackers to manipulate file backup and deletion through unverified input parameters. Attackers can exploit path traversal techniques in index.php to write backup files to arbitrary locations and delete files by ma backup and file delete requests.
CVE-2025-65602	A template injection vulnerability in the /vip/v1/file/save component of ChanCMS v3.3.4 allows attackers to execute arbitrary code via a crafted POST request.
CVE-2025-56431	Directory Traversal vulnerability in Fearless Geek Media FearlessCMS v.0.0.2-15 allows a remote attacker to cause a denial of service via the plugin-handler.php an file_get_contents() function.
CVE-2025-56430	Directory Traversal vulnerability in Fearless Geek Media FearlessCMS v.0.0.2-15 allows a remote attacker to cause a denial of service via the plugin-handler.php an deleteDirectory function.
CVE-2025-56429	Cross Site Scripting vulnerability in Fearless Geek Media FearlessCMS v.0.0.2-15 allows a remote attacker to obtain sensitive information via the login.php compone
CVE-2025-34430	1Panel versions 1.10.33 through 2.0.15 contain a cross-site request forgery (CSRF) vulnerability in the panel name management functionality. The affected endpoi implement CSRF defenses such as anti-CSRF tokens or Origin/Referer validation. An attacker can craft a malicious webpage that submits a panel-name change req victim visits the page while authenticated, the browser includes valid session cookies and the request succeeds. This allows a remote attacker to change the victim name to an arbitrary value without consent.
CVE-2025-34429	1Panel versions 1.10.33 - 2.0.15 contain a cross-site request forgery (CSRF) vulnerability in the web port configuration functionality. The port-change endpoint lack defenses such as anti-CSRF tokens or Origin/Referer validation. An attacker can craft a malicious webpage that submits a port-change request; when a victim visits authenticated, the browser includes valid session cookies and the request succeeds. This allows an attacker to change the port on which the 1Panel web service lis loss of access on the original port and resulting in service disruption or denial of service, and may unintentionally expose the service on an attacker-chosen port.
CVE-2025-34428	MailEnable versions prior to 10.54 contain a cleartext storage of credentials vulnerability that can lead to local credential compromise and account takeover. The p user and administrative passwords in plaintext within AUTH.SAV with overly permissive filesystem access. A local authenticated user with read access to this file ca user passwords and super-admin credentials, then use them to authenticate to MailEnable services such as POP3, SMTP, or the webmail interface, enabling unauth mailbox access and administrative control.
CVE-2025-34427	MailEnable versions prior to 10.54 contain a cleartext storage of credentials vulnerability that can lead to local credential compromise and account takeover. The p user and administrative passwords in plaintext within AUTH.TAB with overly permissive filesystem access. A local authenticated user with read access to this file ca user passwords and super-admin credentials, then use them to authenticate to MailEnable services such as POP3, SMTP, or the webmail interface, enabling unauth mailbox access and administrative control.
CVE-2025-65754	Cross Site Scripting vulnerability in Algernon v1.17.4 allows attackers to execute arbitrary code via injecting a crafted payload into a filename.
CVE-2025-63094	XiangShan Nanhu V2 and XiangShan Kunmighu V3 were discovered to use speculative execution and indirect branch prediction, allowing attackers to access sensi information via side-channel analysis of the data cache.
CVE-2025-5467	It was discovered that process_crash() in data/apport in Canonical's Apport crash reporting tool may create crash files with incorrect group ownership, possibly exp information beyond expected or intended groups.
CVE-2025-34424	MailEnable versions prior to 10.54 contain an unsafe DLL loading vulnerability that can lead to local arbitrary code execution. The MailEnable administrative execut to load MEAIDP.DLL from its installation directory without sufficient integrity validation or a secure search order. A local attacker with write access to that directory malicious MEAIDP.DLL, which is then loaded on execution, resulting in attacker-controlled code running with the privileges of the process.
CVE-2024-58307	CSZCMS 1.3.0 contains an authenticated SQL injection vulnerability in the members view functionality that allows authenticated attackers to manipulate database Attackers can inject malicious SQL code through the view parameter to potentially execute time-based blind SQL injection attacks and extract database informatio
CVE-2024-58309	xbtitFM 4.1.18 contains an unauthenticated SQL injection vulnerability that allows remote attackers to manipulate database queries by injecting malicious SQL cod msgid parameter. Attackers can send crafted requests to /shoutedit.php with EXTRACTVALUE functions to extract database names, user credentials, and password the underlying database.
CVE-2025-67985	Authorization Bypass Through User-Controlled Key vulnerability in Barn2 Plugins Document Library Lite document-library-lite allows Exploiting Incorrectly Configure Control Security Levels.This issue affects Document Library Lite: from n/a through <= 1.1.7.
CVE-2025-13824	A security issue exists due to improper handling of malformed CIP packets during fuzzing. The controller enters a hard fault with solid red Fault LED and becomes u Upon power cycle, the controller will enter recoverable fault where the MS LED and Fault LED become flashing red and reports fault code 0xF019. To recover, clear
CVE-2025-66402	Misskey is an open source, federated social media platform. Starting in version 13.0.0-beta.16 and prior to version 2025.12.0, an actor who does not have permissi favorites or clips can can export the posts and view the contents. Version 2025.12.0 fixes the issue.
