SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 10 September 2025

Generated on 10 September 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-2025-55051	CWE-1392: Use of Default Credentials	10.0	More Details
CVE-2025-54914	Azure Networking Elevation of Privilege Vulnerability	10.0	More Details
CVE-2025-42944	Due to a deserialization vulnerability in SAP NetWeaver, an unauthenticated attacker could exploit the system through the RMI-P4 module by submitting malicious payload to an open port. The deserialization of such untrusted Java objects could lead to arbitrary OS command execution, posing a high impact to the application's confidentiality, integrity, and availability.	10.0	More Details
CVE-2025-55730	XWiki Remote Macros provides XWiki rendering macros that are useful when migrating content from Confluence. Starting in version 1.0 and prior to version 1.26.5, missing escaping of the title in the confluence paste code macro allows remote code execution for any user who can edit any page. The classes parameter is used without escaping in XWiki syntax, thus allowing XWiki syntax injection which enables remote code execution. Version 1.26.5 has a fix for the issue.	10.0	More Details
CVE-2025-55729	XWiki Remote Macros provides XWiki rendering macros that are useful when migrating content from Confluence. Starting in version 1.0 and prior to version 1.26.5, missing escaping of the ac:type in the ConfluenceLayoutSection macro allows remote code execution for any user who can edit any page The classes parameter is used without escaping in XWiki syntax, thus allowing XWiki syntax injection which enables remote code execution. Version 1.26.5 has a fix for the issue.	10.0	More Details
CVE-2025-55728	XWiki Remote Macros provides XWiki rendering macros that are useful when migrating content from Confluence. Starting in version 1.0 and prior to version 1.26.5, missing escaping of the classes parameter in the panel macro allows remote code execution for any user who can edit any page The classes parameter is used without escaping in XWiki syntax, thus allowing XWiki syntax injection which enables remote code execution. Version 1.26.5 contains a patch for the issue.	10.0	More Details
CVE-2025-55727	XWiki Remote Macros provides XWiki rendering macros that are useful when migrating content from Confluence. Starting in version 1.0 and prior to version 1.26.5, missing escaping of the width parameter in the column macro allows remote code execution for any user who can edit any page or who can access the CKEditor converter. The width parameter is used without escaping in XWiki syntax, thus allowing XWiki syntax injection which enables remote code execution when the macro has been installed by a user with programming right, or it at least allows executing Velocity code as the wiki admin. Version 1.26.5 contains a patch for the issue.	10.0	More Details
CVE-2025-42922	SAP NetWeaver AS Java allows an attacker authenticated as a non-administrative user to use a flaw in an available service to upload an arbitrary file. This file when executed can lead to a full compromise of	9.9	More Details

	confidentiality, integrity and availability of the system.		
CVE-2025-55190	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. In versions 2.13.0 through 2.13.8, 2.14.0 through 2.14.15, 3.0.0 through 3.0.12 and 3.1.0-rc1 through 3.1.1, API tokens with project-level permissions are able to retrieve sensitive repository credentials (usernames, passwords) through the project details API endpoint, even when the token only has standard application management permissions and no explicit access to secrets. This vulnerability does not only affect project-level permissions. Any token with project get permissions is also vulnerable, including global permissions such as: `p, role/user, projects, get, *, allow`. This issue is fixed in versions 2.13.9, 2.14.16, 3.0.14 and 3.1.2.	9.9	More Details
CVE-2025-58745	WeGIA is a Web manager for charitable institutions. The fix for CVE-2025-22133 was not enough to remediate the arbitrary file upload vulnerability. The WeGIA only check MIME types for Excel files at endpoint `/html/socio/sistema/controller/controla_xlsx.php`, which can be bypassed by using magic bytes of Excel file in a PHP file. As a result, attacker can upload webshell to the server for remote code execution. Version 3.4.11 contains an updated fix.	9.9	More Details
CVE-2025-56267	A CSV injection vulnerability in the /id_profiles endpoint of Avigilon ACM v7.10.0.20 allows attackers to execute arbitrary code via suuplying a crafted Excel file.	9.8	More Details
CVE-2025-1740	Improper Restriction of Excessive Authentication Attempts vulnerability in Akinsoft MyRezzta allows Authentication Bypass, Password Recovery Exploitation, Brute Force.This issue affects MyRezzta: from s2.03.01 before v2.05.01.	9.8	More Details
CVE-2025-9113	The Doccure theme for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'doccure_temp_upload_to_media' function in all versions up to, and including, 1.4.8. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2025-9114	The Doccure theme for WordPress is vulnerable to Arbitrary User Password Change in versions up to, and including, 1.4.8. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resources. This makes it possible for unauthenticated attackers to change user passwords and potentially take over administrator accounts.	9.8	More Details
CVE-2025-56266	A Host Header Injection vulnerability in Avigilon ACM v7.10.0.20 allows attackers to execute arbitrary code via supplying a crafted URL.	9.8	More Details
CVE-2025-59033	The Microsoft vulnerable driver block list is implemented as Windows Defender Application Control (WDAC) policy. On systems that do not have hypervisor-protected code integrity (HVCI) enabled, entries that specify only the to-be-signed (TBS) part of the code signer certificate are properly blocked, but entries that specify the signing certificateâ€™s TBS hash along with a 'FileAttribRef' qualifier (such as file name or version) will not be blocked. This vulnerability affects any Windows system that does not have HVCI enabled or supported (HVCI is available in Windows 10, Windows 11, and Windows Server 2016 and later). NOTE: The vendor states that the driver blocklist is intended for use with HVCI, while systems without HVCI should use App Control, and any custom blocklist entries require a granular approach for proper enforcement.	9.8	More Details
CVE-2025-57141	rsbi-os 4.7 is vulnerable to Remote Code Execution (RCE) in sqlite-jdbc.	9.8	More Details
CVE-2024-32444	Incorrect Privilege Assignment vulnerability in InspiryThemes RealHomes allows Privilege Escalation.This issue affects RealHomes: from n/a through 4.3.6.	9.8	More Details
CVE-2025-40795	A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), User Management Component (UMC) (All versions < V2.15.1.3). Affected products contain a stack-based buffer overflow vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to execute arbitrary code or to cause a denial of service condition.	9.8	More Details
CVE-2025-22956	OPSI before 4.3 allows any client to retrieve any ProductPropertyState, including those of other clients. This can lead to privilege escalation if any ProductPropertyState contains a secret only intended to be accessible by a subset of clients. One example of this is a domain join account password for the windomain package.	9.8	More Details
CVE-2025-32486	Weak Password Recovery Mechanism for Forgotten Password vulnerability in Hossein Material Dashboard. This issue affects Material Dashboard: from n/a through 1.4.6.	9.8	More Details
CVE-2025-55232	Deserialization of untrusted data in Microsoft High Performance Compute Pack (HPC) allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2025-55048	Multiple CWE-78	9.8	More Details
CVE-2025-55050	CWE-1242: Inclusion of Undocumented Features	9.8	More Details
CVE-2025-10159	An authentication bypass vulnerability allows remote attackers to gain administrative privileges on Sophos AP6 Series Wireless Access Points older than firmware version 1.7.2563 (MR7).	9.8	More Details
CVE-2025-58462	OPEXUS FOIAXpress Public Access Link (PAL) before version 11.13.1.0 allows SQL injection via SearchPopularDocs.aspx. A remote, unauthenticated attacker could read, write, or delete any content in the	9.8	More Details

	underlying database.		
CVE-2025-58447	rAthena is an open-source cross-platform massively multiplayer online role playing game (MMORPG) server. Versions prior to commit 2f5248b have a heap-based buffer overflow in the login server, remote attacker to overwrite adjacent session fields by sending a crafted `CA_SSO_LOGIN_REQ` with an oversized token length. This leads to immediate denial of service (crash) and it is possible to achieve remote code execution via heap corruption. Commit 2f5248b fixes the issue.	9.8	More Details
CVE-2025-52161	Scholl Communications AG Weblication CMS Core v019.004.000.000 was discovered to contain a cross-site scripting (XSS) vulnerability.	9.8	More Details
CVE-2025-57285	codeceptjs 3.7.3 contains a command injection vulnerability in the emptyFolder function (lib/utils.js). The execSync command directly concatenates the user-controlled directoryPath parameter without sanitization or escaping, allowing attackers to execute arbitrary commands.	9.8	More Details
CVE-2025-8359	The AdForest theme for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 6.0.9. This is due to the plugin not properly verifying a user's identity prior to authenticating them. This makes it possible for unauthenticated attackers to log in as other users, including administrators, without access to a password.	9.8	More Details
CVE-2025-41033	An SQL injection vulnerability has been found in appRain CMF 4.0.5. This vulnerability allows an attacker to retrieve, create, update, and delete the database, through the 'data%5BPage%5D%5Bname%5D' parameter in /apprain/page/manage-dynamic-pages/create.	9.8	More Details
CVE-2024-43166	Incorrect Default Permissions vulnerability in Apache DolphinScheduler. This issue affects Apache DolphinScheduler: before 3.2.2. Users are recommended to upgrade to version 3.3.1, which fixes the issue.	9.8	More Details
CVE-2025-53693	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') vulnerability in Sitecore Sitecore Experience Manager (XM), Sitecore Experience Platform (XP) allows Cache Poisoning.This issue affects Sitecore Experience Manager (XM): from 9.0 through 9.3, from 10.0 through 10.4; Experience Platform (XP): from 9.0 through 9.3, from 10.0 through 10.4.	9.8	More Details
CVE-2025-57052	cJSON 1.5.0 through 1.7.18 allows out-of-bounds access via the decode_array_index_from_pointer function in cJSON_Utils.c, allowing remote attackers to bypass array bounds checking and access restricted data via malformed JSON pointer strings containing alphanumeric characters.	9.8	More Details
CVE-2025-36890	Elevation of Privilege	9.8	More Details
CVE-2025-36896	WLAN in Android before 2025-09-05 on Google Pixel devices allows elevation of privilege, aka A-394765106.	9.8	More Details
CVE-2025-36897	In unknown of cd_CnMsgCodecUserApi.cpp, there is a possible out of bounds write due to a missing 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-2025-36904	WLAN in Android before 2025-09-05 on Google Pixel devices allows elevation of privilege, aka A-396458384.	9.8	More Details
CVE-2025-35452	PTZOptics and possibly other ValueHD-based pan-tilt-zoom cameras use default, shared credentials for the administrative web interface.	9.8	More Details
CVE-2025-41032	An SQL injection vulnerability has been found in appRain CMF 4.0.5. This vulnerability allows an attacker to retrieve, create, update, and delete the database, through the 'data%5BAdmin%5D%5Busername%5D' parameter in /apprain/admin/manage/add/.	9.8	More Details
CVE-2025-59046	The npm package `interactive-git-checkout` is an interactive command-line tool that allows users to checkout a git branch while it prompts for the branch name on the command-line. It is available as an npm package and can be installed via `npm install -g interactive-git-checkout`. Versions up to and including 1.1.4 of the `interactive-git-checkout` tool are vulnerable to a command injection vulnerability because the software passes the branch name to the `git checkout` command using the Node.js child process module's `exec()` function without proper input validation or sanitization. Commit 8dd832dd302af287a61611f4f85e157cd1c6bb41 fixes the issue.	9.8	More Details
CVE-2025-41034	An SQL injection vulnerability has been found in appRain CMF 4.0.5. This vulnerability allows an attacker to retrieve, create, update, and delete the database, through the 'data%5BPage%5D%5Bname%5D' parameter in /apprain/page/manage-static-pages/create/.	9.8	More Details
CVE-2025-35451	PTZOptics and possibly other ValueHD-based pan-tilt-zoom cameras use hard-coded, default administrative credentials. The passwords can readily be cracked. Many cameras have SSH or telnet listening on all interfaces. The passwords cannot be changed by the user, nor can the SSH or telnet service be disabled by the user.	9.8	More Details
CVE-2025-48581	In VerifyNoOverlapInSessions of apexd.cpp, there is a possible way to block security updates through mainline installations due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2025-	Deserialization of Untrusted Data vulnerability in ExpressTech Systems Quiz And Survey Master allows Object		

49401	Injection. This issue affects Quiz And Survey Master: from n/a through 10.2.5.	9.8	More Details
CVE-2025-58768	DeepChat is a smart assistant uses artificial intelligence. Prior to version 0.3.5, in the Mermaid chart rendering component, there is a risky operation of directly using `innerHTML` to set user content. Therefore, any malicious content rendered via Mermaid will directly trigger the exploit chain, leading to command execution. This vulnerability is primarily caused by a failure to fully address the existing XSS issue in the project, leading to another exploit chain. The exploit chain is consistent with the report GHSA-hqr4-4gfc-5p2j, executing arbitrary JavaScript code via XSS and arbitrary commands via exposed IPC. Version 0.3.5 contains an updated fix.	9.6	More Details
CVE-2025-58357	5ire is a cross-platform desktop artificial intelligence assistant and model context protocol client. Version 0.13.2 contains a vulnerability in the chat page's script gadgets that enables content injection attacks through multiple vectors: malicious prompt injection pages, compromised MCP servers, and exploited tool integrations. This is fixed in version 0.14.0.	9.6	More Details
CVE-2025-58997	Cross-Site Request Forgery (CSRF) vulnerability in Frenify Mow allows Code Injection. This issue affects Mow: from n/a through 4.10.	9.6	More Details
CVE-2025-56752	A vulnerability in the Ruijie RG-ES series switch firmware ESW_1.0(1)B1P39 enables remote attackers to fully bypass authentication mechanisms, providing them with unrestricted access to alter administrative settings and potentially seize control of affected devices via crafted HTTP POST request to /user.cgi.	9.4	More Details
CVE-2025-47569	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPSwings WooCommerce Ultimate Gift Card - Create, Sell and Manage Gift Cards with Customized Email Templates. This issue affects WooCommerce Ultimate Gift Card - Create, Sell and Manage Gift Cards with Customized Email Templates: from n/a through 2.8.10.	9.3	More Details
CVE-2025-58628	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in kamleshyadav Miraculous allows Blind SQL Injection. This issue affects Miraculous: from n/a through n/a.	9.3	More Details
CVE-2025-58361	Promptcraft Forge Studio is a toolkit for evaluating, optimizing, and maintaining LLM-powered applications. All versions contain an non-exhaustive URL scheme check that does not protect against XSS. User-controlled URLs pass through src/utils/validation.ts, but the check only strips `javascript:` and a few patterns. `data:` URLs (for example data:image/svg+xml,...) still pass. If a sanitized value is used in href/src, an attacker can execute a script. There is currently no fix for this issue.	9.3	More Details
CVE-2025-58819	Unrestricted Upload of File with Dangerous Type vulnerability in CreedAlly Bulk Featured Image allows Upload a Web Shell to a Web Server. This issue affects Bulk Featured Image: from n/a through 1.2.2.	9.1	More Details
CVE-2025-58448	rAthena is an open-source cross-platform massively multiplayer online role playing game (MMORPG) server. Versions prior to commit 0d89ae0 have a SQL Injection in the PartyBooking component via `WorldName` parameter. Commit 0d89ae0 fixes the issue.	9.1	More Details
CVE-2025-58762	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. In Tautulli v2.15.3 and earlier, an attacker with administrative access can use the `pms_image_proxy` endpoint to write arbitrary python scripts into the application filesystem. This leads to remote code execution when combined with the `Script` notification agent. If an attacker with administrative access changes the URL of the PMS to a server they control, they can then abuse the `pms_image_proxy` to obtain a file write into the application filesystem. This can be done by making a `pms_image_proxy` request with a URL in the `img` parameter and the desired file name in the `img_format` parameter. Tautulli then uses a hash of the desired metadata together with the `img_format` in order to construct a file path. Since the attacker controls `img_format` which occupies the end of the file path, and `img_format` is not sanitised, the attacker can then use path traversal characters to specify filename of their choosing. If the specified file does not exist, Tautaulli will then attempt to fetch the image from the configured PMS. Since the attacker controls the PMS, they can return arbitrary content in response to this request, which will then be written into the specified file. An attacker can write an arbitrary python script into a location on the application file system. The attacker can then make use of the built-in `Script` notification agent to run the local script, obtaining remote code execution on the application server. Users should upgrade to version 2.16.0 to receive a patch.	9.1	More Details
CVE-2025-57148	phpgurukul Online Shopping Portal 2.0 is vulnerable to Arbitrary File Upload in /admin/insert-product.php, due to the lack of extension validation.	9.1	More Details
CVE-2025-42958	Due to a missing authentication check in the SAP NetWeaver application on IBM i-series, the application allows high privileged unauthorized users to read, modify, or delete sensitive information, as well as access administrative or privileged functionalities. This results in a high impact on the confidentiality, integrity, and availability of the application.	9.1	More Details
CVE-2025-10134	The Goza - Nonprofit Charity WordPress Theme theme for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the alone_import_pack_restore_data() function in all versions up to, and including, 3.2.2. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	9.1	More Details
CVE-2025-10183	A blind XML External Entity (XXE) injection in the OpenMessaging webservice in TecCom TecConnect 4.1 allows an unauthenticated attacker to exfiltrate arbitrary files to an attacker-controlled server. TecConnect 4.1 is considered end-of-life as of December 2023. Users are advised to upgrade to TecCom Connect 5.	9.1	More Details

CVE-2025-54236	Adobe Commerce versions 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15 and earlier are affected by an Improper Input Validation vulnerability. A successful attacker can abuse this to achieve session takeover, increasing the confidentiality, and integrity impact to high. Exploitation of this issue does not require user interaction.	9.1	More Details
CVE-2025-40804	A vulnerability has been identified in SIMATIC Virtualization as a Service (SIVaaS) (All versions). The affected application exposes a network share without any authentication. This could allow an attacker to access or alter sensitive data without proper authorization.	9.1	More Details
CVE-2025-55049	Use of Default Cryptographic Key (CWE-1394)	9.1	More Details
CVE-2025-55244	Azure Bot Service Elevation of Privilege Vulnerability	9.0	More Details
CVE-2025-53690	Deserialization of Untrusted Data vulnerability in Sitecore Experience Manager (XM), Sitecore Experience Platform (XP) allows Code Injection.This issue affects Experience Manager (XM): through 9.0; Experience Platform (XP): through 9.0.	9.0	More Details
CVE-2025-55241	Azure Entra Elevation of Privilege Vulnerability	9.0	More Details
CVE-2025-54261	ColdFusion versions 2025.3, 2023.15, 2021.21 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary code execution by an attacker. Scope is changed.	9.0	More Details
CVE-2025-47579	Deserialization of Untrusted Data vulnerability in ThemeGoods Photography. This issue affects Photography: from n/a through 7.5.2.	9.0	More Details
CVE-2025-58746	The Volkov Labs Business Links panel for Grafana provides an interface to navigate using external links, internal dashboards, time pickers, and dropdown menus. Prior to version 2.4.0, a malicious actor with Editor privileges can escalate their privileges to Administrator and perform arbitrary administrative actions. This is possible because the plugin allows arbitrary JavaScript code injection in the [Layout] → [Link] → [URL] field. Version 2.4.0 contains a fix for the issue.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-55145	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker to hijack existing HTML5 connections.	8.9	More Details
CVE-2025-57151	phpgurukul Complaint Management System 2.0 is vulnerable to Cross Site Scripting (XSS) in admin/userprofile.php via the fullname parameter.	8.8	More Details
CVE-2025-9712	Insufficient filename validation in Ivanti Endpoint Manager before 2024 SU3 SR1 and 2022 SU8 SR2 allows a remote unauthenticated attacker to achieve remote code execution. User interaction is required.	8.8	More Details
CVE-2025-48534	In getDefaultCBRPackageName of CellBroadcastHandler.java, there is a possible escalation of privilege due to a logic error in the code. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2025-58755	MONAI (Medical Open Network for AI) is an AI toolkit for health care imaging. The extractall function `zip_file.extractall(output_dir)` is used directly to process compressed files. It is used in many places in the project. In versions up to and including 1.5.0, when the Zip file containing malicious content is decompressed, it overwrites the system files. In addition, the project allows the download of the zip content through the link, which increases the scope of exploitation of this vulnerability. As of time of publication, no known fixed versions are available.	8.8	More Details
CVE-2025-9938	A weakness has been identified in D-Link DI-8400 16.07.26A1. The affected element is the function yyxz_dlink_asp of the file /yyxz.asp. This manipulation of the argument ID causes stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.	8.8	More Details
CVE-2024-36342	Improper input validation in the GPU driver could allow an attacker to exploit a heap overflow potentially resulting in arbitrary code execution.	8.8	More Details
CVE-2025-41682	An authenticated, low-privileged attacker can obtain credentials stored on the charge controller including the manufacturer password.	8.8	More Details
CVE-	MONAI (Medical Open Network for AI) is an AI toolkit for health care imaging. In versions up to and including 1.5.0,		