CVE-2025-58173	FreshRSS is a self-hosted RSS feed aggregator. In versions 1.23.0 through 1.27.0, using a path traversal inside the `language` user configuration parameter, it's po `install.php` and perform various administrative actions as an unprivileged user. These actions include logging in as the admin, creating a new admin user, or set t to an attacker-controlled MySQL server and abuse it to execute code in FreshRSS by setting malicious feed `curl_params` inside the `feed` table. Version 1.27.1 fix
CVE-2025-64725	Weblate is a web based localization tool. In versions prior to 5.15, it was possible to accept an invitation opened by a different user. Version 5.15. contains a patch. workaround, avoid leaving one's Weblate sessions with an invitation opened unattended.
CVE-2025-59947	NanoMQ is a messaging broker/bus for IoT Edge & SDV. Versions prior to 0.24.4 have a buffer overflow case while the PUBLISH packets trigger both shared subscri vanila subscription. This is fixed in version 0.24.4. As a workaround, disable shared subscription.
CVE-	Ateme TITAN File 3.9.12.4 contains an authenticated server-side request forgery vulnerability in the job callback URL parameter that allows attackers to bypass ne

2023-53893	restrictions. Attackers can exploit the unvalidated parameter to initiate file, service, and network enumeration by forcing the application to make HTTP, DNS, or file arbitrary destinations.
CVE-2023-53892	Blackcat CMS 1.4 contains a remote code execution vulnerability that allows authenticated administrators to upload malicious PHP files through the jquery plugin n Attackers can upload a zip file with a PHP shell script and execute arbitrary system commands by accessing the uploaded plugin's PHP file with a 'code' parameter.
CVE-2023-53891	Blackcat CMS 1.4 contains a stored cross-site scripting vulnerability that allows authenticated users to inject malicious scripts into page content. Attackers can inse payloads in the page modification interface that execute when other users view the compromised page.
CVE-2023-53890	Perch CMS 3.2 contains a stored cross-site scripting vulnerability that allows authenticated users to upload malicious SVG files with embedded JavaScript. Attackers SVG files with script tags that execute when the file is viewed, potentially stealing user session information or performing client-side attacks.
CVE-2023-53889	Perch CMS 3.2 contains a remote code execution vulnerability that allows authenticated administrators to upload arbitrary PHP files through the assets manageme Attackers can upload a malicious .phar file with embedded system command execution capabilities to execute arbitrary commands on the server.
CVE-2023-53888	Zomplog 3.9 contains a remote code execution vulnerability that allows authenticated attackers to inject and execute arbitrary PHP code through file manipulation Attackers can upload malicious JavaScript files, rename them to PHP, and execute system commands by exploiting the saveE and rename actions in the applicatior
CVE-2023-53887	Zomplog 3.9 contains a cross-site scripting vulnerability that allows authenticated users to inject malicious scripts when creating new pages. Attackers can craft m source and onerror attributes to execute arbitrary JavaScript code in victim's browser.
CVE-2023-53886	Xlight FTP Server 3.9.3.6 contains a stack buffer overflow vulnerability in the 'Execute Program' configuration that allows attackers to crash the application. Attacke the vulnerability by inserting 294 characters into the program execution configuration, causing a denial of service condition.
CVE-2023-53885	Webutler v3.2 contains a remote code execution vulnerability that allows authenticated administrators to upload PHP files with system command execution. Attack upload a PHAR file with embedded system commands to the media browser and execute arbitrary commands by accessing the uploaded file.
CVE-2023-53884	Webedition CMS v2.9.8.8 contains a stored cross-site scripting vulnerability that allows authenticated users to upload malicious SVG files with embedded JavaScrip can upload crafted SVG files through the media upload feature to inject and execute arbitrary scripts when the file is viewed by other users.
CVE-2023-53883	Webedition CMS v2.9.8.8 contains a remote code execution vulnerability that allows authenticated attackers to inject system commands through PHP page creatio can create a new PHP page with malicious system commands in the description field to execute arbitrary commands on the server.
CVE-2023-53882	JLex GuestBook 1.6.4 contains a reflected cross-site scripting vulnerability in the 'q' URL parameter that allows attackers to inject malicious scripts. Attackers can c links with XSS payloads to steal session tokens or execute arbitrary JavaScript in victims' browsers.
CVE-2023-53881	ReyeeOS 1.204.1614 contains an unencrypted CWMP communication vulnerability that allows attackers to intercept and manipulate device communication throug the-middle attack. Attackers can create a fake CWMP server to inject and execute arbitrary commands on Ruijie Reyee Cloud devices by exploiting the unprotected requests.
CVE-2023-53880	Lucee 5.4.2.17 contains a reflected cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through administrative interface Attackers can craft specific payloads targeting admin pages like server.cfm and web.cfm to execute arbitrary JavaScript in victim's browser sessions.
CVE-2023-53879	NVClient 5.0 contains a stack buffer overflow vulnerability in the user configuration contact field that allows attackers to crash the application. Attackers can overw of memory by pasting a crafted payload into the contact box, causing a denial of service condition.
CVE-2023-53878	Member Login Script 3.3 contains a client-side desynchronization vulnerability that allows attackers to manipulate HTTP request handling by exploiting Content-Ler parsing. Attackers can send crafted POST requests with smuggled secondary requests to potentially bypass server-side request processing controls.
CVE-2023-53877	Bus Reservation System 1.1 contains a SQL injection vulnerability in the pickup_id parameter that allows attackers to manipulate database queries. Attackers can e boolean-based, error-based, and time-based blind SQL injection techniques to steal information from the database.
CVE-2023-53876	Academy LMS 6.1 contains a file upload vulnerability that allows authenticated users to upload malicious SVG files with stored cross-site scripting payloads. Attack malicious scripts through the profile avatar upload feature by modifying file extensions and embedding executable JavaScript code.
CVE-2023-53875	GOM Player 2.3.90.5360 contains a remote code execution vulnerability in its Internet Explorer component that allows attackers to execute arbitrary code through Attackers can redirect victims using a malicious URL shortcut and WebDAV technique to run a reverse shell with SMB server interaction.
CVE-2023-53874	GOM Player 2.3.90.5360 contains a buffer overflow vulnerability in the equalizer preset name input field that allows attackers to crash the application. Attackers ca the preset name with 260 'A' characters to trigger a buffer overflow and cause application instability.
CVE-2023-53873	SyncBreeze 15.2.24 contains a denial of service vulnerability in the login authentication mechanism that allows attackers to crash the service. Attackers can send a password parameter with repeated 'password=' values to overwhelm the login endpoint and potentially disrupt service availability.
CVE-2023-53872	Wp2Fac 1.0 contains an OS command injection vulnerability in the send.php endpoint that allows remote attackers to execute arbitrary system commands. Attacke shell commands through the 'numara' parameter by appending shell commands with '&' operators to execute malicious code.

CVE-2023-53871	Soosyze 2.0.0 contains a file upload vulnerability that allows attackers to upload arbitrary HTML files with embedded PHP code to the application. Attackers can exp broken file upload mechanism to potentially view sensitive file paths and execute malicious PHP scripts on the server.
CVE-2023-53870	Jorani 1.0.3 contains a reflected cross-site scripting vulnerability in the language parameter that allows attackers to inject malicious scripts. Attackers can craft XSS the language parameter to execute arbitrary JavaScript and potentially steal user session information.
CVE-2023-53869	WEBIGniter 28.7.23 contains a file upload vulnerability that allows authenticated attackers to upload and execute dangerous PHP files through the media function. leverage any created account to upload malicious PHP scripts that enable remote code execution on the application server.
CVE-2025-66482	Misskey is an open source, federated social media platform. Attackers who use an untrusted reverse proxy or not using a reverse proxy at all can bypass IP rate lim adding a forged X-Forwarded-For header. Starting with version 2025.9.1, an option (`trustProxy`) has been added in config file to prevent this from happening. How initialized with an insecure default value before version 2025.12.0-alpha.2, making it still vulnerable if the configuration is not set correctly. This is patched in v202 by flipping default value of `trustProxy` to `false`. Users of a trusted reverse proxy who are unsure if they manually overode this value should check their config fo behavior. Users are running Misskey with a trusted reverse proxy should not be affected by this vulnerability. From v2025.9.1 to v2025.11.1, workaround is availab `trustProxy: false` in config file.
CVE-2025-67722	FreePBX is an open-source web-based graphical user interface (GUI) that manages Asterisk. Prior to versions 16.0.45 and 17.0.24 of the FreePBX framework, an au local privilege escalation exists in the deprecated FreePBX startup script `amportal`. In the deprecated `amportal` utility, the lookup for the `freepbx_engine` file c `/etc/asterisk/` directories. Typically, these are configured by FreePBX as writable by the **asterisk** user and any members of the **asterisk** group. This means member of the **asterisk** group can add their own `freepbx_engine` file in `/etc/asterisk/` and upon `amportal` executing, it would exec that file with root permi though the file was created and placed by a non-root user). Version 16.0.45 and 17.0.24 contain a fix for the issue. Other mitigation strategies are also available. C trusted local OS system users are members of the `asterisk` group. Look for suspicious files in the `/etc/asterisk/` directory (via Admin -> Config Edit in the GUI, or Double-check that `live_dangerously = no` is set (or unconfigured, as the default is **no**) in `/etc/asterisk/asterisk.conf` file. Eliminate any unsafe custom use of plan applications and functions that potentially can manipulate the file system, e.g., System(), FILE(), etc.
CVE-2025-67736	The FreePBX module tts (Text to Speech) for FreePBX, an open-source web-based graphical user interface (GUI) that manages Asterisk. Versions prior to 16.0.5 and vulnerable to SQL injection by authenticated users with administrator access. Authenticated users with administrative access to the Administrator Control Panel (A leverage this SQL injection vulnerability to extract sensitive information from the database and execute code on the system as the `asterisk` user with chained ele `root` privileges. Users should upgrade to version 16.0.5 or 17.0.5 to receive a fix.
CVE-2025-64248	Missing Authorization vulnerability in emarket-design Request a Quote request-a-quote allows Exploiting Incorrectly Configured Access Control Security Levels.This Request a Quote: from n/a through <= 2.5.3.
CVE-2025-67983	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in osama.esh WP Visitor Statistics (Real Time Traffic) wp-stats-ma DOM-Based XSS.This issue affects WP Visitor Statistics (Real Time Traffic): from n/a through <= 8.3.