2025-58757	the `pickle_operations` function in `monai/data/utils.py` automatically handles dictionary key-value pairs ending with a specific suffix and deserializes them using `pickle.loads()` . This function also lacks any security measures. The deserialization may lead to code execution. As of time of publication, no known fixed versions are available.	8.8	More Details
CVE-2025-53691	Deserialization of Untrusted Data vulnerability in Sitecore Experience Manager (XM), Sitecore Experience Platform (XP) allows Remote Code Execution (RCE).This issue affects Experience Manager (XM): from 9.0 through 9.3, from 10.0 through 10.4; Experience Platform (XP): from 9.0 through 9.3, from 10.0 through 10.4.	8.8	More Details
CVE-2025-10120	A vulnerability was detected in Tenda AC20 up to 16.03.08.12. The impacted element is the function strcpy of the file /goform/GetParentControlInfo. The manipulation of the argument mac results in buffer overflow. The attack may be performed from remote. The exploit is now public and may be used.	8.8	More Details
CVE-2025-26438	In smp_process_secure_connection_oob_data of smp_act.cc, there is a possible way to bypass SMP authentication due to Incorrect implementation of a protocol. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2025-9872	Insufficient filename validation in Ivanti Endpoint Manager before 2024 SU3 SR1 and 2022 SU8 SR2 allows a remote unauthenticated attacker to achieve remote code execution. User interaction is required.	8.8	More Details
CVE-2025-54106	Integer overflow or wraparound in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2025-10169	A weakness has been identified in UTT 1200GW up to 3.0.0-170831. Affected by this issue is some unknown functionality of the file /goform/ConfigWirelessBase. This manipulation of the argument ssid causes buffer overflow. The attack may be initiated 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.	8.8	More Details
CVE-2025-54110	Integer overflow or wraparound in Windows Kernel allows an authorized attacker to elevate privileges locally.	8.8	More Details
CVE-2025-54113	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2025-9866	Inappropriate implementation in Extensions in Google Chrome prior to 140.0.7339.80 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2025-9864	Use after free in V8 in Google Chrome prior to 140.0.7339.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-55147	CSRF in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote unauthenticated attacker to execute sensitive actions on behalf of the victim user. User interaction is required	8.8	More Details
CVE-2024-43115	Improper Input Validation vulnerability in Apache DolphinScheduler. An authenticated user can execute any shell script server by alert script. This issue affects Apache DolphinScheduler: before 3.2.2. Users are recommended to upgrade to version 3.3.1, which fixes the issue.	8.8	More Details
CVE-2025-54897	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	8.8	More Details
CVE-2025-55142	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure authentication related settings.	8.8	More Details
CVE-2025-55141	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure authentication related settings.	8.8	More Details
CVE-2025-48101	Deserialization of Untrusted Data vulnerability in webdevstudios Constant Contact for WordPress allows Object Injection. This issue affects Constant Contact for WordPress: from n/a through 4.1.1.	8.8	More Details
CVE-2025-58756	MONAI (Medical Open Network for AI) is an AI toolkit for health care imaging. In versions up to and including 1.5.0, in `model_dict = torch.load(full_path, map_location=torch.device(device), weights_only=True)` in monai/bundle/scripts.py , `weights_only=True` is loaded securely. However, insecure loading methods still exist elsewhere in the project, such as when loading checkpoints. This is a common practice when users want to reduce training time and costs by loading pre-trained models downloaded from other platforms. Loading a checkpoint	8.8	More Details

	containing malicious content can trigger a deserialization vulnerability, leading to code execution. As of time of publication, no known fixed versions are available.		
CVE-2025-10170	A security vulnerability has been detected in UTT 1200GW up to 3.0.0-170831. This affects the function sub_4B48F8 of the file /goform/formApLbConfig. Such manipulation of the argument loadBalanceNameOld leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-36855	A vulnerability (CVE-2025-21176 https://www.cve.org/CVERecord) exists in DiaSymReader.dll due to buffer over-read. Per CWE-126: Buffer Over-read https://cwe.mitre.org/data/definitions/126.html , Buffer Over-read is when a product reads from a buffer using buffer access mechanisms such as indexes or pointers that reference memory locations after the targeted buffer. This issue affects EOL ASP.NET 6.0.0 <= 6.0.36 as represented in this CVE, as well as 8.0.0 <= 8.0.11 & <= 9.0.0 as represented in CVE-2025-21176. Additionally, if you've deployed self-contained applications https://docs.microsoft.com/dotnet/core/deploying/#self-contained-deployments-scd targeting any of the impacted versions, these applications are also vulnerable and must be recompiled and redeployed. NOTE: This CVE affects only End Of Life (EOL) software components. The vendor, Microsoft, has indicated there will be no future updates nor support provided upon inquiry.	8.8	More Details
CVE-2025-56265	An arbitrary file upload vulnerability in the Chat Trigger component of N8N v1.95.3, v1.100.1, and v1.101.1 allows attackers to execute arbitrary code via uploading a crafted HTML file.	8.8	More Details
CVE-2025-54918	Improper authentication in Windows NTLM allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2025-10172	A flaw has been found in UTT 750W up to 3.2.2-191225. This issue affects some unknown processing of the file /goform/formPictureUrl. Executing manipulation of the argument importpictureurl can lead to buffer overflow. The attack can be executed remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-9112	The Doccure theme for WordPress is vulnerable to arbitrary file uploads due to incorrect file type validation in the 'doccure_temp_file_uploader' function in all versions up to, and including, 1.4.8. This makes it possible for authenticated attackers, with subscriber-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2025-32318	In Skia, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2025-58163	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Versions 1.8.185 and earlier contain a deserialization of untrusted data vulnerability that allows authenticated attackers with knowledge of the application's APP_KEY to achieve remote code execution. The vulnerability is exploited via endpoint, e.g.: `/help/{mailbox_id}/auth/{customer_id}/{hash}/{timestamp}` where the `customer_id` and `timestamp` parameters are processed through the decrypt function in `app/Helper.php` without proper validation. The code decrypts using Laravel's built-in encryption functions, which subsequently deserialize the decrypted payload without sanitization, allowing attackers to craft malicious serialized PHP objects using classes to trigger arbitrary command execution. This is fixed in version 1.8.186.	8.8	More Details
CVE-2025-55227	Improper neutralization of special elements used in a command ('command injection') in SQL Server allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2025-48543	In multiple locations, there is a possible way to escape chrome sandbox to attack android system_server due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2025-53303	Deserialization of Untrusted Data vulnerability in ThemeMove ThemeMove Core allows Object Injection. This issue affects ThemeMove Core: from n/a through 1.4.2.	8.8	More Details
CVE-2025-36901	WLAN in Android before 2025-09-05 on Google Pixel devices allows elevation of privilege, aka A-396462223.	8.8	More Details
CVE-2025-52389	An Insecure Direct Object Reference (IDOR) in Envasadora H2O Eireli - Soda Cristal v40.20.4 allows authenticated attackers to access sensitive data for other users via a crafted HTTP request.	8.8	More Details
CVE-2025-10171	A vulnerability was detected in UTT 1250GW up to 3.2.2-200710. This vulnerability affects the function sub_453DC of the file /goform/formConfigApConfTemp. Performing manipulation results in buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-	A vulnerability was found in D-Link DIR-825 1.08.01. This impacts the function get_ping6_app_stat of the file ping6_response.cg of the component httpd. Performing manipulation of the argument ping6_ipaddr results in buffer overflow. It is possible to initiate the attack remotely. The exploit has been made public and could be used. This	8.8	More Details

10034	vulnerability only affects products that are no longer supported by the maintainer.		
CVE-2025-42933	When a user logs in via SAP Business One native client, the SLD backend service fails to enforce proper encryption of certain APIs. This leads to exposure of sensitive credentials within http response body. As a result, it has a high impact on the confidentiality, integrity, and availability of the application.	8.8	More Details
CVE-2025-58833	Cross-Site Request Forgery (CSRF) vulnerability in INVELITY Invelity MyGLS connect allows Object Injection. This issue affects Invelity MyGLS connect: from n/a through 1.1.1.	8.8	More Details
CVE-2025-55234	SMB Server might be susceptible to relay attacks depending on the configuration. An attacker who successfully exploited these vulnerabilities could perform relay attacks and make the users subject to elevation of privilege attacks. The SMB Server already supports mechanisms for hardening against relay attacks: SMB Server signing SMB Server Extended Protection for Authentication (EPA) Microsoft is releasing this CVE to provide customers with audit capabilities to help them to assess their environment and to identify any potential device or software incompatibility issues before deploying SMB Server hardening measures that protect against relay attacks. If you have not already enabled SMB Server hardening measures, we advise customers to take the following actions to be protected from these relay attacks: Assess your environment by utilizing the audit capabilities that we are exposing in the September 2025 security updates. See Support for Audit Events to deploy SMB Server Hardening—SMB Server Signing & SMB Server EPA. Adopt appropriate SMB Server hardening measures.	8.8	More Details
CVE-2025-36891	Elevation of privilege	8.8	More Details
CVE-2025-26210	DeepSeek R1 through V3.1 allows XSS, as demonstrated by JavaScript execution in the context of the run-html-chat.deepseeksvc.com domain. NOTE: some third parties have indicated that this is intended behavior.	8.8	More Details
CVE-2025-58176	Dive is an open-source MCP Host Desktop Application that enables integration with function-calling LLMs. In versions 0.9.0 through 0.9.3, there is a one-click Remote Code Execution vulnerability triggered through a custom url value, `transport` in the JSON object. An attacker can exploit the vulnerability in the following two scenarios: a victim visits a malicious website controlled by the attacker and the website redirect to the URL automatically, or a victim clicks on such a crafted link embedded on a legitimate website (e.g., in user-generated content). In both cases, the browser invokes Dive's custom URL handler (dive:), which launches the Dive app and processes the crafted URL, leading to arbitrary code execution on the victim’s machine. This vulnerability is caused by improper processing of custom url. This is fixed in version 0.9.4.	8.8	More Details
CVE-2025-23256	NVIDIA BlueField contains a vulnerability in the management interface, where an attacker with local access could cause incorrect authorization to modify the configuration. A successful exploit of this vulnerability might lead to denial of service, escalation of privileges, information disclosure, and data tampering.	8.7	More Details
CVE-2023-31322	Type confusion in the ASP could allow an attacker to pass a malformed argument to the Reliability, Availability, and Serviceability trusted application (RAS TA) potentially leading to a read or write to shared memory resulting in loss of confidentiality, integrity, or availability.	8.7	More Details
CVE-2025-2411	Improper Restriction of Excessive Authentication Attempts vulnerability in Akinsoft TaskPano allows Authentication Bypass.This issue affects TaskPano: from s1.06.04 before v1.06.06.	8.6	More Details
CVE-2025-2415	Improper Restriction of Excessive Authentication Attempts vulnerability in Akinsoft MyRezzta allows Authentication Bypass.This issue affects MyRezzta: from s2.03.01 before v2.05.01.	8.6	More Details
CVE-2025-2417	Improper Restriction of Excessive Authentication Attempts vulnerability in Akinsoft e-Mutabakat allows Authentication Bypass.This issue affects e-Mutabakat: from 2.02.06 before v2.02.06.	8.6	More Details
CVE-2025-58761	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. The `real_pms_image_proxy` endpoint in Tautulli v2.15.3 and prior is vulnerable to path traversal, allowing unauthenticated attackers to read arbitrary files from the application server's filesystem. The `real_pms_image_proxy` is used to fetch an image directly from the backing Plex Media Server. The image to be fetched is specified through an `img` URL parameter, which can either be a URL or a file path. There is some validation ensuring that `img` begins with the prefix `interfaces/default/images` in order to be served from the local filesystem. However this can be bypassed by passing an `img` parameter which begins with a valid prefix, and then adjoining path traversal characters in order to reach files outside of intended directories. An attacker can exfiltrate files on the application file system, including the `tautulli.db` SQLite database containing active JWT tokens, as well as the `config.ini` file which contains the hashed admin password, the JWT token secret, and the Plex Media Server token and connection details. If the password is cracked, or if a valid JWT token is present in the database, an unauthenticated attacker can escalate their privileges to obtain administrative control over the application. Version 2.16.0 contains a fix for the issue.	8.6	More Details
CVE-	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. The `/image` API endpoint in Tautulli v2.15.3 and earlier is vulnerable to path traversal, allowing unauthenticated attackers to read arbitrary files from the application server's filesystem. In Tautulli, the `/image` API endpoint is used to serve static images from the application's data directory to users. This endpoint can be accessed without authentication, and its intended purpose is for server background images and icons within the user interface. Attackers can exfiltrate files from the		More

2025-58760	application file system, including the `tautulli.db` SQLite database containing active JWT tokens, as well as the `config.ini` file which contains the hashed admin password, the JWT token secret, and the Plex Media Server token and connection details. If the password is cracked, or if a valid JWT token is present in the database, an unauthenticated attacker can escalate their privileges to obtain administrative control over the application. Version 2.16.0 contains a fix for the issue.	8.6	Details
CVE-2025-8085	The Ditty WordPress plugin before 3.1.58 lacks authorization and authentication for requests to its displayItems endpoint, allowing unauthenticated visitors to make requests to arbitrary URLs.	8.6	More Details
CVE-2025-54256	Dreamweaver Desktop versions 21.5 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must click on a malicious link, and scope is changed.	8.6	More Details
CVE-2025-2416	Improper Restriction of Excessive Authentication Attempts vulnerability in Akinsoft LimonDesk allows Authentication Bypass.This issue affects LimonDesk: from s1.02.14 before v1.02.17.	8.6	More Details
CVE-2023-21480	Improper input validation vulnerability in CertByte prior to SMR Apr-2023 Release 1 allows local attackers to launch privileged activities.	8.5	More Details
CVE-2025-58881	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in gopiplus New Simple Gallery allows Blind SQL Injection. This issue affects New Simple Gallery: from n/a through 8.0.	8.5	More Details
CVE-2025-58281	Out-of-bounds read vulnerability in the runtime interpreter module. Impact: Successful exploitation of this vulnerability may affect availability.	8.4	More Details
CVE-2025-54910	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2024-36326	Missing authorization in AMD RomArmor could allow an attacker to bypass ROMArmor protections during system resume from a standby state, potentially resulting in a loss of confidentiality and integrity.	8.4	More Details
CVE-2025-58280	Vulnerability of exposing object heap addresses in the Ark eTS module. Impact: Successful exploitation of this vulnerability may affect availability.	8.4	More Details
CVE-2025-55849	WeiPHP v5.0 and before is vulnerable to SQL Injection via the SucaiController.class.php file and the cancelTemplatee	8.4	More Details
CVE-2025-56803	Figma Desktop for Windows version 125.6.5 contains a command injection vulnerability in the local plugin loader. An attacker can execute arbitrary OS commands by setting a crafted build field in the plugin's manifest.json. This field is passed to child_process.exec without validation, leading to possible RCE. NOTE: this is disputed by the Supplier because the behavior only allows a local user to attack himself via a local plugin. The local build procedure, which is essential to the attack, is not executed for plugins shared to the Figma Community.	8.4	More Details
CVE-2025-36193	IBM Transformation Advisor 2.0.1 through 4.3.1 incorrectly assigns privileges to security critical files which could allow a local root escalation inside a container running the IBM Transformation Advisor Operator Catalog image.	8.4	More Details
CVE-2025-36899	There is a possible escalation of privilege due to test/debugging code left in a production build. This could lead to physical escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.4	More Details
CVE-2025-55047	CWE-798 Use of Hard-coded Credentials	8.4	More Details
CVE-2024-36352	Improper input validation in the AMD Graphics Driver could allow an attacker to supply a specially crafted pointer, potentially leading to arbitrary writes or denial of service.	8.4	More Details
CVE-2025-7388	It was possible to perform Remote Command Execution (RCE) via Java RMI interface in the OpenEdge AdminServer, allowing authenticated users to inject and execute OS commands under the delegated authority of the AdminServer process. An RMI interface permitted manipulation of a configuration property with inadequate input validation leading to OS command injection.	8.4	More Details
CVE-2025-58750	rAthena is an open-source cross-platform massively multiplayer online role playing game (MMORPG) server. Versions prior to commit 0cc348b are missing a bound check in `chclif_parse_moveCharSlot` that can result in reading and writing out of bounds using input from the user. The problem has been fixed in commit 0cc348b.	8.2	More Details

CVE-2025-7040	The Cloud SAML SSO plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'set_organization_settings' action of the csso_handle_actions() function in all versions up to, and including, 1.0.19. The handler reads client-supplied POST parameters for organization settings and passes them directly to update_option() without any check of the user's capabilities or a CSRF nonce. This makes it possible for unauthenticated attackers to change critical configuration (including toggling signing and encryption), potentially breaking the SSO flow and causing a denial-of-service.	8.2	More Details
CVE-2025-23342	The NVIDIA NVDebug tool contains a vulnerability that may allow an actor to gain access to a privileged account . A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure and data tampering.	8.2	More Details
CVE-2025-58353	Promptcraft Forge Studio is a toolkit for evaluating, optimizing, and maintaining LLM-powered applications. All versions of Promptcraft Forge Studio sanitize user input using regex blacklists such as r`eplace(/javascript:/gi, '')`. Because the package uses multi-character tokens and each replacement is applied only once, removing one occurrence can create a new dangerous token due to overlap. The "sanitized" value may still contain an executable payload when used in href/src (or injected into the DOM). There is currently no fix for this issue.	8.2	More Details
CVE-2025-33045	APTIOV contains vulnerabilities in the BIOS where a privileged user may cause "Write-what-where Condition" and "Exposure of Sensitive Information to an Unauthorized Actor" through local access. The successful exploitation of these vulnerabilities can lead to information disclosure, arbitrary data writing, and impact Confidentiality, Integrity, and Availability.	8.2	More Details
CVE-2025-58439	ERP is a free and open source Enterprise Resource Planning tool. In versions below 14.89.2 and 15.0.0 through 15.75.1, lack of validation of parameters left certain endpoints vulnerable to error-based SQL Injection. Some information like version could be retrieved. This issue is fixed in versions 14.89.2 and 15.76.0.	8.1	More Details
CVE-2025-58370	Roo Code is an AI-powered autonomous coding agent that lives in users' editors. Versions below 3.26.0 contain a vulnerability in the command parsing logic where the Bash parameter expansion and indirect reference were not handled correctly. If the agent was configured to auto-approve execution of certain commands, an attacker able to influence prompts could abuse this weakness to execute additional arbitrary commands alongside the intended one. This is fixed in version 3.26.0.	8.1	More Details
CVE-2025-9566	There's a vulnerability in podman where an attacker may use the kube play command to overwrite host files when the kube file container a Secrete or a ConfigMap volume mount and such volume contains a symbolic link to a host file path. In a successful attack, the attacker can only control the target file to be overwritten but not the content to be written into the file. Binary-Affected: podman Upstream-version-introduced: v4.0.0 Upstream-version-fixed: v5.6.1	8.1	More Details
CVE-2025-42916	Due to missing input validation, an attacker with high privilege access to ABAP reports could delete the content of arbitrary database tables, if the tables are not protected by an authorization group. This leads to a high impact on integrity and availability of the database but no impact on confidentiality.	8.1	More Details
CVE-2025-36854	A vulnerability (CVE-2024-38229 https://www.cve.org/CVERecord) exists in EOL ASP.NET when closing an HTTP/3 stream while application code is writing to the response body, a race condition may lead to use-after-free, resulting in Remote Code Execution. Per CWE-416: Use After Free https://cwe.mitre.org/data/definitions/416.html , Use After Free is when a product reuses or references memory after it has been freed. At some point afterward, the memory may be allocated again and saved in another pointer, while the original pointer references a location somewhere within the new allocation. Any operations using the original pointer are no longer valid because the memory "belongs" to the code that operates on the new pointer. This issue affects EOL ASP.NET 6.0.0 <= 6.0.36 as represented in this CVE, as well as 8.0.0 <= 8.0.8, 9.0.0-preview.1.24081.5 <= 9.0.0.RC.1 as represented in CVE-2024-38229 https://www.cve.org/CVERecord . Additionally, if you've deployed self-contained applications https://docs.microsoft.com/dotnet/core/deploying/#self-contained-deployments-scd targeting any of the impacted versions, these applications are also vulnerable and must be recompiled and redeployed. NOTE: This CVE only represents End Of Life (EOL) software components. The vendor, Microsoft, has indicated there will be no future updates nor support provided upon inquiry.	8.1	More Details
CVE-2025-9990	The WordPress Helpdesk Integration plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 5.8.10 via the portal_type parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	8.1	More Details
CVE-2025-58372	Roo Code is an AI-powered autonomous coding agent that lives in users' editors. Versions 3.25.23 and below contain a vulnerability where certain VS Code workspace configuration files (.code-workspace) are not protected in the same way as the .vscode folder. If the agent was configured to auto-approve file writes, an attacker able to influence prompts (for example via prompt injection) could cause malicious workspace settings or tasks to be written. These tasks could then be executed automatically when the workspace is reopened, resulting in arbitrary code execution. This issue is fixed in version 3.26.0.	8.1	More Details
CVE-2025-55998	A cross-site scripting (XSS) vulnerability in Smart Search & Filter Shopify App 1.0 allows a remote attacker to execute arbitrary JavaScript in the web browser of a user, by including a malicious payload into the color filter parameter.	8.1	More Details
CVE-2025-58214	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in gavias Indutri allows PHP Local File Inclusion. This issue affects Indutri: from n/a through n/a.	8.1	More Details