CVE-2025-67976	Missing Authorization vulnerability in Bob Watu Quiz watu allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Watu Quiz: from <= 3.4.5.
CVE-2025-67929	Missing Authorization vulnerability in templateinvaders TI WooCommerce Wishlist ti-woocommerce-wishlist allows Exploiting Incorrectly Configured Access Control Levels.This issue affects TI WooCommerce Wishlist: from n/a through <= 2.10.0.
CVE-2025-66133	Missing Authorization vulnerability in WP Legal Pages WP Cookie Notice for GDPR, CCPA & ePrivacy Consent gdpr-cookie-consent allows Exploiting Incorrectly Confi Control Security Levels.This issue affects WP Cookie Notice for GDPR, CCPA & ePrivacy Consent: from n/a through <= 4.0.7.
CVE-2025-66132	Authorization Bypass Through User-Controlled Key vulnerability in FAPI Business s.r.o. FAPI Member fapi-member allows Exploiting Incorrectly Configured Access C Levels.This issue affects FAPI Member: from n/a through <= 2.2.26.
CVE-2025-66126	Insertion of Sensitive Information Into Sent Data vulnerability in wowpress.host Fix Media Library wow-media-library-fix allows Retrieve Embedded Sensitive Data.T affects Fix Media Library: from n/a through <= 2.0.
CVE-2025-66121	Missing Authorization vulnerability in SiteGround SiteGround Security sg-security allows Exploiting Incorrectly Configured Access Control Security Levels.This issue SiteGround Security: from n/a through <= 1.5.8.
CVE-2025-64635	Missing Authorization vulnerability in Syed Balkhi Feeds for YouTube feeds-for-youtube allows Exploiting Incorrectly Configured Access Control Security Levels.This Feeds for YouTube: from n/a through <= 2.4.0.
CVE-2025-64634	Missing Authorization vulnerability in ThemeFusion Avada avada allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Avada: from n/ 7.13.1.
CVE-2025-64631	Missing Authorization vulnerability in WC Lovers WCFM Marketplace wc-multivendor-marketplace allows Exploiting Incorrectly Configured Access Control Security L issue affects WCFM Marketplace: from n/a through <= 3.6.15.
CVE-2025-64630	Missing Authorization vulnerability in Strategy11 Team Business Directory business-directory-plugin allows Exploiting Incorrectly Configured Access Control Securit issue affects Business Directory: from n/a through <= 6.4.19.
CVE-2025-64253	Path Traversal: '.../...//' vulnerability in WordPress.org Health Check & Troubleshooting health-check allows Path Traversal.This issue affects Health Check & Trouble from n/a through <= 1.7.1.
CVE-2025-64249	Missing Authorization vulnerability in WP-EXPERTS.IN Protect WP Admin protect-wp-admin allows Exploiting Incorrectly Configured Access Control Security Levels.T affects Protect WP Admin: from n/a through <= 4.1.

CVE-2025-64247	Missing Authorization vulnerability in edmon.parker Read More & Accordion expand-maker allows Exploiting Incorrectly Configured Access Control Security Levels.T affects Read More & Accordion: from n/a through <= 3.5.4.1.
CVE-2025-67747	Fickling is a Python pickling decompiler and static analyzer. Versions prior to 0.1.6 are missing `marshal` and `types` from the block list of unsafe module imports. started blocking both modules to address this issue. This allows an attacker to craft a malicious pickle file that can bypass fickling since it misses detections for `types.FunctionType` and `marshal.loads`. A user who deserializes such a file, believing it to be safe, would inadvertently execute arbitrary code on their system. T any user or system that uses Fickling to vet pickle files for security issues. The issue was fixed in version 0.1.6.
CVE-2025-64241	Missing Authorization vulnerability in Imtiaz Rayhan WP Coupons and Deals wp-coupons-and-deals allows Exploiting Incorrectly Configured Access Control Security issue affects WP Coupons and Deals: from n/a through <= 3.2.4.
CVE-2025-54004	Missing Authorization vulnerability in WC Lovers WCFM – Frontend Manager for WooCommerce wc-frontend-manager allows Exploiting Incorrectly Configured Acces Security Levels.This issue affects WCFM – Frontend Manager for WooCommerce: from n/a through <= 6.7.21.
CVE-2025-66635	Stack-based buffer overflow vulnerability exists in SEIKO EPSON Web Config. Specially crafted data input by a logged-in user may execute arbitrary code. As for the affected products and versions, see the information provided by the vendor under [References].
CVE-2025-66357	CHOCO TEI WATCHER mini (IB-MCT001) contains an issue with improper check for unusual or exceptional conditions. When the Video Download feature is in a spec communication state, the product's resources may be consumed abnormally.
CVE-2025-61976	CHOCO TEI WATCHER mini (IB-MCT001) contains an issue with improper check for unusual or exceptional conditions. If a remote attacker sends a specially crafted Video Download interface, the system may become unresponsive.
CVE-2025-59479	CHOCO TEI WATCHER mini (IB-MCT001) contains an issue with improper restriction of rendered UI layers or frames. If a user clicks on content on a malicious web p logged into the product, unintended operations may be performed on the product.
CVE-2025-62849	An SQL injection vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the vulnerability to exec unauthorized code or commands. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3297 build 20251024 and later QuTS hero h5.2.7.329 20251024 and later QuTS hero h5.3.1.3292 build 20251024 and later
CVE-2025-62848	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the vulnerabi a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3297 build 20251024 and later QuTS hero h5.2.7.3297 20251024 and later QuTS hero h5.3.1.3292 build 20251024 and later
CVE-2025-62847	An improper neutralization of argument delimiters in a command vulnerability has been reported to affect several QNAP operating system versions. The remote att then exploit the vulnerability to alter execution logic. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3297 build 20251024 and later Qu h5.2.7.3297 build 20251024 and later QuTS hero h5.3.1.3292 build 20251024 and later
CVE-2025-59385	An authentication bypass by spoofing vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the to access resources which are not otherwise accessible without proper authentication. We have already fixed the vulnerability in the following versions: QTS 5.2.7.3 20251024 and later QuTS hero h5.2.7.3297 build 20251024 and later QuTS hero h5.3.1.3292 build 20251024 and later
CVE-2025-68115	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 8.6.1 and 9.1.0-alpha.3, a Reflected Cr Scripting (XSS) vulnerability exists in Parse Server's password reset and email verification HTML pages. The patch, available in versions 8.6.1 and 9.1.0-alpha.3, es controlled values that are inserted into the HTML pages. No known workarounds are available.
CVE-2025-67874	ChurchCRM is an open-source church management system. Prior to version 6.5.0, the application echoes back plaintext passwords submitted by users in subseque responses. This information disclosure significantly increases the risk of credential compromise and may amplify the impact of other vulnerabilities (e.g., XSS, IDOR fixation), enabling attackers to harvest other users' passwords. Version 6.5.0 fixes the issue.
CVE-2025-67748	Fickling is a Python pickling decompiler and static analyzer. Versions prior to 0.1.6 had a bypass caused by `pty` missing from the block list of unsafe module impo unsafe pickles based on `pty.spawn()` being incorrectly flagged as `LIKELY_SAFE`, and was fixed in version 0.1.6. This impacted any user or system that used Fickl pickle files for security issues.
CVE-2023-53868	Coppermine Gallery 1.6.25 contains a remote code execution vulnerability that allows authenticated attackers to upload malicious PHP files through the plugin ma Attackers can upload a zipped PHP file with system commands to the plugin directory and execute arbitrary code by accessing the uploaded plugin script.
CVE-2025-13823	A security issue was found in the IPv6 stack in the Micro850 and Micro870 controllers when the controllers received multiple malformed packets during fuzzing. The will go into recoverable fault with fault code 0xFE60. To recover the controller, clear the fault.
CVE-2024-58310	APC Network Management Card 4 contains a path traversal vulnerability that allows unauthenticated attackers to access sensitive system files by manipulating UR Attackers can exploit directory traversal techniques to read critical system files like /etc/passwd by using encoded path traversal characters in HTTP requests.
CVE-2025-34412	The Convercent Whistleblowing Platform operated by EQS Group contains a protection mechanism failure in its browser and session handling. By default, affected omit HTTP security headers such as Content-Security-Policy, Referrer-Policy, Permissions-Policy, Cross-Origin-Embedder-Policy, Cross-Origin-Opener-Policy, and Cro Resource-Policy, and implement incomplete clickjacking protections. The application also issues session cookies with insecure or inconsistent attributes by default, duplicate ASP.NET_SessionId values, an affinity cookie missing the Secure attribute, and mixed or absent SameSite settings. These deficiencies weaken browser-si and session integrity, increasing exposure to client-side attacks, session fixation, and cross-site session leakage.
CVE-2025-43509	This issue was addressed with improved data protection. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. An app may be able to access sensiti
CVE-2025-40345	In the Linux kernel, the following vulnerability has been resolved: usb: storage: sddr55: Reject out-of-bound new_pba Discovered by Atuin - Automated Vulnerabilit Engine. new_pba comes from the status packet returned after each write. A bogus device could report values beyond the block count derived from info->capacity, driver walk off the end of pba_to_lba[] and corrupt heap memory. Reject PBAs that exceed the computed block count and fail the transfer so we avoid touching out mapping entries.

CVE-2025-13733	BuhoNTFS contains an insecure XPC service that allows local, unprivileged users to escalate their privileges to root via insecure functions.This issue affects BuhoNT
CVE-2025-12843	Code Injection using Electron Fuses in waveterm on MacOS allows TCC Bypass. This issue affects waveterm: 0.12.2.
CVE-2025-58770	APTIOV contains a vulnerability in BIOS where a user may cause “Improper Handling of Insufficient Permissions or Privileges” by local access. Successful exploitatic vulnerability can lead to escalation of authorization and potentially impact Integrity and Availability.
CVE-2025-36755	The CleverDisplay BlueOne hardware player is designed with its USB interfaces physically enclosed and inaccessible under normal operating conditions. Researche demonstrated that, after cicumventing the device’s protective enclosure, it was possible to connect a USB keyboard and press ESC during boot to access the BIOS interface. BIOS settings could be viewed but not modified. This behavior slightly increases the attack surface by exposing internal system information (CWE-1244) enclosure is removed, but does not allow integrity or availability compromise under standard or tested configurations.