CVE-2025-54709	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in uxper Sala. This issue affects Sala: from n/a through 1.1.6.	8.1	More Details
CVE-2025-58206	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove MaxCoach allows PHP Local File Inclusion. This issue affects MaxCoach: from n/a through 3.2.5.	8.1	More Details
CVE-2025-57146	phpgurukul Complaint Management System in PHP 2.0 is vulnerable to SQL Injection in user/reset-password.php via the mobileno parameter.	8.1	More Details
CVE-2025-42929	Due to missing input validation, an attacker with high privilege access to ABAP reports could delete the content of arbitrary database tables, if the tables are not protected by an authorization group. This leads to a high impact on integrity and availability of the database.	8.1	More Details
CVE-2025-48530	In multiple locations, there is a possible condition that results in OOB accesses due to an incorrect bounds check. This could lead to remote code execution in combination with other bugs, with no additional execution privileges needed. User interaction is not needed for exploitation.	8.1	More Details
CVE-2025-58437	Coder allows organizations to provision remote development environments via Terraform. In versions 2.22.0 through 2.24.3, 2.25.0 and 2.25.1, Coder can be compromised through insecure session handling in prebuilt workspaces. Coder automatically generates a session token for a user when a workspace is started. It is automatically exposed via coder_workspace_owner.session_token. Prebuilt workspaces are initially owned by a built-in prebuilds system user. When a prebuilt workspace is claimed, a new session token is generated for the user that claimed the workspace, but the previous session token for the prebuilds user was not expired. Any Coder workspace templates that persist this automatically generated session token are potentially impacted. This is fixed in versions 2.24.4 and 2.25.2.	8.1	More Details
CVE-2025-58215	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in gavias Ziston allows PHP Local File Inclusion. This issue affects Ziston: from n/a through n/a.	8.1	More Details
CVE-2023-21475	Out-of-bounds Write vulnerability in libaudiosaplus_sec.so library prior to SMR Apr-2023 Release 1 allows local attacker to execute arbitrary code.	8.0	More Details
CVE-2025-9539	The AutomatorWP – Automator plugin for no-code automations, webhooks & custom integrations in WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the automatorwp_ajax_import_automation_from_url function in all versions up to, and including, 5.3.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create arbitrary automations, which can lead to Remote Code Execution or Privilege escalation once such automation is activated by the administrator	8.0	More Details
CVE-2025-48539	In SendPacketToPeer of acl_arbiter.cc, there is a possible out of bounds read due to a use after free. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	8.0	More Details
CVE-2025-58763	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. A command injection vulnerability in Tautulli v2.15.3 and prior allows attackers with administrative privileges to obtain remote code execution on the application server. This vulnerability requires the application to have been cloned from GitHub and installed manually. When Tautulli is cloned directly from GitHub and installed manually, the application manages updates and versioning through calls to the `git` command. In the code, this is performed through the `runGit` function in `versioncheck.py`. Since `shell=True` is passed to `subproces.Popen`, this call is vulnerable to subject to command injection, as shell characters within arguments will be passed to the underlying shell. A concrete location where this can be triggered is in the `checkout_git_branch` endpoint. This endpoint stores a user-supplied remote and branch name into the `GIT_REMOTE` and `GIT_BRANCH` configuration keys without sanitization. Downstream, these keys are then fetched and passed directly into `runGit` using a format string. Hence, code execution can be obtained by using `$()` interpolation in a command. Version 2.16.0 contains a fix for the issue.	8.0	More Details
CVE-2023-21476	Out-of-bounds Write vulnerability in libaudiosaplus_sec.so library prior to SMR Apr-2023 Release 1 allows local attacker to execute arbitrary code.	8.0	More Details
CVE-2025-9636	pgAdmin <= 9.7 is affected by a Cross-Origin Opener Policy (COOP) vulnerability. This vulnerability allows an attacker to manipulate the OAuth flow, potentially leading to unauthorised account access, account takeover, data breaches, and privilege escalation.	7.9	More Details
CVE-2023-21477	Access of Memory Location After End of Buffer vulnerability in TIGERF trustlet prior to SMR Apr-2023 Release 1 allows local attackers to access protected data.	7.9	More Details
CVE-2021-26383	Insufficient bounds checking in AMD TEE (Trusted Execution Environment) could allow an attacker with a compromised userspace to invoke a command with malformed arguments leading to out of bounds memory access, potentially resulting in loss of integrity or availability.	7.9	More Details
CVE-	In setDisplayName of AssociationRequest.java, there is a possible way for an app to retain CDM association due to a		More

2025-48522	logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	Details
CVE-2025-54242	Premiere Pro versions 25.3, 24.6.5 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file, and scope is unchanged.	7.8	More Details
CVE-2025-32345	In updateState of ContentProtectionTogglePreferenceController.java, there is a possible way for a secondary user to disable the primary user's deceptive app scanning setting due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-32346	In onActivityResult of VoicemailSettingsActivity.java, there is a possible work profile contact number leak due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48531	In getCallingPackageName of CredentialStorage, there is a possible permission bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-32347	In onStart of BiometricEnrollIntroduction.java, there is a possible way to determine the device's location due to an unsafe PendingIntent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2025-0089	In multiple locations, there is a possible way to hijack the Launcher app due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-26431	In setupAccessibilityServices of AccessibilityFragment.java, there is a possible way to hide an enabled accessibility service due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-9365	Fuji Electric FRENIC-Loader 4 is vulnerable to a deserialization of untrusted data when importing a file through a specified window, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2025-54098	Improper access control in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-48552	In saveGlobalProxyLocked of DevicePolicyManagerService.java, there is a possible way to desync from persistence due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-26439	In getComponentName of AccessibilitySettingsUtils.java, there is a possible way to for a malicious Talkback service to be enabled instead of the system component due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54111	Use after free in Windows UI XAML Phone DatePickerFlyout allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-48553	In handlePackagesChanged of DevicePolicyManagerService.java, there is a possible DoS of a device admin due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54257	Acrobat Reader versions 24.001.30254, 20.005.30774, 25.001.20672 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file, and scope is unchanged.	7.8	More Details
CVE-2025-54102	Use after free in Windows Connected Devices Platform Service allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-48558	In multiple functions of BatteryService.java, there is a possible way to hijack implicit intent intended for system app due to Implicit intent hijacking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-32350	In maybeShowDialog of ControlsSettingsDialogManager.kt, there is a possible overlay of the ControlsSettingsDialog due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-32322	In onCreate of MediaProjectionPermissionActivity.java , there is a possible way to grant a malicious app a token enabling unauthorized screen recording capabilities due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-	In onCreate of SelectAccountActivity.java, there is a possible way to add contacts without permission due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User	7.8	More Details

48523	interaction is not needed for exploitation.		
CVE-2025-32349	In multiple locations, there is a possible privilege escalation due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-32333	In startSpaActivityForApp of SpaActivity.kt, there is a possible cross-user permission bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54243	Substance3D - Viewer versions 0.25.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-48546	In checkPermissions of SafeActivityOptions.java, there is a possible background activity launch due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-53801	Untrusted pointer dereference in Windows DWM allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-53800	No cwe for this issue in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-48544	In multiple locations, there is a possible way to read files belonging to other apps due to SQL injection. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54260	Substance3D - Modeler versions 1.22.2 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is unchanged.	7.8	More Details
CVE-2025-54091	Integer overflow or wraparound in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-54092	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-32320	In System UI, there is a possible way to view other users' images due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54259	Substance3D - Modeler versions 1.22.2 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is unchanged.	7.8	More Details
CVE-2025-36906	In ConvertReductionOp of darwinn_mlir_converter_aidl.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-36905	In gxp_mapping_create of gxp_mapping.c, there is a possible privilege escalation due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-36903	In lwis_io_buffer_write, there is a possible OOB read/write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48549	In multiple locations, there is a possible way to record audio via a background app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54258	Substance3D - Modeler versions 1.22.2 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is unchanged.	7.8	More Details
CVE-2025-49459	Missing authorization in the installer for Zoom Workplace for Windows on ARM before version 6.5.0 may allow an authenticated user to conduct an escalation of privilege via local access.	7.8	More Details
CVE-2025-	In onCreate of FaceSettings.java, there is a possible way to remove biometric unlock across user profiles due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges	7.8	More Details

48541	needed. User interaction is not needed for exploitation.		
CVE-2025-36898	There is a possible escalation of privilege due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48540	In processTransactInternal of RpcState.cpp, there is a possible local out of memory write due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-49692	Improper access control in Azure Windows Virtual Machine Agent allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-54245	Substance3D - Viewer versions 0.25.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-36887	In wl_cfgscan_update_v3_schedscan_results() of wl_cfgscan.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54244	Substance3D - Viewer versions 0.25.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-56190	In wl_update_hidden_ap_ie() of wl_cfgscan.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48535	In assertSafeToStartCustomActivity of AppRestrictionsFragment.java , there is a possible way to exploit a parcel mismatch resulting in a launch anywhere vulnerability due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-26450	In onInputEvent of IInputMethodSessionWrapper.java, there is a possible way for an untrusted app to inject key and motion events to the default IME due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-26435	In updateState of ContentProtectionTogglePreferenceController.java, there is a possible way for a secondary user to disable the primary user's deceptive app scanning setting due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-26458	In multiple functions of LocationProviderManager.java, there is a possible background activity launch due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54902	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-26436	In clearAllowBgActivityStarts of PendingIntentRecord.java, there is a possible way for an application to launch an activity from the background due to BAL Bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-26462	In AccessibilityServiceConnection.java, there is a possible background activity launch due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54903	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-55317	Improper link resolution before file access ('link following') in Microsoft AutoUpdate (MAU) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-26440	In multiple functions of CameraService.cpp, there is a possible way to use the camera from the background due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54904	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-32332	In multiple locations, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details

CVE-2025-55316	External control of file name or path in Azure Arc allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-55245	Improper link resolution before file access ('link following') in Xbox allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-54913	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows UI XAML Maps MapControlSettings allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-55228	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to execute code locally.	7.8	More Details
CVE-2025-26444	In onHandleForceStop of VoiceInteractionManagerService.java, there is a bug that could cause the system to incorrectly revert to the default assistant application when a user-selected assistant is forcibly stopped due to a logic error in the code. This could lead to local escalation of privilege where the default assistant app is automatically granted ROLE_ASSISTANT with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-32321	In isSafeIntent of AccountTypePreferenceLoader.java, there is a possible way to bypass an intent type check due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54906	Free of memory not on the heap in Microsoft Office allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-26464	In executeAppFunction of AppSearchManagerService.java, there is a possible background activity launch due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54907	Heap-based buffer overflow in Microsoft Office Visio allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-41701	An unauthenticated attacker can trick a local user into executing arbitrary commands by opening a deliberately manipulated project file with an affected engineering tool. These arbitrary commands are executed in the user context.	7.8	More Details
CVE-2025-54908	Use after free in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-54912	Use after free in Windows BitLocker allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-48563	In onNullBinding of RemoteFillService.java, there is a possible background activity launch due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-26455	In multiple functions of NdkMediaCodec.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54900	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-26452	In loadDrawableForCookie of ResourcesImpl.java, there is a possible way to access task snapshots of other apps due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-32312	In createIntentsList of PackageParser.java , there is a possible way to bypass lazy bundle hardening, allowing modified data to be passed to the next process due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-32327	In multiple functions of PickerDbFacade.java, there is a possible unauthorized data access due to SQL injection. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-55224	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to execute code locally.	7.8	More Details

CVE-2025-9817	SSH dissector crash in Wireshark 4.4.0 to 4.4.8 allows denial of service	7.8	More Details
CVE-2025-54894	Local Security Authority Subsystem Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2025-58374	Roo Code is an AI-powered autonomous coding agent that lives in users' editors. Versions 3.25.23 and below contain a default list of allowed commands that do not need manual approval if auto-approve is enabled, and npm install is included in that list. Because npm install executes lifecycle scripts, if a repository's package.json file contains a malicious postinstall script, it would be executed automatically without user approval. This means that enabling auto-approved commands and opening a malicious repo could result in arbitrary code execution. This is fixed in version 3.26.0.	7.8	More Details
CVE-2025-54895	Integer overflow or wraparound in Windows SPNEGO Extended Negotiation allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-22414	In FrpBypassAlertActivity of FrpBypassAlertActivity.java, there is a possible way to bypass FRP due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54916	Stack-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.	7.8	More Details
CVE-2025-32326	In multiple functions of AppRestrictionsFragment.java, there is a possible way to bypass intent security check due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2025-32325	In appendFrom of Parcel.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54896	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-26430	In getDestinationForApp of SpaAppBridgeActivity, there is a possible cross-user file reveal due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-32324	In onCommand of ActivityManagerShellCommand.java, there is a possible arbitrary activity launch due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-32323	In getCallingAppName of Shared.java, there is a possible way to trick users into granting file access via deceptive text in a permission popup due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-32331	In showDismissibleKeyguard of KeyguardService.java, there is a possible way to bypass app pinning due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-26454	In validateUriSchemeAndPermission of DisclaimersParserImpl.java , there is a possible way to access data from another user due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54898	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-54899	Free of memory not on the heap in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2024-49714	In avrc_vendor_msg of avrc_opt.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to paired device escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-34598	Improper export of component in GoodLock prior to version 2.2.04.95 allows local attackers to install arbitrary applications from Galaxy Store.	7.7	More Details
CVE-2025-	Soft Serve is a self-hostable Git server for the command line. In versions 0.9.1 and below, attackers can create or	7.7	More

58355	override arbitrary files with uncontrolled data through its SSH API. This issue is fixed in version 0.10.0.		Details
CVE-2025-54248	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access. Scope is changed	7.7	More Details
CVE-2025-58789	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeisle WP Full Stripe Free allows SQL Injection. This issue affects WP Full Stripe Free: from n/a through 8.3.0.	7.6	More Details
CVE-2025-58604	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPFunnels Mail Mint allows SQL Injection. This issue affects Mail Mint: from n/a through 1.18.5.	7.6	More Details
CVE-2025-58788	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Saad Iqbal License Manager for WooCommerce allows Blind SQL Injection. This issue affects License Manager for WooCommerce: from n/a through 3.0.12.	7.6	More Details
CVE-2025-23343	The NVIDIA NVDebug tool contains a vulnerability that may allow an actor to write files to restricted components. A successful exploit of this vulnerability may lead to information disclosure, denial of service, and data tampering.	7.6	More Details
CVE-2025-45805	In phpgurukul Doctor Appointment Management System 1.0, an authenticated doctor user can inject arbitrary JavaScript code into their profile name. This payload is subsequently rendered without proper sanitization, when a user visits the website and selects the doctor to book an appointment.	7.6	More Details
CVE-2025-55148	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure restricted settings.	7.6	More Details
CVE-2025-9959	Incomplete validation of dunder attributes allows an attacker to escape from the Local Python execution environment sandbox, enforced by smolagents. The attack requires a Prompt Injection in order to trick the agent to create malicious code.	7.6	More Details
CVE-2025-59008	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in PressTigers ZIP Code Based Content Protection allows SQL Injection. This issue affects ZIP Code Based Content Protection: from n/a through 1.0.0.	7.6	More Details
CVE-2025-58993	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeum Tutor LMS allows SQL Injection. This issue affects Tutor LMS: from n/a through 3.7.4.	7.6	More Details
CVE-2025-40796	A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), User Management Component (UMC) (All versions < V2.15.1.3). Affected products contain a out-of-bounds read vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to cause a denial of service condition.	7.5	More Details
CVE-2025-40797	A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), User Management Component (UMC) (All versions < V2.15.1.3). Affected products contain a out-of-bounds read vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to cause a denial of service condition.	7.5	More Details
CVE-2025-52288	Assertion failure in function ngap_build_downlink_nas_transport in file src/amf/ngap-build.c, the Access and Mobility Management Function (AMF) component, in Open5GS thru 2.7.5 allowing attackers to cause a denial of service or other unspecified impacts via repeated UE connect and disconnect message sequences.	7.5	More Details
CVE-2025-53805	Out-of-bounds read in Windows Internet Information Services allows an unauthorized attacker to deny service over a network.	7.5	More Details
CVE-2025-40798	A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), User Management Component (UMC) (All versions < V2.15.1.3). Affected products contain a out-of-bounds read vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to cause a denial of service condition.	7.5	More Details
CVE-2025-58296	Race condition vulnerability in the audio module. Impact: Successful exploitation of this vulnerability may affect function stability.	7.5	More Details
CVE-2025-47571	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in highwarden Super Store Finder. This issue affects Super Store Finder: from n/a through 6.9.7.	7.5	More Details
CVE-2025-48317	Path Traversal vulnerability in Stefan Keller WooCommerce Payment Gateway for Saferpay allows Path Traversal. This issue affects WooCommerce Payment Gateway for Saferpay: from n/a through 0.4.9.	7.5	More Details

CVE-2025-32689	Improper Validation of Specified Quantity in Input vulnerability in ThemesGrove WP SmartPay. This issue affects WP SmartPay: from n/a through 2.7.13.	7.5	More Details
CVE-2025-47695	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in solwin Blog Designer PRO. This issue affects Blog Designer PRO: from n/a through 3.4.7.	7.5	More Details
CVE-2025-54588	Envoy is an open source L7 proxy and communication bus designed for large modern service oriented architectures. Versions 1.34.0 through 1.34.4 and 1.35.0 contain a use-after-free (UAF) vulnerability in the DNS cache, causing abnormal process termination. The vulnerability is in Envoy's Dynamic Forward Proxy implementation, occurring when a completion callback for a DNS resolution triggers new DNS resolutions or removes existing pending resolutions. This condition may occur when the following conditions are met: dynamic Forwarding Filter is enabled, the `envoy.reloadable_features.dfp_cluster_resolves_hosts` runtime flag is enabled, and the Host header is modified between the Dynamic Forwarding Filter and Router filters. This issue is resolved in versions 1.34.5 and 1.35.1. To work around this issue, set the envoy.reloadable_features.dfp_cluster_resolves_hosts runtime flag to false.	7.5	More Details
CVE-2025-0280	A security vulnerability in HCL Compass can allow attacker to gain unauthorized database access.	7.5	More Details
CVE-2025-53694	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Sitecore Sitecore Experience Manager (XM), Sitecore Experience Platform (XP).This issue affects Sitecore Experience Manager (XM): from 9.2 through 10.4; Experience Platform (XP): from 9.2 through 10.4.	7.5	More Details
CVE-2025-55852	Tenda AC8 v16.03.34.06 is vulnerable to Buffer Overflow in the formWifiBasicSet function via the parameter security or security_5g.	7.5	More Details
CVE-2025-57889	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in RealMag777 InPost Gallery allows PHP Local File Inclusion. This issue affects InPost Gallery: from n/a through 2.1.4.5.	7.5	More Details
CVE-2025-52494	Adacore Ada Web Server (AWS) before 25.2 is vulnerable to a denial-of-service (DoS) condition due to improper handling of SSL handshakes during connection initialization. When a client initiates an HTTPS connection, the server performs the SSL handshake before assigning the connection to a processing slot. However, there is no specific timeout set for this phase, and the server uses the default socket timeout, which is effectively infinite. An attacker can exploit this by sending a malformed TLS ClientHello message with incorrect length values. This causes the server to wait indefinitely for data that never arrives, blocking the worker thread (Line) handling the connection. By opening multiple such connections, up to the server's maximum limit, the attacker can exhaust all available working threads, preventing the server from handling new, legitimate requests.	7.5	More Details
CVE-2025-58637	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in immonex immonex Kickstart allows PHP Local File Inclusion. This issue affects immonex Kickstart: from n/a through 1.11.6.	7.5	More Details
CVE-2024-21947	Improper input validation in the system management mode (SMM) could allow a privileged attacker to overwrite arbitrary memory potentially resulting in arbitrary code execution at the SMM level.	7.5	More Details
CVE-2025-55238	Dynamics 365 FastTrack Implementation Assets Information Disclosure Vulnerability	7.5	More Details
CVE-2025-58608	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in BuddyDev MediaPress allows PHP Local File Inclusion. This issue affects MediaPress: from n/a through 1.5.9.1.	7.5	More Details
CVE-2025-41664	A low-privileged remote attacker could gain unauthorized access to critical resources, such as firmware and certificates, due to improper permission handling during the runtime of services (e.g., FTP/SFTP). This access could allow the attacker to escalate privileges and modify firmware.	7.5	More Details
CVE-2025-58056	Netty is an asynchronous event-driven network application framework for development of maintainable high performance protocol servers and clients. In versions 4.1.124.Final, and 4.2.0.Alpha3 through 4.2.4.Final, Netty incorrectly accepts standalone newline characters (LF) as a chunk-size line terminator, regardless of a preceding carriage return (CR), instead of requiring CRLF per HTTP/1.1 standards. When combined with reverse proxies that parse LF differently (treating it as part of the chunk extension), attackers can craft requests that the proxy sees as one request but Netty processes as two, enabling request smuggling attacks. This is fixed in versions 4.1.125.Final and 4.2.5.Final.	7.5	More Details
CVE-2025-54919	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to execute code locally.	7.5	More Details
CVE-2025-	A SQL Injection vulnerability was found in phpgurukul Complaint Management System 2.0. The vulnerability is due to	7.5	More