CVE-2025-36745	SolarEdge SE3680H ships with an outdated Linux kernel containing unpatched vulnerabilities in core subsystems. An attacker with network or local access can exp flaws to achieve remote code execution, privilege escalation, or disclosure of sensitive information.
CVE-2025-36744	SolarEdge SE3680H has unauthenticated disclosure of sensitive information during the bootloader loop. While the device repeatedly initializes and waits for boot in the bootloader emits diagnostic output this behavior can leak operating system information.
CVE-2025-36743	SolarEdge SE3680H has an exposed debug/test interface accessible to unauthenticated actors, allowing disclosure of system internals and execution of debug com
CVE-2025-23408	Weak Password Requirements vulnerability in Apache Fineract. This issue affects Apache Fineract: through 1.10.1. The issue is fixed in version 1.11.0. Users are en upgrade to version 1.13.0, the latest release.
CVE-2025-67731	Servify Express is a Node.js package to start an Express server and log the port it's running on. Prior to 1.2, the Express server used express.json() without a size li could allow attackers to send extremely large request bodies. This can cause excessive memory usage, degraded performance, or process crashes, resulting in a D Service (DoS). Any application using the JSON parser without limits and exposed to untrusted clients is affected. The issue is not a flaw in Express itself, but in conf issue is fixed in version 1.2. To work around, consider adding a limit option to the JSON parser, rate limiting at the application or reverse-proxy level, rejecting unus requests before parsing, or using a reverse proxy (such as NGINX) to enforce maximum request body sizes.
CVE-2025-67727	Parse Server is an open source backend that can be deployed to any infrastructure that runs Node.js. In versions prior to 8.6.0-alpha.2, a GitHub CI workflow is trig that grants the GitHub Actions workflow elevated permissions, giving it access to GitHub secrets and write permissions which are defined in the workflow. Code fro lifecycle scripts is potentially included. Only the repository's CI/CD infrastructure is affected, including any public GitHub forks with GitHub Actions enabled. This iss version 8.6.0-alpha.2 and commits 6b9f896 and e3d27fe.
CVE-2025-67508	gardenctl is a command-line client for the Gardener which configures access to clusters and cloud provider CLI tools. When using non-POSIX shells such as Fish and versions 2.11.0 and below of gardenctl allow an attacker with administrative privileges for a Gardener project to craft malicious credential values. The forged crede are used in infrastructure Secret objects that break out of the intended string context when evaluated in Fish or PowerShell environments used by the Gardener se operators. This issue is fixed in version 2.12.0.
CVE-2025-66284	Stored cross-site scripting vulnerabilities exist in GroupSession Free edition prior to ver5.7.1, GroupSession byCloud prior to ver5.7.1, and GroupSession ZION prior logged-in user can prepare a malicious page or URL, and an arbitrary script may be executed on the web browser when another user accesses it.
CVE-2025-65120	Reflected cross-site scripting vulnerability exists in GroupSession Free edition prior to ver5.7.1, GroupSession byCloud prior to ver5.7.1, and GroupSession ZION pri If a user accesses a crafted page or URL, an arbitrary script may be executed on the web browser of the user.
CVE-2025-64781	In GroupSession Free edition prior to ver5.7.1, GroupSession byCloud prior to ver5.7.1, and GroupSession ZION prior to ver5.7.1, "External page display restriction" not limit" in the initial configuration. With this configuration, the user may be redirected to an arbitrary website when accessing a specially crafted URL.
CVE-2025-62192	SQL Injection vulnerability exists in GroupSession Free edition prior to ver5.3.0, GroupSession byCloud prior to ver5.3.3, and GroupSession ZION prior to ver5.3.2. I information stored in the database may be obtained or altered by an authenticated user.
CVE-2025-61987	GroupSession Free edition prior to ver5.3.0, GroupSession byCloud prior to ver5.3.3, and GroupSession ZION prior to ver5.3.2. do not validate origins in WebSocket accesses a crafted page, Chat information sent to the user may be exposed.
CVE-2025-61950	In GroupSession, a Circular notice can be created with its memo field non-editable, but the authorization check is improperly implemented. With some crafted requ in user may alter the memo field. The affected products and versions are GroupSession Free edition prior to ver5.3.0, GroupSession byCloud prior to ver5.3.3, and ZION prior to ver5.3.2.
CVE-2025-58576	Cross-site request forgery vulnerability exists in GroupSession Free edition prior to ver5.3.0, GroupSession byCloud prior to ver5.3.3, and GroupSession ZION prior a user accesses a malicious page while logged in, unintended operations may be performed.
CVE-2025-57883	Reflected cross-site scripting vulnerability exists in GroupSession Free edition prior to ver5.3.0, GroupSession byCloud prior to ver5.3.3, and GroupSession ZION pri If a user accesses a crafted page or URL, an arbitrary script may be executed on the web browser of the user.
CVE-2025-54407	Stored cross-site scripting vulnerability exists in GroupSession Free edition prior to ver5.3.0, GroupSession byCloud prior to ver5.3.3, and GroupSession ZION prior a user accesses a crafted page or URL, an arbitrary script may be executed on the web browser of the user.
CVE-2025-53523	Stored cross-site scripting vulnerabilities exist in GroupSession Free edition prior to ver5.3.0, GroupSession byCloud prior to ver5.3.3, and GroupSession ZION prior logged-in user can prepare a malicious page or URL, and an arbitrary script may be executed on the web browser when another user accesses it.

CVE-2025-13053	When a user configures the NAS to retrieve UPS status or control the UPS, a non-enforced TLS certificate verification can allow an attacker able to intercept networ between the client and server can perform a man-in-the-middle (MITM) attack, which may obtain the sensitive information of the UPS server configuation. This issu from 4.1.0 through 4.3.3.RKD2, from 5.0.0 through 5.1.0.RN42.
CVE-2025-13052	When the user set the Notification's sender to send emails to the SMTP server via msmtp, an improper validated TLS/SSL certificates allows an attacker who can int network traffic between the SMTP client and server to execute a man-in-the-middle (MITM) attack, which may obtain the sensitive information of the SMTP. Affecte and versions include: from ADM 4.1.0 through ADM 4.3.3.RKD2 as well as from ADM 5.0.0 through ADM 5.1.0.RN42.
CVE-2025-64721	Sandboxie is a sandbox-based isolation software for 32-bit and 64-bit Windows NT-based operating systems. In versions 1.16.6 and below, the SYSTEM-level servic exposes SbieIniServer::RC4Crypt to sandboxed processes. The handler adds a fixed header size to a caller-controlled value_len without overflow checking. A large (e.g., 0xFFFFFFF0) wraps the allocation size, causing a heap overflow when attacker data is copied into the undersized buffer. This allows sandboxed processes to e arbitrary code as SYSTEM, fully compromising the host. This issue is fixed in version 1.16.7.
CVE-2025-34499	AnyDesk 7.0.15 and 9.0.1 contains an unquoted service path vulnerability that allows local non-privileged users to potentially execute code with elevated SYSTEM Attackers can exploit the unquoted service path configuration to inject malicious executables that will be run with high-level system permissions.
CVE-2024-58313	xbtitFM 4.1.18 contains an insecure file upload vulnerability that allows authenticated attackers with administrative privileges to upload and execute arbitrary PHP the file_hosting feature. Attackers can bypass file type restrictions by modifying the Content-Type header to image/gif, adding GIF89a magic bytes, and using alter to upload web shells that execute system commands.
CVE-2024-58312	xbtitFM 4.1.18 contains a path traversal vulnerability that allows unauthenticated attackers to access sensitive system files by manipulating URL parameters. Attac exploit directory traversal techniques to read critical system files like using encoded path traversal characters in HTTP requests.
CVE-2025-43510	A memory corruption issue was addressed with improved lock state checking. This issue is fixed in watchOS 26.1, iOS 18.7.2 and iPadOS 18.7.2, macOS Tahoe 26.1 26.1, tvOS 26.1, macOS Sonoma 14.8.2, macOS Sequoia 15.7.2, iOS 26.1 and iPadOS 26.1. A malicious application may cause unexpected changes in memory sha processes.
CVE-2025-46289	A logic issue was addressed with improved file handling. This issue is fixed in macOS Sonoma 14.8.3, macOS Sequoia 15.7.3. An app may be able to access protect
CVE-2025-14066	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2025-67869	Rejected reason: Not used
CVE-2025-34411	The Convercent Whistleblowing Platform operated by EQS Group exposes an unauthenticated API endpoint at /GetLegalEntity that returns internal customer legal-e based on a supplied searchText fragment. A remote unauthenticated attacker can query the endpoint using common legal-suffix terms to enumerate Convercent t identifying organizations using the platform. This disclosure can facilitate targeted phishing, extortion, or other attacks against whistleblowing programs and revea business relationships and compliance infrastructure.
CVE-2025-34181	NetSupport Manager < 14.12.0001 contains an arbitrary file write vulnerability in its Connectivity Server/Gateway PUTFILE request handler. An attacker with a valid can supply a crafted filename containing directory traversal sequences to write files to arbitrary locations on the server. This can be leveraged to place attacker-co or executables in privileged paths and achieve remote code execution in the context of the NetSupport Manager connectivity service.
CVE-2025-34180	NetSupport Manager < 14.12.0001 relies on a shared Gateway Key for authentication between Manager/Control, Client, and Connectivity Server components. The using a reversible encoding scheme. An attacker who obtains access to a deployed client configuration file can decode the stored value to recover the plaintext Ga Possession of the Gateway Key allows unauthorized access to NetSupport Manager connectivity services and enables remote control of systems managed through
CVE-2025-34179	NetSupport Manager < 14.12.0001 contains an unauthenticated SQL injection vulnerability in its Connectivity Server/Gateway HTTPS request handling. The server request URIs using an unsanitized SQLite query against the FileLinks table in gateway.db. By injecting SQL through the LinkName/URI value, a remote attacker can FileName field used by the server to read and return files from disk, resulting in arbitrary local file disclosure.
CVE-2025-65782	An issue was discovered in Wekan The Open Source kanban board system up to version 18.15, fixed in 18.16. Authorization flaw in card update handling allows bo (and potentially other authenticated users) to add/remove arbitrary user IDs in vote.positive / vote.negative arrays, enabling vote forgery and unauthorized voting.