57147	lack of input validation of multiple parameters including fullname, email, and contactno in user/registration.php.		Details
CVE-2025-36853	A vulnerability (CVE-2025-21172) exists in msdia140.dll due to integer overflow and heap-based overflow. Per CWE-122: Heap-based Buffer Overflow, a heap overflow condition is a buffer overflow, where the buffer that can be overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a routine such as malloc(). Per CWE-190: Integer Overflow or Wraparound, is when a product performs a calculation that can produce an integer overflow or wraparound when the logic assumes that the resulting value will always be larger than the original value. This occurs when an integer value is incremented to a value that is too large to store in the associated representation. When this occurs, the value may become a very small or negative number. NOTE: This CVE affects only End Of Life (EOL) software components. The vendor, Microsoft, has indicated there will be no future updates nor support provided upon inquiry.	7.5	More Details
CVE-2024-36354	Improper input validation for DIMM serial presence detect (SPD) metadata could allow an attacker with physical access, ring0 access on a system with a non-compliant DIMM, or control over the Root of Trust for BIOS update, to bypass SMM isolation potentially resulting in arbitrary code execution at the SMM level.	7.5	More Details
CVE-2025-36892	Denial of service	7.5	More Details
CVE-2025-36895	Information disclosure	7.5	More Details
CVE-2025-58358	Markdownify is a Model Context Protocol server for converting almost anything to Markdown. Versions below 0.0.2 contain a command injection vulnerability, caused by the unsanitized use of input parameters within a call to child_process.exec, enabling an attacker to inject arbitrary system commands. Successful exploitation can lead to remote code execution under the server process's privileges. The server constructs and executes shell commands using unvalidated user input directly within command-line strings. This introduces the possibility of shell metacharacter injection (|, >, &&, etc.). This issue is fixed in version 0.0.2.	7.5	More Details
CVE-2025-58362	Hono is a Web application framework that provides support for any JavaScript runtime. Versions 4.8.0 through 4.9.5 contain a flaw in the getPath utility function which could allow path confusion and potential bypass of proxy-level ACLs (e.g. Nginx location blocks). The original implementation relied on fixed character offsets when parsing request URLs. Under certain malformed absolute-form Request-URIs, this could lead to incorrect path extraction depending on the application and environment. If proxy ACLs are used to protect sensitive endpoints such as /admin, this flaw could have allowed unauthorized access. The confidentiality impact depends on what data is exposed: if sensitive administrative data is exposed, the impact may be high, otherwise it may be moderate. This issue is fixed in version 4.9.6.	7.5	More Details
CVE-2025-58057	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In netty-codec-compression versions 4.1.124.Final and below, and netty-codec versions 4.2.4.Final and below, when supplied with specially crafted input, BrotliDecoder and certain other decompression decoders will allocate a large number of reachable byte buffers, which can lead to denial of service. BrotliDecoder.decompress has no limit in how often it calls pull, decompressing data 64K bytes at a time. The buffers are saved in the output list, and remain reachable until OOM is hit. This is fixed in versions 4.1.125.Final of netty-codec and 4.2.5.Final of netty-codec-compression.	7.5	More Details
CVE-2014-125127	The mikecao/flight PHP framework in versions prior to v1.2 is vulnerable to Denial of Service (DoS) attacks due to eager loading of request bodies in the Request class constructor. The framework automatically reads the entire request body on every HTTP request, regardless of whether the application needs it. An attacker can exploit this by sending requests with large payloads, causing excessive memory consumption and potentially exhausting available server memory, leading to application crashes or service unavailability. The vulnerability was fixed in v1.2 by implementing lazy loading of request bodies.	7.5	More Details
CVE-2025-55243	Exposure of sensitive information to an unauthorized actor in Microsoft Office Plus allows an unauthorized attacker to perform spoofing over a network.	7.5	More Details
CVE-2025-40928	JSON::XS before version 4.04 for Perl has an integer buffer overflow causing a segfault when parsing crafted JSON, enabling denial-of-service attacks or other unspecified impact	7.5	More Details
CVE-2025-40930	JSON::SIMD before version 1.07 and earlier for Perl has an integer buffer overflow causing a segfault when parsing crafted JSON, enabling denial-of-service attacks or other unspecified impact.	7.5	More Details
CVE-2025-36894	In TBD of TBD, there is a possible DoS due to a missing null check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2025-41708	Due to an unsecure default configuration HTTP is used instead of HTTPS for the web interface. An unauthenticated attacker on the same network could exploit this to learn sensitive data during transmission.	7.4	More Details
CVE-			

2025-54103	Use after free in Windows Management Services allows an unauthorized attacker to elevate privileges locally.	7.4	More Details
CVE-2025-10030	A weakness has been identified in Campcodes Grocery Sales and Inventory System 1.0. This issue affects some unknown processing of the file /ajax.php?action=save_receiving. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-7366	The The REHub - Price Comparison, Multi Vendor Marketplace Wordpress Theme theme for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 19.9.7. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2025-10031	A security vulnerability has been detected in Campcodes Grocery Sales and Inventory System 1.0. Impacted is an unknown function of the file /ajax.php?action=delete_sales. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-10033	A vulnerability has been found in itsourcecode Online Discussion Forum 1.0. This affects an unknown function of the file /admin. Such manipulation of the argument Username leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-26443	In parseHtml of HtmlToSpannedParser.java, there is a possible way to install apps without allowing installation from unknown sources due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2025-10062	A vulnerability was determined in itsourcecode Student Information Management System 1.0. This affects an unknown part of the file /admin/login.php. Executing manipulation of the argument uname can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-48556	In multiple methods of NotificationChannel.java, there is a possible desynchronization from persistence due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2025-23258	NVIDIA DOCA contains a vulnerability in the collectx-dpeserver Debian package for arm64 that could allow an attacker with low privileges to escalate privileges. A successful exploit of this vulnerability might lead to escalation of privileges.	7.3	More Details
CVE-2025-48532	In markMediaAsFavorite of MediaProvider.java, there is a possible way to bypass the WRITE_EXTERNAL_STORAGE permission due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2025-23257	NVIDIA DOCA contains a vulnerability in the collectx-clxapidev Debian package that could allow an actor with low privileges to escalate privileges. A successful exploit of this vulnerability might lead to escalation of privileges.	7.3	More Details
CVE-2025-22441	In getContextForResourcesEnsuringCorrectCachedApkPaths of RemoteViews.java, there is a possible way to load arbitrary java code in a privileged context due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2025-10103	A weakness has been identified in code-projects Online Event Judging System 1.0. This impacts an unknown function of the file /home.php. Executing manipulation of the argument main_event can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-10068	A flaw has been found in itsourcecode Online Discussion Forum 1.0. This affects an unknown function of the file /admin/admin_forum/add_views.php. Executing manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-10092	A vulnerability was found in Jinher OA up to 1.2. This impacts an unknown function of the file /c6/Jhsoft.Web.projectmanage/TaskManage/AddTask.aspx/?Type=add of the component XML Handler. The manipulation results in xml external entity reference. The attack can be executed remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-10100	A vulnerability was detected in SourceCodester Simple Forum Discussion System 1.0. This impacts an unknown function of the file /admin_class.php?action=login. Performing manipulation 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.	7.3	More Details
CVE-2025-10104	A security vulnerability has been detected in code-projects Online Event Judging System 1.0. Affected is an unknown function of the file /review_search.php. The manipulation of the argument txtsearch leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-56630	FoxCMS v1.2.5 and before is vulnerable to SQL Injection via the column_model parameter in the app/admin/controller/Column.php file.	7.3	More Details
CVE-2025-	A vulnerability was found in Campcodes Online Loan Management System 1.0. This vulnerability affects unknown code of the file /ajax.php?action=delete_loan. Performing manipulation of the argument ID results in sql injection.	7.3	More Details

10108	The attack may be initiated remotely. The exploit has been made public and could be used.		
CVE-2025-10109	A vulnerability was determined in Campcodes Online Loan Management System 1.0. This issue affects some unknown processing of the file /ajax.php?action=delete_payment. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-10111	A security flaw has been discovered in itsourcecode Student Information Management System 1.0. The affected element is an unknown function of the file /admin/modules/instructor/index.php. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-10025	A vulnerability has been found in PHPGurukul Online Course Registration 3.1. Affected is an unknown function of the file /admin/semester.php. The manipulation of the argument semester leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-10112	A weakness has been identified in itsourcecode Student Information Management System 1.0. The impacted element is an unknown function of the file /admin/modules/department/index.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-10113	A security vulnerability has been detected in itsourcecode Student Information Management System 1.0. This affects an unknown function of the file /admin/modules/room/index.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-10091	A vulnerability has been found in Jinher OA up to 1.2. This affects an unknown function of the file /c6/Jhsoft.Web.projectmanage/ProjectManage/XmlHttp.aspx/?Type=add of the component XML Handler. The manipulation leads to xml external entity reference. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-10076	A weakness has been identified in SourceCodester Online Polling System 1.0. This affects an unknown function of the file /manage-profile.php. This manipulation of the argument email causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-10090	A flaw has been found in Jinher OA up to 1.2. The impacted element is an unknown function of the file /C6/Jhsoft.Web.departments/GetTreeDate.aspx. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-10114	A vulnerability was found in PHPGurukul Small CRM 4.0. Affected by this issue is some unknown functionality of the file /profile.php. The manipulation of the argument Name results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-10082	A vulnerability has been found in SourceCodester Online Polling System 1.0. Affected is an unknown function of the file /admin/manage-admins.php. Such manipulation of the argument email leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-10115	A vulnerability was determined in SiempreCMS up to 1.3.6. This affects an unknown part of the file user_search_ajax.php. This manipulation of the argument name/userName causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-10116	A vulnerability was identified in SiempreCMS up to 1.3.6. This vulnerability affects unknown code of the file /docs/admin/file_upload.php. Such manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-10102	A security flaw has been discovered in code-projects Online Event Judging System 1.0. This affects an unknown function of the file /index.php. Performing manipulation of the argument Username results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-10079	A flaw has been found in PHPGurukul Small CRM 4.0. Affected by this vulnerability is an unknown functionality of the file /get-quote.php. Executing manipulation of the argument Contact can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-10078	A vulnerability was detected in SourceCodester Online Polling System 1.0. Affected is an unknown function of the file /admin/candidates.php. Performing manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	7.3	More Details
CVE-2025-10077	A security vulnerability has been detected in SourceCodester Online Polling System 1.0. This impacts an unknown function of the file /registeracc.php. Such manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-10118	A security vulnerability has been detected in itsourcecode E-Logbook with Health Monitoring System for COVID-19 1.0. The affected element is an unknown function of the file /login.php. The manipulation of the argument Username leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-	In multiple locations, there is a possible one-time permission bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for	7.3	More

48547	exploitation.		Details
CVE-2025-9932	A flaw has been found in PHPGurukul Beauty Parlour Management System 1.1. Affected by this vulnerability is an unknown functionality of the file /admin/update-image.php. This manipulation of the argument lid causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-9924	A vulnerability has been found in projectworlds Travel Management System 1.0. This vulnerability affects unknown code of the file /enquiry.php. The manipulation of the argument t2 leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-5005	A vulnerability was detected in Shanghai Lingdang Information Technology Lingdang CRM up to 8.6.5.4. This affects an unknown function of the file crm/WeiXinApp/dingtalk/index_event.php. The manipulation of the argument corpurl results in server-side request forgery. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-36907	In draw_surface_image() of abl/android/lib/draw/draw.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege via USB fastboot, after a bootloader unlock, with no additional execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2025-9928	A security flaw has been discovered in projectworlds Travel Management System 1.0. The impacted element is an unknown function of the file /viewcategory.php. Performing manipulation of the argument t1 results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-9927	A vulnerability was identified in projectworlds Travel Management System 1.0. The affected element is an unknown function of the file /viewpackage.php. Such manipulation of the argument t1 leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-48548	In multiple functions of AppOpsControllerImpl.java, there is a possible way to record audio without displaying the privacy indicator due to a race condition. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2025-9930	A security vulnerability has been detected in 1000projects Beauty Parlour Management System 1.0. This impacts an unknown function of the file /admin/contact-us.php. The manipulation of the argument mobnumber leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-9933	A vulnerability has been found in PHPGurukul Beauty Parlour Management System 1.1. Affected by this issue is some unknown functionality of the file /admin/view-appointment.php. Such manipulation of the argument viewid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-9926	A vulnerability was determined in projectworlds Travel Management System 1.0. Impacted is an unknown function of the file /viewsubcategory.php. This manipulation of the argument t1 causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-9935	A vulnerability was determined in TOTOLINK N600R 4.3.0cu.7866_B20220506. This vulnerability affects the function sub_4159F8 of the file /web_cste/cgi-bin/cstecgi.cgi. Executing manipulation can lead to command injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-23344	The NVIDIA NVDebug tool contains a vulnerability that may allow an actor to run code on the platform host as a non-privileged user. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure and data tampering.	7.3	More Details
CVE-2025-9925	A vulnerability was found in projectworlds Travel Management System 1.0. This issue affects some unknown processing of the file /detail.php. The manipulation of the argument pid results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-10164	A security flaw has been discovered in lmsys sglang 0.4.6. Affected by this vulnerability is the function main of the file /update_weights_from_tensor. The manipulation of the argument serialized_named_tensors results in deserialization. The attack can be launched 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.	7.3	More Details
CVE-2025-9919	A vulnerability was identified in 1000projects Beauty Parlour Management System 1.0. This affects an unknown function of the file /admin/bwdates-reports-details.php. The manipulation of the argument fromdate/todate leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2024-13068	Origin Validation Error vulnerability in Akinsoft LimonDesk allows Forceful Browsing.This issue affects LimonDesk: from s1.02.14 before v1.02.17.	7.3	More Details
CVE-2025-10123	A vulnerability was determined in D-Link DIR-823X up to 250416. Affected by this vulnerability is the function sub_415028 of the file /goform/set_static_leases. Executing manipulation of the argument Hostname can lead to command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-9848	A security vulnerability has been detected in ScriptAndTools Real Estate Management System 1.0. The affected element is an unknown function of the file /admin/userlist.php. Such manipulation leads to execution after redirect. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details

CVE-2025-54911	Use after free in Windows BitLocker allows an authorized attacker to elevate privileges locally.	7.3	More Details
CVE-2025-54116	Improper access control in Windows MultiPoint Services allows an authorized attacker to elevate privileges locally.	7.3	More Details
CVE-2025-55236	Time-of-check time-of-use (toctou) race condition in Graphics Kernel allows an authorized attacker to execute code locally.	7.3	More Details
CVE-2025-9517	The atec Debug plugin for WordPress is vulnerable to remote code execution in all versions up to, and including, 1.2.22 via the 'custom_log' parameter. This is due to insufficient sanitization when saving the custom log path. This makes it possible for authenticated attackers, with Administrator-level access and above, to execute code on the server.	7.2	More Details
CVE-2025-6085	The Make Connector plugin for WordPress is vulnerable to arbitrary file uploads due to misconfigured file type validation in the 'upload_media' function in all versions up to, and including, 1.5.10. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2025-58642	Deserialization of Untrusted Data vulnerability in eniturechnology LTL Freight Quotes – Day & Ross Edition allows Object Injection. This issue affects LTL Freight Quotes – Day & Ross Edition: from n/a through 2.1.11.	7.2	More Details
CVE-2025-9515	The Multi Step Form plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation via the import functionality in all versions up to, and including, 1.7.25. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2023-31325	Improper isolation of shared resources on System-on-a-chip (SOC) could a privileged attacker to tamper with the contents of the PSP reserved DRAM region potentially resulting in loss of confidentiality and integrity.	7.2	More Details
CVE-2025-58179	Astro is a web framework for content-driven websites. Versions 11.0.3 through 12.6.5 are vulnerable to SSRF when using Astro's Cloudflare adapter. When configured with output: 'server' while using the default imageService: 'compile', the generated image optimization endpoint doesn't check the URLs it receives, allowing content from unauthorized third-party domains to be served. a A bug in impacted versions of the @astrojs/cloudflare adapter for deployment on Cloudflare’s infrastructure, allows an attacker to bypass the third-party domain restrictions and serve any content from the vulnerable origin. This issue is fixed in version 12.6.6.	7.2	More Details
CVE-2025-58643	Deserialization of Untrusted Data vulnerability in eniturechnology LTL Freight Quotes – Daylight Edition allows Object Injection. This issue affects LTL Freight Quotes – Daylight Edition: from n/a through 2.2.7.	7.2	More Details
CVE-2025-58780	index.em7 in ScienceLogic SL1 before 12.1.1 allows SQL Injection via a parameter in a request. NOTE: this is disputed by the Supplier because it "inaccurately describes the vulnerability."	7.2	More Details
CVE-2025-57150	phpgurukul Complaint Management System in PHP 2.0 is vulnerable to Cross Site Scripting (XSS) in admin/subcategory.php via the categoryName parameter.	7.2	More Details
CVE-2025-58839	Deserialization of Untrusted Data vulnerability in aThemeArt Translations eDS Responsive Menu allows Object Injection. This issue affects eDS Responsive Menu: from n/a through 1.2.	7.2	More Details
CVE-2025-0032	Improper cleanup in AMD CPU microcode patch loading could allow an attacker with local administrator privilege to load malicious CPU microcode, potentially resulting in loss of integrity of x86 instruction execution.	7.2	More Details
CVE-2025-9518	The atec Debug plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation on the 'debug_path' parameter in all versions up to, and including, 1.2.22. This makes it possible for authenticated attackers, with Administrator-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	7.2	More Details
CVE-2025-58815	Deserialization of Untrusted Data vulnerability in Rubel Miah Aitasi Coming Soon allows Object Injection. This issue affects Aitasi Coming Soon: from n/a through 2.0.2.	7.2	More Details
CVE-2025-57263	An authenticated SQL injection vulnerability in VX Guestbook 1.07 allows attackers with admin access to inject malicious SQL payloads via the "word" POST parameter in the words.php admin panel.	7.2	More Details
CVE-2025-	ECOVACS vacuum robot base stations do not validate firmware updates, so malicious over-the-air updates can be	7.2	More

30199	sent to base station via insecure connection between robot and base station.		Details
CVE-2025-9519	The Easy Timer plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.2.1 via the plugin's shortcodes. This is due to insufficient restriction of shortcode attributes. This makes it possible for authenticated attackers, with Editor-level access and above, to execute code on the server.	7.2	More Details
CVE-2025-58644	Deserialization of Untrusted Data vulnerability in eniturechnology LTL Freight Quotes - TQL Edition allows Object Injection. This issue affects LTL Freight Quotes - TQL Edition: from n/a through 1.2.6.	7.2	More Details
CVE-2025-49430	Server-Side Request Forgery (SSRF) vulnerability in FWDesign Ultimate Video Player allows Server Side Request Forgery. This issue affects Ultimate Video Player: from n/a through 10.1.	7.2	More Details
CVE-2025-58859	Cross-Site Request Forgery (CSRF) vulnerability in David Merinas Add to Feedly allows Stored XSS. This issue affects Add to Feedly: from n/a through 1.2.11.	7.1	More Details
CVE-2025-58854	Cross-Site Request Forgery (CSRF) vulnerability in Samer Bechara Ultimate AJAX Login allows Reflected XSS. This issue affects Ultimate AJAX Login: from n/a through 1.2.1.	7.1	More Details
CVE-2025-58807	Cross-Site Request Forgery (CSRF) vulnerability in Dsingh Purge Varnish Cache allows Stored XSS. This issue affects Purge Varnish Cache: from n/a through 2.6.	7.1	More Details
CVE-2025-58063	CoreDNS is a DNS server that chains plugins. Starting in version 1.2.0 and prior to version 1.12.4, the CoreDNS etcd plugin contains a TTL confusion vulnerability where lease IDs are incorrectly used as TTL values, enabling DNS cache pinning attacks. This effectively creates a DoS condition for DNS resolution of affected services. The `TTL()` function in `plugin/etcd/etcd.go` incorrectly casts etcd lease IDs (64-bit integers) to uint32 and uses them as TTL values. Large lease IDs become very large TTLs when cast to uint32. This enables cache pinning attacks. Version 1.12.4 contains a fix for the issue.	7.1	More Details
CVE-2025-58857	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in KaizenCoders Table of content allows Stored XSS. This issue affects Table of content: from n/a through 1.5.3.1.	7.1	More Details
CVE-2025-58809	Cross-Site Request Forgery (CSRF) vulnerability in Nick Ciske To Lead For Salesforce allows Reflected XSS. This issue affects To Lead For Salesforce: from n/a through 2.7.3.9.	7.1	More Details
CVE-2025-57833	An issue was discovered in Django 4.2 before 4.2.24, 5.1 before 5.1.12, and 5.2 before 5.2.6. FilteredRelation is subject to SQL injection in column aliases, using a suitably crafted dictionary, with dictionary expansion, as the **kwargs passed QuerySet.annotate() or QuerySet.alias().	7.1	More Details
CVE-2025-58855	Improper Neutralization of Formula Elements in a CSV File vulnerability in Denis V (Artprima) AP HoneyPot WordPress Plugin allows Reflected XSS. This issue affects AP HoneyPot WordPress Plugin: from n/a through 1.4.	7.1	More Details
CVE-2025-58848	Cross-Site Request Forgery (CSRF) vulnerability in aakash1911 WP likes allows Reflected XSS. This issue affects WP likes: from n/a through 3.1.1.	7.1	More Details
CVE-2025-58991	Cross-Site Request Forgery (CSRF) vulnerability in Cristiano Zanca WooCommerce Booking Bundle Hours allows Stored XSS. This issue affects WooCommerce Booking Bundle Hours: from n/a through 0.7.4.	7.1	More Details
CVE-2025-58853	Cross-Site Request Forgery (CSRF) vulnerability in OTWthemes Popping Sidebars and Widgets Light allows Reflected XSS. This issue affects Popping Sidebars and Widgets Light: from n/a through 1.27.	7.1	More Details
CVE-2025-58843	Cross-Site Request Forgery (CSRF) vulnerability in David Merinas Auto Last Youtube Video allows Stored XSS. This issue affects Auto Last Youtube Video: from n/a through 1.0.7.	7.1	More Details
CVE-2025-53307	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brent Jett Assistant allows Reflected XSS. This issue affects Assistant: from n/a through 1.5.2.	7.1	More Details
CVE-2025-58861	Cross-Site Request Forgery (CSRF) vulnerability in WP Corner Quick Event Calendar allows Stored XSS. This issue affects Quick Event Calendar: from n/a through 1.4.9.	7.1	More Details
CVE-2025-47570	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in villatheme WooCommerce Photo Reviews. This issue affects WooCommerce Photo Reviews: from n/a through 1.3.13.	7.1	More Details