CVE-2025-65780	An issue was discovered in Wekan The Open Source kanban board system up to version 18.15, fixed in 18.16. Authenticated users can update their entire user doc (beyond profile fields), including orgs/teams and loginDisabled, due to missing server-side authorization checks; this enables privilege escalation and unauthorized other teams/orgs.
CVE-2025-65779	An issue was discovered in Wekan The Open Source kanban board system up to version 18.15, fixed in 18.16. Unauthenticated attackers can update a board's "sor (Boards.allow returns true without verifying userId), allowing arbitrary reordering of boards.
CVE-2025-14714	An Authentication Bypass vulnerability existed where the application bundled an interpreter (Python) that inherits the Transparency, Consent, and Control (TCC) permissions granted by the user to the main application bundle By executing the bundled interpreter directly the attacker's scripts run with the application's TCC p fixed versions parent-constraints are used to allow only the main application to launch interpreter with those permissions This issue affects LibreOffice on macOS: f before < 25.2.4.
CVE-2025-14549	In the Eclipse OMR compiler component, since release 0.7.0, an optimization enabled for Eclipse OpenJ9 consumers of OMR on Z processors incorrectly handles NU characters during the Latin-compatible charset (UTF-8, ISO8859-1, ASCII, etc) to IBM-1047/037 translation sequence. This can cause the output byte array to be tru discarding the first NUL byte and all subsequent characters, and thereby exposing a possible buffer over-read problem. This issue is fixed in Eclipse OMR version 0.
CVE-2025-67907	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2025-67906. Reason: This candidate is a reservation duplicate of CVE-2025-67906. Note users should reference CVE-2025-67906 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usag
CVE-2025-13832	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-	

2025-67871	Rejected reason: Not used
CVE-2025-67870	Rejected reason: Not used
CVE-2025-67868	Rejected reason: Not used
CVE-2025-67721	Aircompressor is a library with ports of the Snappy, LZO, LZ4, and Zstandard compression algorithms to Java. In versions 3.3 and below, incorrect handling of malfo Java-based decompressor implementations for Snappy and LZ4 allow remote attackers to read previous buffer contents via crafted compressed input. With certain compressed inputs, elements from the output buffer can end up in the uncompressed output, potentially leaking sensitive data. This is relevant for applications tha same output buffer to uncompress multiple inputs. This can be the case of a web server that allocates a fix-sized buffer for performance purposes. There is similar in GHSA-cmp6-m4wj-q63q. This issue is fixed in version 3.4.
CVE-2025-67867	Rejected reason: Not used
CVE-2025-67866	Rejected reason: Not used
CVE-2025-67865	Rejected reason: Not used
CVE-2025-67864	Rejected reason: Not used
CVE-2025-67863	Rejected reason: Not used
CVE-2025-36754	The authentication mechanism on web interface is not properly implemented. It is possible to bypass authentication checks by crafting a post request with new set there is no session token or authentication in place. This would allow an attacker for instance to point the device to an arbitrary address for domain name resolutio facililitate a man-in-the-middle (MitM) attack.
CVE-2025-36753	The SWD debug interface on the Growatt ShineLan-X communication dongle is available by default, allowing an attacker to attain debug access to the device and t secrets or domains from within the device
CVE-2025-36752	Growatt ShineLan-X communication dongle has an undocumented backup account with undocumented credentials which allows significant level access to the devi as allowing any attacker to access the Setting Center. This means that this is effectively backdoor for all devices utilizing a Growatt ShineLan-X communication dor
CVE-2025-36751	Encryption is missing on the configuration interface for Growatt ShineLan-X and MIC 3300TL-X. This allows an attacker with access to the network to intercept and manipulate communication requests between the inverter and its cloud endpoint.
CVE-2025-36750	ShineLan-X contains a stored cross site scripting (XSS) vulnerability in the Plant Name field. A HTML payload will be displayed on the plant management page via a post. This may allow attackers to force a legitimate user’s browser’s JavaScript engine to run malicious code.
CVE-2025-36748	ShineLan-X contains a stored cross site scripting (XSS) vulnerability in the local configuration web server. The JavaScript code snippet can be inserted in the comm module’s settings center. This may allow attackers to force a legitimate user’s browser’s JavaScript engine to run malicious code.
CVE-2025-36747	ShineLan-X contains a set of credentials for an FTP server was found within the firmware, allowing testers to establish an insecure FTP connection with the server. an attacker to replace legitimate files being deployed to devices with their own malicious versions, since the firmware signature verification is not enforced.
CVE-2025-67749	PCSX2 is a free and open-source PlayStation 2 (PS2) emulator. In versions 2.5.377 and below, an unchecked offset and size used in a memcpy operation inside PCS SCMD 0x91 and SCMD 0x8F handlers allow a specially crafted disc image or ELF to cause an out-of-bounds read from emulator memory. Because the offset and siz through MG header fields, a specially crafted ELF can read data beyond the bounds of mg_buffer and have it reflected back into emulated memory. This issue is fix 2.5.378.
CVE-2025-34288	Nagios XI versions prior to 2026R1.1 are vulnerable to local privilege escalation due to an unsafe interaction between sudo permissions and application file permiss user-accessible maintenance script may be executed as root via sudo and includes an application file that is writable by a lower-privileged user. A local attacker wi the application account can modify this file to introduce malicious code, which is then executed with elevated privileges when the script is run. Successful exploitat arbitrary code execution as the root user.