CVE-2025-58765	wabac.js provides a full web archive replay system, or 'wayback machine', using Service Workers. A Reflected Cross-Site Scripting (XSS) vulnerability exists in the 404 error handling logic of wabac.js v2.23.10 and below. The parameter `requestURL` (derived from the original request target) is directly embedded into an inline `<script>` block without sanitization or escaping. This allows an attacker to craft a malicious URL that executes arbitrary JavaScript in the victim’s browser. The scope may be limited by CORS policies, depending on the situation in which wabac.js is used. The vulnerability is fixed in wabac.js v2.23.11.	7.1	More Details
CVE-2025-48104	Cross-Site Request Forgery (CSRF) vulnerability in ericzane Floating Window Music Player allows Stored XSS. This issue affects Floating Window Music Player: from n/a through 3.4.2.	7.1	More Details
CVE-2025-58844	Cross-Site Request Forgery (CSRF) vulnerability in Subhash Kumar Database to Excel allows Stored XSS. This issue affects Database to Excel: from n/a through 1.0.	7.1	More Details
CVE-2025-47694	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in solwin Blog Designer PRO. This issue affects Blog Designer PRO: from n/a through 3.4.7.	7.1	More Details
CVE-2025-48537	In multiple locations, there is a possible way to persistently DoS the device due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	7.1	More Details
CVE-2025-58845	Cross-Site Request Forgery (CSRF) vulnerability in ChrisHurst Bulk Watermark allows Reflected XSS. This issue affects Bulk Watermark: from n/a through 1.6.10.	7.1	More Details
CVE-2025-58846	Cross-Site Request Forgery (CSRF) vulnerability in Dejan Markovic WordPress Buffer – HYPESocial. Social Media Auto Post, Social Media Auto Publish and Schedule allows Reflected XSS. This issue affects WordPress Buffer – HYPESocial. Social Media Auto Post, Social Media Auto Publish and Schedule: from n/a through 2020.1.0.	7.1	More Details
CVE-2025-58847	Cross-Site Request Forgery (CSRF) vulnerability in Yaidier WN Flipbox Pro allows Reflected XSS. This issue affects WN Flipbox Pro: from n/a through 2.1.	7.1	More Details
CVE-2025-54905	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	7.1	More Details
CVE-2025-58849	Cross-Site Request Forgery (CSRF) vulnerability in Deepak S Hide Real Download Path allows Stored XSS. This issue affects Hide Real Download Path: from n/a through 1.6.	7.1	More Details
CVE-2025-58806	Cross-Site Request Forgery (CSRF) vulnerability in imjoehaines WordPress Error Monitoring by Bugsnag allows Stored XSS. This issue affects WordPress Error Monitoring by Bugsnag: from n/a through 1.6.3.	7.1	More Details
CVE-2025-58852	Cross-Site Request Forgery (CSRF) vulnerability in Mark O'Donnell MSTW League Manager allows Stored XSS. This issue affects MSTW League Manager: from n/a through 2.10.	7.1	More Details
CVE-2025-58860	Cross-Site Request Forgery (CSRF) vulnerability in KaizenCoders Enable Latex allows Stored XSS. This issue affects Enable Latex: from n/a through 1.2.16.	7.1	More Details
CVE-2025-54114	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Connected Devices Platform Service allows an authorized attacker to deny service locally.	7.0	More Details
CVE-2025-55223	Concurrent execution using shared resource with improper synchronization ('race condition') in Graphics Kernel allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-54115	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-53807	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-54112	Use after free in Microsoft Virtual Hard Drive allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-	Concurrent execution using shared resource with improper synchronization ('race condition') in Capability Access		More

2025-54108	Management Service (camsvc) allows an authorized attacker to elevate privileges locally.	7.0	Details
CVE-2025-54105	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-53802	Use after free in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-54099	Stack-based buffer overflow in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-48533	In multiple locations, there is a possible way to use apps linked from a context menu of a lockscreen app due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.0	More Details
CVE-2025-49734	Improper restriction of communication channel to intended endpoints in Windows PowerShell allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-54093	Time-of-check time-of-use (toctou) race condition in Windows TCP/IP allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-58351	Outline is a service that allows for collaborative documentation. In versions 0.72.0 through 0.83.0, Outline introduced a feature which facilitates local file system storage capabilities as an optional file storage strategy. This feature allowed a CSP bypass as well as a ContentType bypass that might facilitate further attacks. In the case of self-hosting and using Outline FILE_STORAGE=local on the same domain as the Outline application, a malicious payload can be uploaded as a file attachment and bypass those CSP restrictions, allowing script execution within the context of another user. This is fixed in version 0.84.0.	6.8	More Details
CVE-2023-21472	Improper input validation with Exynos Fastboot USB Interface prior to SMR Apr-2023 Release 1 allows a physical attacker to execute arbitrary code in bootloader.	6.8	More Details
CVE-2024-13063	Authorization Bypass Through User-Controlled Key vulnerability in Akinsoft MyRezzta allows Forceful Browsing.This issue affects MyRezzta: from s2.02.02 before v2.05.01.	6.8	More Details
CVE-2025-55139	SSRF in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with admin privileges to enumerate internal services.	6.8	More Details
CVE-2025-58276	Permission verification vulnerability in the home screen module Impact: Successful exploitation of this vulnerability may affect availability.	6.8	More Details
CVE-2023-21473	Improper input validation with Exynos Fastboot USB Interface prior to SMR Apr-2023 Release 1 allows a physical attacker to execute arbitrary code in bootloader.	6.8	More Details
CVE-2025-21031	Improper access control in ImsService prior to SMR Sep-2025 Release 1 allows local attackers to use the privileged APIs.	6.8	More Details
CVE-2024-45325	An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerabilities [CWE-78] in Fortinet FortiDDoS-F version 7.0.0 through 7.02 and before 6.6.3 may allow a privileged attacker to execute unauthorized code or commands via crafted CLI requests.	6.7	More Details
CVE-2025-54915	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	6.7	More Details
CVE-2025-55226	Concurrent execution using shared resource with improper synchronization ('race condition') in Graphics Kernel allows an authorized attacker to execute code locally.	6.7	More Details
CVE-2025-43722	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an improper privilege management vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.	6.7	More Details
CVE-2025-53808	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	6.7	More Details

CVE-2025-54109	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	6.7	More Details
CVE-2025-53810	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	6.7	More Details
CVE-2025-36908	In lwis_top_register_io of lwis_device_top.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2025-36902	In syna_cdev_ioctl_store_pid() of syna_tcm2_sysfs.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2025-36900	In lwis_test_register_io of lwis_device_test.c, there is a possible OOB Write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2025-54094	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	6.7	More Details
CVE-2025-54104	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	6.7	More Details
CVE-2025-58598	Insertion of Sensitive Information Into Debugging Code vulnerability in Klarna Klarna Order Management for WooCommerce allows Retrieve Embedded Sensitive Data. This issue affects Klarna Order Management for WooCommerce: from n/a through 1.9.8.	6.6	More Details
CVE-2025-58131	Race condition in the Zoom Workplace VDI Plugin macOS Universal installer for VMware Horizon before version 6.4.10 (or before 6.2.15 and 6.3.12 in their respective tracks) may allow an authenticated user to conduct a disclosure of information via network access.	6.6	More Details
CVE-2025-58850	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in marcshowpass Showpass WordPress Extension allows Stored XSS. This issue affects Showpass WordPress Extension: from n/a through 4.0.3.	6.5	More Details
CVE-2025-58851	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DigitalCourt Boxed Content allows Stored XSS. This issue affects Boxed Content: from n/a through 1.0.	6.5	More Details
CVE-2025-58842	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in givecloud Donation Forms WP by Givecloud allows Stored XSS. This issue affects Donation Forms WP by Givecloud: from n/a through 1.0.9.	6.5	More Details
CVE-2025-58856	Cross-Site Request Forgery (CSRF) vulnerability in ablancodev Woocommerce Notify Updated Product allows Stored XSS. This issue affects Woocommerce Notify Updated Product: from n/a through 1.6.	6.5	More Details
CVE-2025-58862	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in George Sexton WordPress Events Calendar Plugin – connectDaily allows Stored XSS. This issue affects WordPress Events Calendar Plugin – connectDaily: from n/a through 1.5.3.	6.5	More Details
CVE-2025-58863	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SdeWijs Zoomify embed for WP allows Stored XSS. This issue affects Zoomify embed for WP: from n/a through 1.5.2.	6.5	More Details
CVE-2025-58858	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBean WPB Image Widget allows Stored XSS. This issue affects WPB Image Widget: from n/a through 1.1.	6.5	More Details
CVE-2025-54744	Missing Authorization vulnerability in Stylemix MasterStudy LMS allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects MasterStudy LMS: from n/a through 3.6.15.	6.5	More Details
CVE-2025-10003	The UsersWP – Front-end login form, User Registration, User Profile & Members Directory plugin for WordPress plugin for WordPress is vulnerable to time-based SQL Injection via the ‘upload_file_remove’ function and 'htmlvar' parameter in all versions up to, and including, 1.2.44 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.	6.5	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ram Ratan		More

2025-58814	Maurya Stagtools allows Stored XSS. This issue affects Stagtools: from n/a through 2.3.8.	6.5	Details
CVE-2025-55242	Exposure of sensitive information to an unauthorized actor in Xbox allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2025-10061	An authorized user can cause a crash in the MongoDB Server through a specially crafted $group query. This vulnerability is related to the incorrect handling of certain accumulator functions when additional parameters are specified within the $group operation. This vulnerability could lead to denial of service if triggered repeatedly. This issue affects MongoDB Server v6.0 versions prior to 6.0.25, MongoDB Server v7.0 versions prior to 7.0.22, MongoDB Server v8.0 versions prior to 8.0.12 and MongoDB Server v8.1 versions prior to 8.1.2	6.5	More Details
CVE-2025-58808	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Babar prettyPhoto allows Stored XSS. This issue affects prettyPhoto: from n/a through 1.2.4.	6.5	More Details
CVE-2025-10060	MongoDB Server may allow upsert operations retried within a transaction to violate unique index constraints, potentially causing an invariant failure and server crash during commit. This issue may be triggered by improper WriteUnitOfWork state management. This issue affects MongoDB Server v6.0 versions prior to 6.0.25, MongoDB Server v7.0 versions prior to 7.0.22 and MongoDB Server v8.0 versions prior to 8.0.12	6.5	More Details
CVE-2025-10059	An improper setting of the lsid field on any sharded query can cause a crash in MongoDB routers. This issue occurs when a generic argument (lsid) is provided in a case when it is not applicable. This affects MongoDB Server v6.0 versions prior to 6.0.x, MongoDB Server v7.0 versions prior to 7.0.18 and MongoDB Server v8.0 versions prior to 8.0.6.	6.5	More Details
CVE-2025-58887	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Course Finder | andré martin - it solutions & research UG Course Booking Platform allows Stored XSS. This issue affects Course Booking Platform: from n/a through 1.0.0.	6.5	More Details
CVE-2025-7445	Kubernetes secrets-store-sync-controller in versions before 0.0.2 discloses service account tokens in logs.	6.5	More Details
CVE-2025-9260	The Fluent Forms – Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder plugin for WordPress is vulnerable to PHP Object Injection in versions 5.1.16 to 6.1.1 via deserialization of untrusted input in the parseUserProperties function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject a PHP Object. The additional presence of a POP chain allows attackers to read arbitrary files. If allow_url_include is enabled on the server, remote code execution is possible. While the vendor patched this issue in version 6.1.0, the patch caused a fatal error in the vulnerable code, due to a missing class import, so we consider 6.1.2 to be the most complete and best patched version	6.5	More Details
CVE-2025-48103	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mulscully Today's Date Inserter allows Stored XSS. This issue affects Today's Date Inserter: from n/a through 1.2.1.	6.5	More Details
CVE-2025-58796	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dudaster Elementor Element Condition allows Stored XSS. This issue affects Elementor Element Condition: from n/a through 1.0.5.	6.5	More Details
CVE-2025-48105	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vincent Boiardt Easy Flash Embed allows Stored XSS. This issue affects Easy Flash Embed: from n/a through 1.0.	6.5	More Details
CVE-2025-58793	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBean WPB Elementor Addons allows Stored XSS. This issue affects WPB Elementor Addons: from n/a through 1.6.	6.5	More Details
CVE-2025-58790	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPKube Kiwi allows Stored XSS. This issue affects Kiwi: from n/a through 2.1.8.	6.5	More Details
CVE-2025-58787	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themifyme Themify Popup allows Stored XSS. This issue affects Themify Popup: from n/a through 1.4.4.	6.5	More Details
CVE-2025-58786	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VW THEMES Ibtana – Ecommerce Product Addons allows DOM-Based XSS. This issue affects Ibtana – Ecommerce Product Addons: from n/a through 0.4.7.4.	6.5	More Details
CVE-2025-53571	Missing Authorization vulnerability in VillaTheme HAPPY allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects HAPPY: from n/a through 1.0.6.	6.5	More Details
CVE-2025-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in arisoft ARI Fancy Lightbox allows Stored XSS. This issue affects ARI Fancy Lightbox: from n/a through 1.4.0.	6.5	More Details

58784			
CVE-2025-58812	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PriceListo Best Restaurant Menu by PriceListo allows Stored XSS. This issue affects Best Restaurant Menu by PriceListo: from n/a through 1.4.3.	6.5	More Details
CVE-2025-58882	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in w1zzard Simple Text Slider allows Stored XSS. This issue affects Simple Text Slider: from n/a through 1.0.5.	6.5	More Details
CVE-2025-58868	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Simasicher SimaCookie allows Stored XSS. This issue affects SimaCookie: from n/a through 1.3.2.	6.5	More Details
CVE-2025-58878	Cross-Site Request Forgery (CSRF) vulnerability in usamafarooq Woocommerce Gifts Product allows Cross Site Request Forgery. This issue affects Woocommerce Gifts Product: from n/a through 1.0.0.	6.5	More Details
CVE-2025-58840	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ibnul H. Custom Team Manager allows Stored XSS. This issue affects Custom Team Manager: from n/a through 2.4.2.	6.5	More Details
CVE-2025-58838	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zakir Smooth Accordion allows Stored XSS. This issue affects Smooth Accordion: from n/a through 2.1.	6.5	More Details
CVE-2025-58837	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shiful H SS Font Awesome Icon allows Stored XSS. This issue affects SS Font Awesome Icon: from n/a through 4.1.3.	6.5	More Details
CVE-2025-58836	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tikolan FW Anker allows Stored XSS. This issue affects FW Anker: from n/a through 1.2.6.	6.5	More Details
CVE-2025-58869	Cross-Site Request Forgery (CSRF) vulnerability in Simasicher SimaCookie allows Stored XSS. This issue affects SimaCookie: from n/a through 1.3.2.	6.5	More Details
CVE-2025-58834	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gugu short.io allows DOM-Based XSS. This issue affects short.io: from n/a through 2.4.0.	6.5	More Details
CVE-2025-58870	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DeBAAT WP-GraphViz allows DOM-Based XSS. This issue affects WP-GraphViz: from n/a through 1.5.1.	6.5	More Details
CVE-2025-58871	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Luis Rock Master Paper Collapse Toggle allows Stored XSS. This issue affects Master Paper Collapse Toggle: from n/a through 1.1.	6.5	More Details
CVE-2025-58830	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in snagysandor Parallax Scrolling Enllax.js allows Stored XSS. This issue affects Parallax Scrolling Enllax.js: from n/a through 0.0.6.	6.5	More Details
CVE-2025-58872	Insertion of Sensitive Information Into Sent Data vulnerability in premiumbizthemes Simple Price Calculator allows Retrieve Embedded Sensitive Data. This issue affects Simple Price Calculator: from n/a through 1.3.	6.5	More Details
CVE-2025-58828	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codemstory allows Stored XSS. This issue affects : from n/a through 1.2.1.	6.5	More Details
CVE-2025-58826	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Eric Mann WP Publication Archive allows Stored XSS. This issue affects WP Publication Archive : from n/a through 3.0.1.	6.5	More Details
CVE-2025-58874	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in josepsitjar StoryMap allows DOM-Based XSS. This issue affects StoryMap: from n/a through 2.1.	6.5	More Details
CVE-2025-58875	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sudar Muthu WP Github Gist allows Stored XSS. This issue affects WP Github Gist: from n/a through 0.5.	6.5	More Details
CVE-2025-58823	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in The African Boss Get Cash allows Stored XSS. This issue affects Get Cash: from n/a through 3.2.2.	6.5	More Details

CVE-2025-58822	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mndpsingh287 WP Mail allows DOM-Based XSS. This issue affects WP Mail: from n/a through 1.3.	6.5	More Details
CVE-2025-58876	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ali Aghdam Aparat Video Shortcode allows Stored XSS. This issue affects Aparat Video Shortcode: from n/a through 0.2.4.	6.5	More Details
CVE-2025-58880	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in reubenthiessen Translate This gTranslate Shortcode allows Stored XSS. This issue affects Translate This gTranslate Shortcode: from n/a through 1.0.	6.5	More Details
CVE-2025-25048	IBM Jazz Foundation 7.0.2 through 7.0.2 iFix033, 7.0.3 through 7.0.3 iFix012, and 7.1.0 through 7.1.0 iFix002 could allow an authenticated user to upload files to the system due to improper neutralization of sequences that can resolve to a restricted directory.	6.5	More Details
CVE-2025-53796	Buffer over-read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2025-58623	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bohemia Plugins Event Feed for Eventbrite allows DOM-Based XSS. This issue affects Event Feed for Eventbrite: from n/a through 1.3.2.	6.5	More Details
CVE-2025-58626	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RumbleTalk RumbleTalk Live Group Chat allows Stored XSS. This issue affects RumbleTalk Live Group Chat: from n/a through 6.3.5.	6.5	More Details
CVE-2025-58632	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dadevarzan Dadevarzan WordPress Common allows Stored XSS. This issue affects Dadevarzan WordPress Common: from n/a through 2.2.2.	6.5	More Details
CVE-2025-58633	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Deetronix Booking Ultra Pro allows Stored XSS. This issue affects Booking Ultra Pro: from n/a through 1.1.21.	6.5	More Details
CVE-2025-58640	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MatrixAddons Document Engine allows Stored XSS. This issue affects Document Engine: from n/a through 1.2.	6.5	More Details
CVE-2025-54249	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to manipulate server-side requests and bypass security controls allowing unauthorized read access.	6.5	More Details
CVE-2025-54247	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access.	6.5	More Details
CVE-2025-54246	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access.	6.5	More Details
CVE-2025-54097	Out-of-bounds read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2025-54096	Out-of-bounds read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2025-8268	The AI Engine plugin for WordPress is vulnerable to unauthorized access and loss of data due to a missing capability check on the rest_list and delete_files functions in all versions up to, and including, 2.9.5. This makes it possible for unauthenticated attackers to list and delete files uploaded by other users.	6.5	More Details
CVE-2025-54095	Out-of-bounds read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2024-56189	In SAEMM_DiscloseMsId of SAEMM_RadioMessageCodec.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure post authentication with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2025-53809	Improper input validation in Windows Local Security Authority Subsystem Service (LSASS) allows an authorized attacker to deny service over a network.	6.5	More Details
CVE-	Buffer over-read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose		More

2025-53806	information over a network.	6.5	Details
CVE-2025-53798	Buffer over-read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2025-53797	Buffer over-read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2025-47997	Concurrent execution using shared resource with improper synchronization ('race condition') in SQL Server allows an authorized attacker to disclose information over a network.	6.5	More Details
CVE-2025-41035	A problem has been discovered in appRain CMF 4.0.5. An authenticated Path Traversal vulnerability in /apprain/common/download/ allows remote users to bypass the intended SecurityManager restrictions and download any file if they have adequate permissions outside the document root configured on the server via the base64 path after /download/.	6.5	More Details
CVE-2025-39541	Missing Authorization vulnerability in Roland Murg WP Simple Booking Calendar. This issue affects WP Simple Booking Calendar: from n/a through 2.0.13.	6.5	More Details
CVE-2025-58624	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in falselight Exchange Rates allows Stored XSS. This issue affects Exchange Rates: from n/a through 1.2.5.	6.5	More Details
CVE-2025-58621	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Amuse Labs PuzzleMe for WordPress allows Stored XSS. This issue affects PuzzleMe for WordPress: from n/a through 1.2.0.	6.5	More Details
CVE-2025-58867	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Remi Corson Easy Download Media Counter allows Stored XSS. This issue affects Easy Download Media Counter: from n/a through 1.2.	6.5	More Details
CVE-2025-58620	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in add-ons.org PDF for WPForms allows Stored XSS. This issue affects PDF for WPForms: from n/a through 6.2.1.	6.5	More Details
CVE-2025-49458	Buffer overflow in certain Zoom Workplace Clients may allow an authenticated user to conduct a denial of service via network access.	6.5	More Details
CVE-2025-55053	CWE-328: Use of Weak Hash	6.5	More Details
CVE-2025-58990	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasTech ShopLentor allows Stored XSS. This issue affects ShopLentor: from n/a through 3.2.0.	6.5	More Details
CVE-2025-58989	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in silverplugins217 Dynamic Text Field For Contact Form 7 allows Stored XSS. This issue affects Dynamic Text Field For Contact Form 7: from n/a through 1.0.	6.5	More Details
CVE-2025-58988	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Joe Dolson My Tickets allows Stored XSS. This issue affects My Tickets: from n/a through 2.0.22.	6.5	More Details
CVE-2025-58987	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AntoineH Football Pool allows Stored XSS. This issue affects Football Pool: from n/a through 2.12.6.	6.5	More Details
CVE-2025-58985	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Additional Custom Product Tabs for WooCommerce allows Stored XSS. This issue affects Additional Custom Product Tabs for WooCommerce: from n/a through 1.7.3.	6.5	More Details
CVE-2025-57149	phpgurukul Complaint Management System 2.0 is vulnerable to SQL Injection in /complaint-details.php via the cid parameter.	6.5	More Details
CVE-2025-55225	Out-of-bounds read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeisle Orbit		More

2025-58593	Fox by ThemeIsle allows Stored XSS. This issue affects Orbit Fox by ThemeIsle: from n/a through 3.0.0.	6.5	Details
CVE-2025-58602	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in IfSo Dynamic Content If-So Dynamic Content Personalization allows Stored XSS. This issue affects If-So Dynamic Content Personalization: from n/a through 1.9.4.	6.5	More Details
CVE-2025-58605	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Delicious WP Delicious allows Stored XSS. This issue affects WP Delicious: from n/a through 1.8.7.	6.5	More Details
CVE-2025-58607	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GDPR Info Cookie Notice & Consent Banner for GDPR & CCPA Compliance allows Stored XSS. This issue affects Cookie Notice & Consent Banner for GDPR & CCPA Compliance: from n/a through 1.7.11.	6.5	More Details
CVE-2025-58609	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Iulia Cazan Latest Post Shortcode allows Stored XSS. This issue affects Latest Post Shortcode: from n/a through 14.0.3.	6.5	More Details
CVE-2025-58610	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Chill Gallery PhotoBlocks allows Stored XSS. This issue affects Gallery PhotoBlocks: from n/a through 1.3.1.	6.5	More Details
CVE-2025-58612	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Property Hive PropertyHive allows Stored XSS. This issue affects PropertyHive: from n/a through 2.1.5.	6.5	More Details
CVE-2025-58614	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jamel.Z Tooltipy allows Stored XSS. This issue affects Tooltipy: from n/a through 5.5.6.	6.5	More Details
CVE-2025-58616	Missing Authorization vulnerability in Frisbii Frisbii Pay allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Frisbii Pay: from n/a through 1.8.2.1.	6.5	More Details
CVE-2025-58618	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jonathan Jernigan Pie Calendar allows DOM-Based XSS. This issue affects Pie Calendar: from n/a through 1.2.8.	6.5	More Details
CVE-2025-8889	The Compress & Upload WordPress plugin before 1.0.5 does not properly validate uploaded files, allowing high privilege users such as admin to upload arbitrary files on the server even when they should not be allowed to (for example in multisite setup)	6.5	More Details
CVE-2025-58864	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in iamroody 金数据 allows Stored XSS. This issue affects 金数据: from n/a through 1.0.	6.5	More Details
CVE-2025-42930	SAP Business Planning and Consolidation allows an authenticated standard user to call a function module by crafting specific parameters that causes a loop, consuming excessive resources and resulting in system unavailability. This leads to high impact on the availability of the application, there is no impact on confidentiality or integrity.	6.5	More Details
CVE-2025-42917	SAP HCM Approve Timesheets Fiori 2.0 application does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This issue has a significant impact on the application's integrity, while confidentiality and availability remain unaffected.	6.5	More Details
CVE-2025-58782	Deserialization of Untrusted Data vulnerability in Apache Jackrabbit Core and Apache Jackrabbit JCR Commons. This issue affects Apache Jackrabbit Core: from 1.0.0 through 2.22.1; Apache Jackrabbit JCR Commons: from 1.0.0 through 2.22.1. Deployments that accept JNDI URIs for JCR lookup from untrusted users allows them to inject malicious JNDI references, potentially leading to arbitrary code execution through deserialization of untrusted data. Users are recommended to upgrade to version 2.22.2. JCR lookup through JNDI has been disabled by default in 2.22.2. Users of this feature need to enable it explicitly and are adviced to review their use of JNDI URI for JCR lookup.	6.5	More Details
CVE-2025-26441	In add_attr of sdp_discovery.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2025-23259	NVIDIA Mellanox DPDK contains a vulnerability in Poll Mode Driver (PMD), where an attacker on a VM in the system might be able to cause information disclosure and denial of service on the network interface.	6.5	More Details
CVE-2025-42912	SAP HCM My Timesheet Fiori 2.0 application does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This issue has a significant impact on the application's integrity, while confidentiality and availability remain unaffected.	6.5	More Details
CVE-2025-	The Cloud SAML SSO plugin for WordPress is vulnerable to Identity Provider Deletion due to a missing capability check on the delete_config action of the csso_handle_actions() function in all versions up to, and including, 1.0.19.	6.5	More

7045	This makes it possible for unauthenticated attackers to delete any configured IdP, breaking the SSO authentication flow and causing a denial-of-service.		Details
CVE-2025-8564	The SKT Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 3.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8722	The Content Views plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Grid and List widgets in all versions up to, and including, 4.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9126	The Smart Table Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘id’ parameter in all versions up to, and including, 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 inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9378	The Vayu Blocks – Website Builder for the Block Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple attributes in the Lottie block in all versions up to, and including, 1.3.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9057	The Biagiotti Core plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 2.1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-36125	IBM Hardware Management Console - Power 10.3.1050.0 and 11.1.1110.0 is vulnerable to stored cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.4	More Details
CVE-2025-9493	The Admin Menu Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘placeholder’ parameter in all versions up to, and including, 1.14 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8149	The aThemes Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown widget in all versions up to, and including, 1.1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-6067	The Easy Social Feed – Social Photos Gallery – Post Feed – Like Box plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `data-caption` and `data-linktext` parameters in all versions up to, and including, 6.6.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-6757	The Recent Posts Widget Extended plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'rpwe' 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 authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-21483	Improper Access Control vulnerability in Galaxy Store prior to version 4.5.53.6 allows local attacker to access protected data using exported service.	6.4	More Details
CVE-2025-8684	The Flatsome Theme for WordPress is vulnerable to Stored Cross-Site Scripting via the theme's shortcodes in all versions up to, and including, 3.20.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9442	The StreamWeasels Kick Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘vodsChannel’ parameter in all versions up to, and including, 1.1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9853	The Optio Dentistry plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'optio-lightbox' shortcode in all versions up to, and including, 2.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9061	The Wilmer Core plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 2.4.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web	6.4	More Details

	scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-8360	The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several of the plugin's widgets in all versions up to, and including, 1.5.5.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-47437	Server-Side Request Forgery (SSRF) vulnerability in LiteSpeed Technologies LiteSpeed Cache. This issue affects LiteSpeed Cache: from n/a through 7.0.1.	6.4	More Details
CVE-2025-9058	The Mikado Core plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 1.5.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-40594	A vulnerability has been identified in SINAMICS G220 V6.4 (All versions < V6.4 HF2), SINAMICS S200 V6.4 (All versions), SINAMICS S210 V6.4 (All versions < V6.4 HF2). The affected devices allow a factory reset to be executed without the required privileges due to improper privilege management as well as manipulation of configuration data because of leaked privileges of previous sessions. This could allow an unauthorized attacker to escalate their privileges.	6.3	More Details
CVE-2025-9934	A vulnerability was found in TOTOLINK X5000R 9.1.0cu.2415_B20250515. This affects the function sub_410C34 of the file /cgi-bin/cstecgi.cgi. Performing manipulation of the argument pid results in command injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	6.3	More Details
CVE-2024-13065	Improper Enforcement of Behavioral Workflow, Uncontrolled Resource Consumption vulnerability in Akinsoft MyRezzta allows Input Data Manipulation, CAPEC - 125 - Flooding.This issue affects MyRezzta: from s2.02.02 before v2.05.01.	6.3	More Details
CVE-2025-10086	A weakness has been identified in fuyang_lipengjun platform 1.0.0. This issue affects the function queryAll of the file /adposition/queryAll of the component AdPositionController. This manipulation causes improper authorization. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited. Affects another part than CVE-2025-9936.	6.3	More Details
CVE-2025-10085	A security flaw has been discovered in SourceCodester Pet Grooming Management Software 1.0. This vulnerability affects unknown code of the file manage_website.php. The manipulation results in unrestricted upload. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-10083	A vulnerability was determined in SourceCodester Pet Grooming Management Software 1.0. Affected by this issue is some unknown functionality of the file /admin/profile.php. Executing manipulation can lead to unrestricted upload. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-10096	A vulnerability was determined in SimStudioAI sim up to 1.0.0. This affects an unknown function of the file apps/sim/app/api/files/parse/route.ts. Executing manipulation of the argument filePath can lead to server-side request forgery. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. This patch is called 3424a338b763115f0269b209e777608e4cd31785. Applying a patch is advised to resolve this issue.	6.3	More Details
CVE-2025-10072	A vulnerability was found in Portabilis i-Educar up to 2.10. This issue affects some unknown processing of the file /matricula/[ID_STUDENT]/enturmar/. Performing manipulation results in improper access controls. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-10071	A vulnerability has been found in Portabilis i-Educar up to 2.10. This vulnerability affects unknown code of the file /cancelar-enturmacao-em-lote/. Such manipulation leads to improper access controls. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-10070	A flaw has been found in Portabilis i-Educar up to 2.10. This affects an unknown part of the file /enturmacao-em-lote/. This manipulation causes improper access controls. The attack is possible to be carried out remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-10012	A security vulnerability has been detected in Portabilis i-Educar up to 2.10. The impacted element is an unknown function of the file educar_historico_escolar_lst.php. Such manipulation of the argument ref_cod_aluno leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-9942	A vulnerability has been found in CodeAstro Real Estate Management System 1.0. Affected is an unknown function of the file /submitproperty.php. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-10011	A weakness has been identified in Portabilis i-Educar up to 2.10. The affected element is an unknown function of the file /module/TabelaArredondamento/edit. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-30198	ECOVACS robot vacuums and base stations communicate via an insecure Wi-Fi network with a deterministic WPA2-PSK, which can be easily derived.	6.3	More Details

CVE-2025-9941	A flaw has been found in CodeAstro Real Estate Management System 1.0. This impacts an unknown function of the file /register.php. Executing manipulation of the argument uimage can lead to unrestricted upload. The attack can be launched remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-10097	A vulnerability was identified in SimStudioAI sim up to 1.0.0. This impacts an unknown function of the file apps/sim/app/api/function/execute/route.ts. The manipulation of the argument code leads to code injection. The attack is possible to be carried out remotely.	6.3	More Details
CVE-2025-10098	A security flaw has been discovered in PHPGurukul User Management System 1.0. Affected is an unknown function of the file /admin/edit-user-profile.php. The manipulation of the argument uid results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-10105	A flaw has been found in yanyutao0402 ChanCMS up to 3.3.1. Affected by this issue is some unknown functionality of the file /cms/article/search. This manipulation of the argument keyword causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-55162	Envoy is an open source L7 proxy and communication bus designed for large modern service oriented architectures. In versions below 1.32.10 and 1.33.0 through 1.33.6, 1.34.0 through 1.34.4 and 1.35.0, insufficient Session Expiration in the Envoy OAuth2 filter leads to failed logout operations. When configured with __Secure- or __Host-prefixed cookie names, the filter fails to append the required Secure attribute to the Set-Cookie header during deletion. Modern browsers ignore this invalid request, causing the session cookie to persist. This allows a user to remain logged in after they believe they have logged out, creating a session hijacking risk on shared computers. The current implementation iterates through the configured cookie names to generate deletion headers but does not check for these prefixes. This failure to properly construct the deletion header means the user's session cookies are never removed by the browser, leaving the session active and allowing the next user of the same browser to gain unauthorized access to the original user's account and data. This is fixed in versions 1.32.10, 1.33.7, 1.34.5 and 1.35.1.	6.3	More Details
CVE-2025-10106	A vulnerability has been found in yanyutao0402 ChanCMS up to 3.3.1. This affects an unknown part of the file /cms/collect/search. Such manipulation of the argument keyword leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2023-21474	Intent redirection vulnerability in SecSettings prior to SMR Apr-2022 Release 1 allows attackers to access arbitrary file with system privilege.	6.3	More Details
CVE-2025-9847	A weakness has been identified in ScriptAndTools Real Estate Management System 1.0. Impacted is an unknown function of the file register.php. This manipulation of the argument uimage causes unrestricted upload. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-10110	A vulnerability was identified in ChanCMS up to 3.3.1. Impacted is an unknown function of the file /search/. The manipulation with the input '%20or%201=1%20%23/words.html leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-9841	A security vulnerability has been detected in code-projects Mobile Shop Management System 1.0. This affects an unknown function of the file AddNewProduct.php. The manipulation of the argument ProductImage leads to unrestricted upload. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-10013	A vulnerability was detected in Portabilis i-Educar up to 2.10. This affects an unknown function of the file /exportacao-para-o-seb. Performing manipulation results in improper access controls. The attack is possible to be carried out remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2025-30200	ECOVACS robot vacuums and base stations communicate via an insecure Wi-Fi network with a deterministic AES encryption key, which can be easily derived.	6.3	More Details
CVE-2025-10121	A flaw has been found in uverif up to 3.2. This affects the function addbatch of the file /admin/kami_list. This manipulation of the argument note causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-23262	NVIDIA ConnectX contains a vulnerability in the management interface, where an attacker with local access could cause incorrect authorization to modify the configuration. A successful exploit of this vulnerability might lead to denial of service, escalation of privileges, information disclosure, and data tampering.	6.3	More Details
CVE-2025-21041	Insecure Storage of Sensitive Information in Secure Folder prior to Android 16 allows local attackers to access sensitive information.	6.2	More Details
CVE-2025-48527	In multiple locations, there is a possible way to leak hidden work profile notifications due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	6.2	More Details
CVE-2025-26423	In validateIpConfiguration of WifiConfigurationUtil.java, there is a possible way to trigger a permanent DoS due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	6.2	More Details

CVE-2024-40664	In setupAccessibilityServices of AccessibilityFragment.java , there is a possible way to hide an enabled accessibility service due to a logic error in the code. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	6.2	More Details
CVE-2025-9111	The AI ChatBot for WordPress WordPress plugin before 7.1.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	6.1	More Details
CVE-2024-43184	IBM Jazz Foundation 7.0.2 through 7.0.2 iFix033, 7.0.3 through 7.0.3 iFix012, and 7.1.0 through 7.1.0 iFix002 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.1	More Details
CVE-2023-21482	Missing authorization vulnerability in Camera prior to versions 11.1.02.18 in Android 11, 12.1.03.8 in Android 12 and 13.1.01.4 in Android 13 allows physical attackers to install package through Galaxy store before completion of Setup wizard.	6.1	More Details
CVE-2025-42938	Due to a Cross-Site Scripting (XSS) vulnerability in the SAP NetWeaver ABAP Platform, an unauthenticated attacker could generate a malicious link and make it publicly accessible. If an authenticated user clicks on this link, the injected input is processed during the website&#65533;s page generation, resulting in the creation of malicious content. When executed, this content allows the attacker to access or modify information within the victim's browser scope, impacting the confidentiality and integrity&#65533;while availability remains unaffected.	6.1	More Details
CVE-2025-55054	CWE-79 Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')	6.1	More Details
CVE-2025-42920	Due to a Cross-Site Scripting (XSS) vulnerability in the SAP Supplier Relationship Management, an unauthenticated attacker could generate a malicious link and make it publicly accessible. If an authenticated victim clicks on the link, the injected input is processed during the page generation, resulting in the execution of malicious content. This execution allows the attacker to access and modify information within the victim's browser scope, impacting confidentiality and integrity, while availability remains unaffected.	6.1	More Details
CVE-2025-20330	A vulnerability in the web-based management interface of Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2025-55944	Slink v1.4.9 allows stored cross-site scripting (XSS) via crafted SVG uploads. When a user views the shared image in a new browser tab, the embedded JavaScript executes. The issue affects both authenticated and unauthenticated users.	6.1	More Details
CVE-2014-125128	'sanitize-html' prior to version 1.0.3 is vulnerable to Cross-site Scripting (XSS). The function 'naughtyHref' doesn't properly validate the hyperreference (`href`) attribute in anchor tags (`<a>`), allowing bypasses that contain different casings, whitespace characters, or hexadecimal encodings.	6.1	More Details
CVE-2025-48554	In handlePackagesChanged of DevicePolicyManagerService.java, there is a possible persistent denial of service due to a logic error in the code. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	6.1	More Details
CVE-2025-55305	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. In versions below 35.7.5, 36.0.0-alpha.1 through 36.8.0, 37.0.0-alpha.1 through 37.3.1 and 38.0.0-alpha.1 through 38.0.0-beta.6, ASAR Integrity Bypass via resource modification. This only impacts apps that have the embeddedAsarIntegrityValidation and onlyLoadAppFromAsar fuses enabled. Apps without these fuses enabled are not impacted. This issue is fixed in versions 35.7.5, 36.8.1, 37.3.1 and 38.0.0-beta.6.	6.1	More Details
CVE-2025-55143	Reflected text injection in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote unauthenticated attacker to inject arbitrary text into a crafted HTTP response. User interaction is required.	6.1	More Details
CVE-2025-0010	An out of bounds write in the Linux graphics driver could allow an attacker to overflow the buffer potentially resulting in loss of confidentiality, integrity, or availability.	6.1	More Details
CVE-2019-25225	`sanitize-html` prior to version 2.0.0-beta is vulnerable to Cross-site Scripting (XSS). The `sanitizeHtml()` function in `index.js` does not sanitize content when using the custom `transformTags` option, which is intended to convert attribute values into text. As a result, malicious input can be transformed into executable code.	6.1	More Details
CVE-2024-36346	Improper input validation in AMD Power Management Firmware (PMFW) could allow a privileged attacker from Guest VM to send arbitrary input data potentially causing a GPU Reset condition.	6.0	More Details
CVE-2023-	Improper input validation vulnerability in TIGERF trustlet prior to SMR Apr-2023 Release 1 allows local attackers to	6.0	More

21478	access protected data.		Details
CVE-2025-58984	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in nanbu Welcart e-Commerce allows Stored XSS. This issue affects Welcart e-Commerce: from n/a through 2.11.20.	5.9	More Details
CVE-2025-58883	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Thomas Harris Search Cloud One allows Stored XSS. This issue affects Search Cloud One: from n/a through 2.2.5.	5.9	More Details
CVE-2025-58983	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stefano Lissa Include Me allows Stored XSS. This issue affects Include Me: from n/a through 1.3.2.	5.9	More Details
CVE-2025-58873	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pusheco Pushe Web Push Notification allows Stored XSS. This issue affects Pushe Web Push Notification: from n/a through 0.5.0.	5.9	More Details
CVE-2025-58982	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pixeline Pixeline's Email Protector allows Stored XSS. This issue affects Pixeline's Email Protector: from n/a through 1.3.8.	5.9	More Details
CVE-2025-30875	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alexandre Froger WP Weixin allows Stored XSS. This issue affects WP Weixin: from n/a through 1.3.16.	5.9	More Details
CVE-2025-58884	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ivan Drago vipdrv allows Stored XSS. This issue affects vipdrv: from n/a through 1.0.3.	5.9	More Details
CVE-2025-58886	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tan Nguyen Instant Locations allows Stored XSS. This issue affects Instant Locations: from n/a through 1.0.	5.9	More Details
CVE-2025-1761	IBM Concert Software 1.0.0 through 1.1.0 could allow a remote attacker to obtain sensitive information from allocated memory due to improper clearing of heap memory.	5.9	More Details
CVE-2025-48102	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gourl GoUrl Bitcoin Payment Gateway & Paid Downloads & Membership allows Stored XSS. This issue affects GoUrl Bitcoin Payment Gateway & Paid Downloads & Membership: from n/a through 1.6.6.	5.9	More Details
CVE-2025-58805	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OTWthemes Widgetize Pages Light allows Stored XSS. This issue affects Widgetize Pages Light: from n/a through 3.0.	5.9	More Details
CVE-2025-58820	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Carousel Ultimate allows Stored XSS. This issue affects Carousel Ultimate: from n/a through 1.8.	5.9	More Details
CVE-2025-9824	ImpactThe attacker can validate if a user exists by checking the time login returns. This timing difference can be used to enumerate valid usernames, after which an attacker could attempt brute force attacks. PatchesThis vulnerability has been patched, implementing a timing-safe form login authenticator that ensures consistent response times regardless of whether a user exists or not. Technical DetailsThe vulnerability was caused by different response times when: * A valid username was provided (password hashing occurred) * An invalid username was provided (no password hashing occurred) The fix introduces a TimingSafeFormLoginAuthenticator that performs a dummy password hash verification even for non-existent users, ensuring consistent timing. WorkaroundsNo workarounds are available. Users should upgrade to the patched version. References * https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/03-Identity_Management_Testing/04-Testing_for_Account_Enumeration_and_Guessable_User_Account	5.9	More Details
CVE-2025-58631	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ZEEN101 IssueM allows DOM-Based XSS. This issue affects IssueM: from n/a through 2.9.0.	5.9	More Details
CVE-2023-21468	Improper access control vulnerability in Telephony prior to SMR Apr-2023 Release 1 allows attackers to access files with escalated permission.	5.9	More Details
CVE-2025-58630	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rbaer Simple Matomo Tracking Code allows Stored XSS. This issue affects Simple Matomo Tracking Code: from n/a through 1.1.0.	5.9	More Details
CVE-2025-58625	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Spiffy Plugins WP Flow Plus allows Stored XSS. This issue affects WP Flow Plus: from n/a through 5.2.5.	5.9	More Details

CVE-2025-21032	Improper access control in One UI Home prior to SMR Sep-2025 Release 1 allows physical attackers to bypass Kiosk mode under limited conditions.	5.9	More Details
CVE-2025-58810	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jimmywb Simple Link List Widget allows Stored XSS. This issue affects Simple Link List Widget: from n/a through 0.3.2.	5.9	More Details
CVE-2025-58811	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP CodeUs Ultimate Client Dash allows Stored XSS. This issue affects Ultimate Client Dash: from n/a through 4.6.	5.9	More Details
CVE-2025-58791	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Arjan Olsder SEO Auto Linker allows Stored XSS. This issue affects SEO Auto Linker: from n/a through 1.5.3.	5.9	More Details
CVE-2025-58821	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdever WP Notification Bell allows Stored XSS. This issue affects WP Notification Bell: from n/a through 1.4.5.	5.9	More Details
CVE-2025-9901	A flaw was found in libsoup’s caching mechanism, SoupCache, where the HTTP Vary header is ignored when evaluating cached responses. This header ensures that responses vary appropriately based on request headers such as language or authentication. Without this check, cached content can be incorrectly reused across different requests, potentially exposing sensitive user information. While the issue is unlikely to affect everyday desktop use, it could result in confidentiality breaches in proxy or multi-user environments.	5.9	More Details
CVE-2025-58596	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in properfraction MailOptin allows Stored XSS. This issue affects MailOptin: from n/a through 1.2.75.0.	5.9	More Details
CVE-2025-58825	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Habibur Rahman Comment Form WP – Customize Default Comment Form allows Stored XSS. This issue affects Comment Form WP – Customize Default Comment Form: from n/a through 2.0.0.	5.9	More Details
CVE-2025-58832	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly Search by Google allows Stored XSS. This issue affects Search by Google: from n/a through 1.9.	5.9	More Details
CVE-2025-32330	In generateRandomPassword of LocalBluetoothLeBroadcast.java, there is a possible way to intercept the Auracast audio stream due to an insecure default value. This could lead to remote (proximal/adjacent) information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.7	More Details
CVE-2025-40929	Cpanel::JSON::XS before version 4.40 for Perl has an integer buffer overflow causing a segfault when parsing crafted JSON, enabling denial-of-service attacks or other unspecified impact	5.6	More Details
CVE-2025-26449	In multiple locations, there is a possible permanent denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-54241	After Effects versions 25.3, 24.6.7 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure, potentially disclosing sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-54240	After Effects versions 25.3, 24.6.7 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure, potentially disclosing sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-54239	After Effects versions 25.3, 24.6.7 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure, potentially disclosing sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-54901	Buffer over-read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	5.5	More Details
CVE-2025-53803	Generation of error message containing sensitive information in Windows Kernel allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-9822	SummaryA user with administrator rights can change the configuration of the mautic application and extract secrets that are not normally available. ImpactAn administrator who usually does not have access to certain parameters, such as database credentials, can disclose them.	5.5	More Details
CVE-2025-26437	In CredentialManagerServiceStub of CredentialManagerService.java, there is a possible way to retrieve candidate credentials due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details

CVE-2025-36893	In ReadTachyonCommands of gxp_main_actor.cc, there is a possible information leak due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-26448	In writeToParcel of CursorWindow.cpp, there is a possible out of bounds read due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-26442	In onCreate of NotificationAccessConfirmationActivity.java, there is a possible incorrect verification of proper intent filters in NLS due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-21028	Improper privilege management in ThemeManager prior to SMR Sep-2025 Release 1 allows local privileged attackers to reuse trial items.	5.5	More Details
CVE-2025-26463	In allowPackageAccess of multiple files, resource exhaustion is possible when repeatedly adding allowed packages. This could lead to a local persistent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-26456	In multiple functions of DexUseManagerLocal.java, there is a possible way to crash system server due to a logic error in the code. This could lead to local permanent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-53804	Exposure of sensitive information to an unauthorized actor in Windows Kernel allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-48524	In isSystem of WifiPermissionsUtil.java, there is a possible permission bypass due to a missing permission check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-53799	Use of uninitialized resource in Windows Imaging Component allows an unauthorized attacker to disclose information locally.	5.5	More Details
CVE-2025-26445	In offerNetwork of ConnectivityService.java, there is a possible leak of sensitive data due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-26432	In multiple locations, there is a possible way to persistently DoS the device due to a missing length check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-26453	In isContentUriForOtherUser of BluetoothOppSendFileInfo.java, there is a possible cross user data leak due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-48529	In setRingtoneUri of VoicemailNotificationSettingsUtil.java , there is a possible cross user data leak due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-32317	In App Widget, there is a possible Information Disclosure due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-48545	In isSystemUid of AccountManagerService.java, there is a possible way for an app to access privileged APIs due to a confused deputy. This could lead to local privilege escalation with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-48561	In multiple locations, there is a possible way to access data displayed on the screen due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-0028	In Audio Service, there is a possible way to obtain MAC addresses of nearby Bluetooth devices due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-26434	In libxml2, there is a possible out of bounds read due to a buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-58373	Roo Code is an AI-powered autonomous coding agent that lives in users' editors. Versions 3.25.23 and below contain a vulnerability where .rooignore protections could be bypassed using symlinks. This allows an attacker with write access to the workspace to trick the extension into reading files that were intended to be excluded. As a result, sensitive files such as .env or configuration files could be exposed. An attacker able to modify files within the	5.5	More Details

	workspace could gain unauthorized access to sensitive information by bypassing .rooignore rules. This could include secrets, configuration details, or other excluded project data. This is fixed in version 3.26.0.		
CVE-2025-59036	Infrahub offers a central hub to manage data, templates, and playbooks. Prior to versiond 1.3.9 and 1.4.5, a bug in the authentication logic will cause API tokens that were deleted and/or expired to be considered valid. This means that any API token that is associated with an active user account can authenticate successfully. This issue is fixed in versions 1.3.9 and 1.4.5. As a workaround, users can delete or deactivate the account associated with a deleted API token to prevent that token from authenticating.	5.5	More Details
CVE-2025-48560	In AndroidManifest.xml, there is a possible way for an app to monitor motion events due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-32316	In gralloc4, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-23261	NVIDIA Cumulus Linux and NVOS products contain a vulnerability, where hashed user passwords are not properly suppressed in log files, potentially disclosing information to unauthorized users.	5.5	More Details
CVE-2025-48542	In multiple functions of AccountManagerService.java, there is a possible permanent denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-26429	In collectOps of AppOpsService.java, there is a possible way to cause permanent DoS due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-48559	In multiple functions of AppOpsService.java, there is a possible add a large amount of app ops due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-0009	A NULL pointer dereference in AMD Crash Defender could allow an attacker to write a NULL output to a log file potentially resulting in a system crash and loss of availability.	5.5	More Details
CVE-2025-48538	In setApplicationHiddenSettingAsUser of PackageManagerService.java, there is a possible way to hide a system critical package due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-58841	Incorrect Privilege Assignment vulnerability in John Luetke Media Author allows Privilege Escalation. This issue affects Media Author: from n/a through 1.0.4.	5.5	More Details
CVE-2025-48550	In testGrantSlicePermission of SliceManagerTest.java, there is a possible permanent denial of service due to a path traversal error. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-57576	PHPGurukul Online Shopping Portal 2.1 is vulnerable to Cross Site Scripting (XSS) in /admin/updateorder.php.	5.4	More Details
CVE-2025-41048	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/admin.	5.4	More Details
CVE-2025-55144	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure restricted settings.	5.4	More Details
CVE-2025-41049	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/appform.	5.4	More Details
CVE-2025-41039	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[sconfig][admin_landing_page]', 'data[sconfig][currency]', 'data[sconfig][db_version]', 'data[sconfig][default_pagination]', 'data[sconfig][emailsetup_from_email]', 'data[sconfig][emailsetup_host]', 'data[sconfig][emailsetup_password]', 'data[sconfig][emailsetup_port]', 'data[sconfig][emailsetup_username]', 'data[sconfig][fileresource_id]', 'data[sconfig][large_image_height]', 'data[sconfig][large_image_width]' and 'data[sconfig][time_zone_padding]' parameters in /apprain/admin/config/opts.	5.4	More Details
CVE-2025-32688	Missing Authorization vulnerability in Sovica Target Video Easy Publish. This issue affects Target Video Easy Publish: from n/a through 3.8.8.	5.4	More Details

CVE-2025-41047	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/ace.	5.4	More Details
CVE-2025-9937	A security flaw has been discovered in elunez eladmin 1.1. Impacted is the function deleteFile of the component LocalStorageController. The manipulation results in improper authorization. The attack may be performed from remote. The exploit has been released to the public and may be exploited.	5.4	More Details
CVE-2025-41041	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[code]', 'data[lang][0][key]', 'data[lang][0][value]', 'data[lang][1][key]' and 'data[title]' parameters in /apprain/developer/language/default.xml.	5.4	More Details
CVE-2025-41045	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[sconfig][ethical_licensekey]' parameter in /apprain/admin/config/ethical.	5.4	More Details
CVE-2025-41040	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[code]', 'data[lang][0][key]', 'data[lang][0][value]', 'data[lang][1][key]' and 'data[title]' parameters in /apprain/developer/language/lipsum.xml.	5.4	More Details
CVE-2025-8711	CSRF in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote unauthenticated attacker to execute limited actions on behalf of the victim user. User interaction is required.	5.4	More Details
CVE-2025-41042	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Option][message]', 'data[Option][subject]' and 'data[Option][templatetype]' parameters in /apprain/information/manage/emailtemplate/add.	5.4	More Details
CVE-2025-41044	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Page][name]' parameter in /apprain/page/manage-static-pages/create.	5.4	More Details
CVE-2025-9867	Inappropriate implementation in Downloads in Google Chrome on Android prior to 140.0.7339.80 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	5.4	More Details
CVE-2025-9865	Inappropriate implementation in Toolbar in Google Chrome on Android prior to 140.0.7339.80 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform domain spoofing via a crafted HTML page. (Chromium security severity: Medium)	5.4	More Details
CVE-2025-56761	Memos 0.22 is vulnerable to Stored Cross site scripting (XSS) vulnerabilities by the upload attachment and user avatar features. Memos does not verify the content type of the uploaded data and serve it back as is. An authenticated attacker can use this to elevate their privileges when the stored XSS is viewed by an admin.	5.4	More Details
CVE-2025-8712	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 22.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure restricted settings.	5.4	More Details
CVE-2025-58639	Missing Authorization vulnerability in Ali Khallad Contact Form By Mega Forms allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Contact Form By Mega Forms: from n/a through 1.6.1.	5.4	More Details
CVE-2025-58641	Server-Side Request Forgery (SSRF) vulnerability in kamleshyadav Exit Intent Popup allows Server Side Request Forgery. This issue affects Exit Intent Popup: from n/a through 1.0.1.	5.4	More Details
CVE-2025-54252	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. This could result in bypassing security features within the application. Exploitation of this issue requires user interaction in that a victim must browse to the page containing the vulnerable field.	5.4	More Details
CVE-2025-41043	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[AppReportCode][id]' and 'data[AppReportCode][name]' parameters in /apprain/appreport/manage/.	5.4	More Details
CVE-2025-41050	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/base_libs.	5.4	More Details
CVE-2025-41046	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/960grid.	5.4	More Details
CVE-	A vulnerability in the user profile component of Cisco Webex Meetings could have allowed an authenticated, remote attacker with low privileges to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. Cisco has addressed this vulnerability in the Cisco Webex Meetings service, and no customer action is needed. This		More

2025-20328	vulnerability existed because of insufficient validation of user-supplied input to the user profile component of Cisco Webex Meetings. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could have allowed the attacker to conduct an XSS attack against the targeted user.	5.4	Details
CVE-2025-41051	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/bootstrap.	5.4	More Details
CVE-2025-53291	Missing Authorization vulnerability in spoddev2021 Spreadconnect. This issue affects Spreadconnect: from n/a through 2.1.5.	5.4	More Details
CVE-2025-9542	The AutomatorWP – Automator plugin for no-code automations, webhooks & custom integrations in WordPress plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on multiple plugin's functions in all versions up to, and including, 5.3.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify integration settings or view existing automations.	5.4	More Details
CVE-2025-41057	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/rich_text_editor.	5.4	More Details
CVE-2025-41052	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/canvasjs.	5.4	More Details
CVE-2025-41059	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/tablesorter.	5.4	More Details
CVE-2025-41060	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/tree.	5.4	More Details
CVE-2025-58785	Missing Authorization vulnerability in jbhovik Ray Enterprise Translation allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Ray Enterprise Translation: from n/a through 1.7.1.	5.4	More Details
CVE-2025-41061	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/uploadify.	5.4	More Details
CVE-2025-41062	A vulnerability has been discovered in version 4.0.5 of appRain CMF, consisting of an authenticated reflected XSS due to a lack of proper validation of user input, through the 'page' parameter in /apprain/developer/addons.	5.4	More Details
CVE-2025-41037	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[FileManager][search]' parameter in /apprain/admin/filemanager.	5.4	More Details
CVE-2025-41063	A vulnerability has been discovered in version 4.0.5 of appRain CMF, consisting of an authenticated reflected XSS due to a lack of proper validation of user input, through the 's' parameter in /apprain/developer/debug-log/db.	5.4	More Details
CVE-2025-58801	Cross-Site Request Forgery (CSRF) vulnerability in KCS Responder allows Cross Site Request Forgery. This issue affects Responder: from n/a through 4.3.8.	5.4	More Details
CVE-2025-41036	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Admin][description]', 'data[Admin][f_name]' and 'data[Admin][l_name]' parameters in /apprain/admin/account/edit.	5.4	More Details
CVE-2025-8695	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Netcad NetGIS Server allows Reflected XSS.This issue affects NetGIS Server: from 5.2.4 through 22.08.2025.	5.4	More Details
CVE-2025-58818	Cross-Site Request Forgery (CSRF) vulnerability in SwiftNinjaPro Developer Tools Blocker allows Cross Site Request Forgery. This issue affects Developer Tools Blocker: from n/a through 3.2.1.	5.4	More Details
CVE-2025-42915	Fiori app Manage Payment Blocks does not perform the necessary authorization checks, allowing an attacker with basic user privileges to abuse functionalities that should be restricted to specific user groups.This issue could impact both the confidentiality and integrity of the application without affecting the availability.	5.4	More Details
CVE-2023-21481	Improper URL input validation vulnerability in Samsung Account application prior to version 14.1.0.0 allows remote attackers to get sensitive information.	5.4	More Details

CVE-2025-41058	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/row_manager.	5.4	More Details
CVE-2025-41055	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/dialogs.	5.4	More Details
CVE-2025-41056	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/hysontable.	5.4	More Details
CVE-2025-41038	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Group][name]' parameter in /apprain/admin/managegroup/add/.	5.4	More Details
CVE-2025-41054	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/cycle.	5.4	More Details
CVE-2025-41053	A vulnerability has been discovered in appRain CMF version 4.0.5, consisting of a stored authenticated XSS due to a lack of proper validation of user input, through the 'data[Addon][layouts]' and 'data[Addon][layouts_except]' parameters in /apprain/developer/addons/update/commonresource.	5.4	More Details
CVE-2025-58981	Missing Authorization vulnerability in Equalize Digital Accessibility Checker by Equalize Digital allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Accessibility Checker by Equalize Digital: from n/a through 1.31.0.	5.4	More Details
CVE-2025-42926	SAP NetWeaver Application Server Java does not perform an authentication check when an attacker attempts to access internal files within the web application.Upon successfully exploitation, an unauthenticated attacker could access these files to gather additional sensitive information about the system.This vulnerability has a low impact on confidentiality and does not affect the integrity or availability of the server.	5.3	More Details
CVE-2025-10093	A vulnerability was identified in D-Link DIR-852 up to 1.00CN B09. Affected by this vulnerability is the function phpcgi_main of the file /getcfg.php of the component Device Configuration Handler. Such manipulation leads to information disclosure. The attack may be performed from remote. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2025-58135	Improper action enforcement in certain Zoom Workplace Clients for Windows may allow an unauthenticated user to conduct a disclosure of information via network access.	5.3	More Details
CVE-2025-36909	Information disclosure	5.3	More Details
CVE-2025-3212	Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user process to perform valid GPU memory processing operations to gain access to already freed memory.This issue affects Bifrost GPU Kernel Driver: from r41p0 through r49p4, from r50p0 through r51p0; Valhall GPU Kernel Driver: from r41p0 through r49p4, from r50p0 through r54p0; Arm 5th Gen GPU Architecture Kernel Driver: from r41p0 through r49p4, from r50p0 through r54p0.	5.3	More Details
CVE-2025-58980	Missing Authorization vulnerability in recorp Export WP Page to Static HTML/CSS allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Export WP Page to Static HTML/CSS: from n/a through 4.1.0.	5.3	More Details
CVE-2025-58613	Missing Authorization vulnerability in Barn2 Plugins Posts Table with Search & Sort allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Posts Table with Search & Sort: from n/a through 1.4.10.	5.3	More Details
CVE-2025-20335	A vulnerability in the directory permissions of Cisco Desk Phone 9800 Series, Cisco IP Phone 7800 and 8800 Series, and Cisco Video Phone 8875 could allow an unauthenticated, remote attacker to write arbitrary files on an affected device. This vulnerability is due to a lack of proper authentication controls. An attacker could exploit this vulnerability by sending a crafted request to an affected device. A successful exploit could allow the attacker to perform arbitrary file writes to specific directories in the underlying operating system. Note: To exploit this vulnerability, Web Access must be enabled on the phone. Web Access is disabled by default.	5.3	More Details
CVE-2025-7368	The REHub - Price Comparison, Multi Vendor Marketplace Wordpress Theme theme for WordPress is vulnerable to Information Exposure in all versions up to, and including, 19.9.7 via the 'ajax_action_re_getfullcontent' function due to insufficient restrictions on which posts can be included. This makes it possible for unauthenticated attackers to extract data from password protected posts that they should not have access to.	5.3	More Details
CVE-2025-9849	The Html Social share buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'zm_sh_btn' shortcode in all versions up to, and including, 2.1.16 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected	5.3	More Details

	page.		
CVE-2025-58979	Missing Authorization vulnerability in BerqWP BerqWP allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects BerqWP: from n/a through 2.2.53.	5.3	More Details
CVE-2025-9842	A vulnerability was detected in Das Parking Management System 停车场管理系统 6.2.0. This impacts an unknown function of the file /Operator/Search. The manipulation results in information disclosure. The attack may be performed from remote. The exploit is now public and may be used.	5.3	More Details
CVE-2025-56139	LinkedIn Mobile Application for Android version 4.1.1087.2 fails to update link preview metadata (image, title, description) when a user replaces the original URL in a post or comment before publishing. As a result, the stale preview remains visible while the clickable link points to a different URL, which can be malicious. This UI misrepresentation enables attackers to deceive users by displaying trusted previews for harmful links, facilitating phishing attacks and user confusion.	5.3	More Details
CVE-2025-58978	Missing Authorization vulnerability in WP Swings PDF Generator for WordPress allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects PDF Generator for WordPress: from n/a through 1.5.4.	5.3	More Details
CVE-2025-20336	A vulnerability in the directory permissions of Cisco Desk Phone 9800 Series, Cisco IP Phone 7800 and 8800 Series, and Cisco Video Phone 8875 could allow an unauthenticated, remote attacker to access sensitive information on an affected device. This vulnerability exists because the product exposes sensitive information to an actor that is not explicitly authorized to have access to that information. An attacker could exploit this vulnerability by sending a crafted packet to the IP address of a device that has Web Access enabled. A successful exploit could allow the attacker to access sensitive information from the device. Note: To exploit this vulnerability, Web Access must be enabled on the phone. Web Access is disabled by default.	5.3	More Details
CVE-2025-58835	Improper Validation of Specified Quantity in Input vulnerability in calliko Bonus for Woo allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Bonus for Woo: from n/a through 7.4.1.	5.3	More Details
CVE-2025-58369	fs2 is a compositional, streaming I/O library for Scala. Versions 3.12.2 and lower and 3.13.0-M1 through 3.13.0-M6 is vulnerable to denial of service attacks though TLS sessions using fs2-io on the JVM using the fs2.io.net.tls package. When establishing a TLS session, if one side of the connection shuts down `write` while the peer side is awaiting more data to progress the TLS handshake, the peer side will spin loop on the socket read, fully utilizing a CPU. The CPU is consumed until the overall connection is closed, potentially shutting down a fs2-io powered server. This issue is fixed in versions 3.12.1 and 3.13.0-M7.	5.3	More Details
CVE-2025-58795	Missing Authorization vulnerability in Payoneer Checkout Payoneer Checkout allows Content Spoofing. This issue affects Payoneer Checkout: from n/a through 3.4.0.	5.3	More Details
CVE-2025-58797	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Mahmudul Hasan Arif Ninja Charts allows Retrieve Embedded Sensitive Data. This issue affects Ninja Charts: from n/a through 3.3.2.	5.3	More Details
CVE-2023-21466	PendingIntent hijacking vulnerability in CertificatePolicy in framework prior to SMR Apr-2023 Release 1 allows local attackers to access contentProvider without proper permission.	5.3	More Details
CVE-2025-49860	Missing Authorization vulnerability in Majestic Support Majestic Support. This issue affects Majestic Support: from n/a through 1.1.0.	5.3	More Details
CVE-2025-40757	A vulnerability has been identified in APOGEE PXC Series (BACnet) (All versions), APOGEE PXC Series (P2 Ethernet) (All versions), TALON TC Series (BACnet) (All versions). Affected devices connected to the network allow unrestricted access to sensitive files, such as databases. This could allow an attacker to download encrypted .db file containing passwords.	5.3	More Details
CVE-2023-21479	Improper authorization in Smart suggestions prior to SMR Apr-2023 Release 1 in Android 13 and 4.1.01.0 in Android 12 allows remote attackers to register a schedule.	5.3	More Details
CVE-2023-31351	Improper restriction of operations in the IOMMU could allow a malicious hypervisor to access guest private memory resulting in loss of integrity.	5.3	More Details
CVE-2025-58603	Missing Authorization vulnerability in Surfer Surfer allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Surfer: from n/a through 1.6.4.574.	5.3	More Details
CVE-2025-58634	Missing Authorization vulnerability in peachpay PeachPay Payments allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects PeachPay Payments: from n/a through 1.117.4.	5.3	More Details

CVE-2025-58635	Missing Authorization vulnerability in PalsCode Support Genix allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Support Genix: from n/a through 1.4.23.	5.3	More Details
CVE-2025-58600	Missing Authorization vulnerability in Cozmoslabs Paid Member Subscriptions allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Paid Member Subscriptions: from n/a through 2.15.9.	5.3	More Details
CVE-2025-58442	Saleor is an e-commerce platform. Starting in version 3.21.0 and prior to version 3.21.16, requesting certain fields in the response of `accountRegister` may result in errors that could unintentionally reveal whether a user with the provided email already exists in Saleor. Version 3.21.16 fixes the issue. As a workaround, rate-limit the mutation to reduce the impact.	5.3	More Details
CVE-2025-9843	A flaw has been found in Das Parking Management System 停车场管理系统 6.2.0. Affected is an unknown function of the file /Operator/FindAll. This manipulation causes information disclosure. It is possible to initiate the attack remotely. The exploit has been published and may be used.	5.3	More Details
CVE-2025-9616	The PopAd plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.4. This is due to missing or incorrect nonce validation on the PopAd_reset_cookie_time function. This makes it possible for unauthenticated attackers to reset cookie time settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.3	More Details
CVE-2025-5500	A flaw has been found in ZhenShi Mibro Fit App 1.6.3.17499 on Android. This impacts an unknown function of the file AndroidManifest.xml of the component com.xiaoxun.xunoversea.mibrofit. This manipulation causes improper export of android application components. The attack requires local access. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-53340	Missing Authorization vulnerability in awesomesupport Awesome Support. This issue affects Awesome Support: from n/a through 6.3.4.	5.3	More Details
CVE-2025-56435	SQL Injection vulnerability in FoxCMS v1.2.6 and before allows a remote attacker to execute arbitrary code via the. file /DataBackup.php and the operation on the parameter id.	5.3	More Details
CVE-2025-56498	An OS command injection vulnerability exists in PLDT WiFi Router's Prolink PGN6401V Firmware 8.1.2 web management interface. The ping6.asp page submits user input to the /boaform/formPing6 endpoint via the pingAddr parameter, which is not properly sanitized. An authenticated attacker can exploit this flaw by injecting arbitrary system commands, which are executed by the underlying operating system with root privileges. The router uses the Boa web server (version 0.93.15) to handle the request. Successful exploitation can lead to full system compromise and unauthorized control of the network device.	5.3	More Details
CVE-2025-53348	Missing Authorization vulnerability in Laborator Kalium. This issue affects Kalium: from n/a through 3.18.3.	5.3	More Details
CVE-2025-58210	Missing Authorization vulnerability in ThemeMove Makeaholic allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Makeaholic: from n/a through 1.8.5.	5.3	More Details
CVE-2025-26426	In BroadcastController.java of registerReceiverWithFeatureTraced, there is a possible way to receive broadcasts meant for the "android" package due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.1	More Details
CVE-2025-36100	IBM MQ LTS 9.1.0.0 through 9.1.0.29, 9.2.0.0 through 9.2.0.36, 9.3.0.0 through 9.3.0.30 and 9.4.0.0 through 9.4.0.12 and IBM MQ CD 9.3.0.0 through 9.3.5.1 and 9.4.0.0 through 9.4.3.0 Java and JMS stores a password in client configuration files when trace is enabled which can be read by a local user.	5.1	More Details
CVE-2025-22425	In onCreate of InstallStart.java, there is a possible permissions bypass due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	5.1	More Details
CVE-2025-58313	Race condition vulnerability in the device standby module. Impact: Successful exploitation of this vulnerability may cause feature exceptions of the device standby module.	5.1	More Details
CVE-2025-58759	TinyEnv is an environment variable loader for PHP applications. In versions 1.0.9 and 1.0.10, TinyEnv did not properly strip inline comments inside .env values. This could lead to unexpected behavior or misconfiguration, where variables contain unintended characters (including # or comment text). Applications depending on strict environment values may expose logic errors, insecure defaults, or failed authentication. The issue is fixed in v1.0.11. Users should upgrade to the latest patched version. As a temporary workaround, avoid using inline comments in .env files, or sanitize loaded values manually.	5.1	More Details
CVE-2025-	TinyEnv is an environment variable loader for PHP applications. In versions 1.0.1, 1.0.2, 1.0.9, and 1.0.10, TinyEnv did not require the `.env` file to exist when loading environment variables. This could lead to unexpected behavior where the application silently ignores missing configuration, potentially causing insecure defaults or deployment	5.1	More Details

58758	misconfigurations. The issue has been fixed in version 1.0.11. All users should upgrade to 1.0.11 or later. As a workaround, users can manually verify the existence of the `.env` file before initializing TinyEnv.		
CVE-2025-21025	Improper access control in MARsExemptionManager prior to SMR Sep-2025 Release 1 allows local attackers to be excluded from background execution management.	5.1	More Details
CVE-2025-21027	Improper verification of intent by broadcast receiver in ImsService prior to SMR Sep-2025 Release 1 allows local attackers to temporarily disable the SIM.	5.1	More Details
CVE-2025-21038	Improper verification of intent by SamsungExceptionalBroadcastReceiver in S Assistant prior to version 9.3.2 allows local attackers to modify itinerary information.	5.1	More Details
CVE-2025-21039	Improper verification of intent by SystemExceptionalBroadcastReceiver in S Assistant prior to version 9.3.2 allows local attackers to modify itinerary information.	5.1	More Details
CVE-2025-21040	Improper verification of intent by ExternalBroadcastReceiver in S Assistant prior to version 9.3.2 allows local attackers to modify itinerary information.	5.1	More Details
CVE-2025-0087	In onCreate of UninstallerActivity.java, there is a possible way to uninstall a different user's app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.1	More Details
CVE-2025-9489	The The WP-Members Membership Plugin plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 3.5.4.2. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes.	5.0	More Details
CVE-2025-21036	Improper access control in Samsung Notes prior to version 4.4.30.63 allows local privileged attackers to access exported note files. User interaction is required for triggering this vulnerability.	5.0	More Details
CVE-2025-58606	Missing Authorization vulnerability in CozyThemes SaasLauncher allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects SaasLauncher: from n/a through 1.3.0.	5.0	More Details
CVE-2025-42911	SAP NetWeaver (Service Data Download) allows an authenticated user to call a remote-enabled function module, which could grant access to information about the SAP system and operating system. This leads to a low impact on confidentiality, with no effect on the integrity and availability of the application	5.0	More Details
CVE-2025-48551	In multiple locations, there is a possible leak of an image across the Android User isolation boundary due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	5.0	More Details
CVE-2025-48562	In writeContent of RemotePrintDocument.java, there is a possible information disclosure due to a logic error. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	5.0	More Details
CVE-2025-55146	An unchecked return value in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with admin privileges to trigger a denial of service.	4.9	More Details
CVE-2025-58977	Server-Side Request Forgery (SSRF) vulnerability in Rhys Wynne WP eBay Product Feeds allows Server Side Request Forgery. This issue affects WP eBay Product Feeds: from n/a through 3.4.8.	4.9	More Details
CVE-2025-58829	Server-Side Request Forgery (SSRF) vulnerability in aitool Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One allows Server Side Request Forgery. This issue affects Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One: from n/a through 2.2.6.	4.9	More Details
CVE-2025-9085	The User Registration & Membership plugin for WordPress is vulnerable to SQL Injection via the 's' parameter in version 4.3.0. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2025-54250	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A high-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access.	4.9	More Details
CVE-2025-	The atec Debug plugin for WordPress is vulnerable to arbitrary file read in all versions up to, and including, 1.2.22 via the 'custom_log' parameter. This makes it possible for authenticated attackers, with Administrator-level access	4.9	More Details

9516	and above, to view the contents of files outside of the originally intended directory.		
CVE-2025-53609	A Relative Path Traversal vulnerability [CWE-23] in FortiWeb 7.6.0 through 7.6.4, 7.4.0 through 7.4.8, 7.2.0 through 7.2.11, 7.0.2 through 7.0.11 may allow an authenticated attacker to perform an arbitrary file read on the underlying system via crafted requests.	4.9	More Details
CVE-2025-10046	The ELEX WooCommerce Google Shopping (Google Product Feed) plugin for WordPress is vulnerable to SQL Injection via the 'file_to_delete' parameter in all versions up to, and including, 1.4.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2025-2694	IBM Sterling B2B Integrator 6.0.0.0 through 6.1.2.7_1 and 6.2.0.0 through 6.2.0.4 and IBM Sterling File Gateway 6.0.0.0 through 6.1.2.7_1 and 6.2.0.0 through 6.2.0.4 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	4.8	More Details
CVE-2025-54101	Use after free in Windows SMBv3 Client allows an authorized attacker to execute code over a network.	4.8	More Details
CVE-2025-20280	A vulnerability in the web-based management interface of Cisco Evolved Programmable Network Manager (EPNM) and Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against users of the interface of an affected system. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious code into specific data fields in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, an attacker must have valid administrative credentials.	4.8	More Details
CVE-2025-39523	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in GoodBarber GoodBarber. This issue affects GoodBarber: from n/a through 1.0.26.	4.7	More Details
CVE-2025-10107	A vulnerability has been found in TRENDnet TEW-831DR 1.0 (601.130.1.1410). Impacted is an unknown function of the file /boafrm/formSysCmd. The manipulation of the argument sysHost leads to command injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-10122	A vulnerability was found in Maccms10 2025.1000.4050. Affected is the function rep of the file application/admin/controller/Database.php. Performing manipulation of the argument where results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	4.7	More Details
CVE-2025-0034	Insufficient parameter sanitization in TEE SOC Driver could allow an attacker to issue a malformed DRV_SOC_CMD_ID_SRIOV_SPATIAL_PART and cause read or write past the end of allocated arrays, potentially resulting in a loss of platform integrity or denial of service.	4.7	More Details
CVE-2025-48395	An attacker with authenticated and privileged access could modify the contents of a non-sensitive file by traversing the path in the limited shell of the CLI. This security issue has been fixed in the latest version of NMC G2 which is available on the Eaton download center.	4.7	More Details
CVE-2024-13073	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Akinsoft TaskPano allows Cross-Site Scripting (XSS).This issue affects TaskPano: s1.06.04.	4.7	More Details
CVE-2025-0878	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Akinsoft LimonDesk allows Cross-Site Scripting (XSS).This issue affects LimonDesk: from s1.02.14 before v1.02.17.	4.7	More Details
CVE-2025-10087	A security vulnerability has been detected in SourceCodester Pet Grooming Management Software 1.0. Impacted is an unknown function of the file /admin/profit_report.php. Such manipulation of the argument product_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	4.7	More Details
CVE-2025-9920	A security flaw has been discovered in Campcodes Recruitment Management System 1.0. This impacts the function include of the file /admin/index.php. The manipulation of the argument page results in file inclusion. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	4.7	More Details
CVE-2025-53791	Improper access control in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature over a network.	4.7	More Details
CVE-2025-10081	A flaw has been found in SourceCodester Pet Management System 1.0. This impacts an unknown function of the file /admin/profile.php. This manipulation of the argument website_image causes unrestricted upload. Remote exploitation of the attack is possible. The exploit has been published and may be used.	4.7	More Details
CVE-2023-21467	Error in 3GPP specification implementation in Exynos baseband prior to SMR Apr-2023 Release 1 allows incorrect handling of unencrypted message.	4.6	More Details

CVE-2025-56689	One Identity by Quest Safeguard for Privileged Passwords Appliance 7.5.1.20903 is vulnerable to One Time Password (OTP)/Multifactor Authentication (MFA) bypass using response manipulation. An attacker who intercepts or captures a valid OTP response can bypass the OTP verification step by replaying the same response.	4.6	More Details
CVE-2025-21035	Improper access control in Samsung Calendar prior to version 12.5.06.5 in Android 14 and 12.6.01.12 in Android 15 allows physical attackers to access data across multiple user profiles.	4.6	More Details
CVE-2025-26420	In multiple functions of GrantPermissionsActivity.java , there is a possible way to trick the user into granting the incorrect permission due to permission overload. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	4.4	More Details
CVE-2025-59044	Himmelblau is an interoperability suite for Microsoft Azure Entra ID and Intune. Himmelblau 0.9.x derives numeric GIDs for Entra ID groups from the group display name when himmelblau.conf `id_attr_map = name` (the default configuration). Because Microsoft Entra ID allows multiple groups with the same `displayName` (including end-user–created personal/O365 groups, depending on tenant policy), distinct directory groups can collapse to the same numeric GID on Linux. This issue only applies to Himmelblau versions 0.9.0 through 0.9.22. Any resource or service on a Himmelblau-joined host that enforces authorization by numeric GID (files/dirs, etc.) can be unintentionally accessible to a user who creates or joins a different Entra/O365 group that happens to share the same `displayName` as a privileged security group. Users should upgrade to 0.9.23, or 1.0.0 or later, to receive a patch. Group to GID mapping now uses Entra ID object IDs (GUIDs) and does not collide on same-name groups. As a workaround, use tenant policy hardening to restrict arbitrary group creation until all hosts are patched.	4.4	More Details
CVE-2025-26427	In multiple locations, there is a possible Android/data access due to a path traversal error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	4.4	More Details
CVE-2024-21970	Improper validation of an array index in the AND power Management Firmware could allow a privileged attacker to corrupt AGESA memory potentially leading to a loss of integrity.	4.4	More Details
CVE-2025-58615	Server-Side Request Forgery (SSRF) vulnerability in gfazioli WP Bannerize Pro allows Server Side Request Forgery. This issue affects WP Bannerize Pro: from n/a through 1.10.0.	4.4	More Details
CVE-2025-21030	Improper handling of insufficient permission in AppPrelaunchManagerService prior to SMR Sep-2025 Release 1 in Chinese Android 15 allows local attackers to execute arbitrary application in the background.	4.3	More Details
CVE-2025-49461	Cross-site scripting in certain Zoom Workplace Clients may allow an unauthenticated user to conduct a denial of service via network access.	4.3	More Details
CVE-2025-49460	Uncontrolled resource consumption in certain Zoom Workplace Clients may allow an unauthenticated user to conduct a denial of service via network access.	4.3	More Details
CVE-2025-8944	The OceanWP WordPress theme before 4.1.2 is vulnerable to an option update due to a missing capability check on one of its AJAX request handler, allowing any authenticated users, such as subscriber to update the darkMod` setting.	4.3	More Details
CVE-2025-36011	IBM Jazz for Service Management 1.1.3.0 through 1.1.3.24 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic.	4.3	More Details
CVE-2025-55052	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	4.3	More Details
CVE-2025-59005	Missing Authorization vulnerability in frenify Categorify allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Categorify: from n/a through 1.0.7.5.	4.3	More Details
CVE-2025-58783	Missing Authorization vulnerability in gutentor Gutentor allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Gutentor: from n/a through 3.5.1.	4.3	More Details
CVE-2024-13064	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Akinsoft MyRezzta allows Cross-Site Scripting (XSS).This issue affects MyRezzta: from s2.02.02 before v2.05.01.	4.3	More Details
CVE-2025-9219	The Post SMTP – WP SMTP Plugin with Email Logs and Mobile App for Failure Notifications – Gmail SMTP, Office 365, Brevo, Mailgun, Amazon SES and more plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_post_smtp_pro_option_callback' function in all versions up to, and including, 3.4.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to	4.3	More Details

	enable pro extensions.		
CVE-2025-58976	Missing Authorization vulnerability in Equalize Digital Accessibility Checker by Equalize Digital allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Accessibility Checker by Equalize Digital: from n/a through 1.31.0.	4.3	More Details
CVE-2025-58975	Cross-Site Request Forgery (CSRF) vulnerability in Helmut Wandl Advanced Settings allows Cross Site Request Forgery. This issue affects Advanced Settings: from n/a through 3.1.1.	4.3	More Details
CVE-2025-10084	A vulnerability was identified in elunez eladmin up to 2.7. This affects the function queryErrorLogDetail of the file /api/logs/error/1 of the component SysLogController. The manipulation leads to improper authorization. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	4.3	More Details
CVE-2024-13066	Improper Restriction of Rendered UI Layers or Frames vulnerability in Akinsoft LimonDesk allows iFrame Overlay, CAPEC - 103 - Clickjacking.This issue affects LimonDesk: from s1.02.14 before v1.02.17.	4.3	More Details
CVE-2025-58134	Incorrect authorization in certain Zoom Workplace Clients for Windows may allow an authenticated user to conduct an impact to integrity via network access.	4.3	More Details
CVE-2025-58792	Cross-Site Request Forgery (CSRF) vulnerability in WPKube Authors List allows Cross Site Request Forgery. This issue affects Authors List: from n/a through 2.0.6.1.	4.3	More Details
CVE-2022-39888	Improper access control vulnerability in retrieveExternalProxy in MiscPolicy prior to SMR Nov-2022 Release 1 allows local attacker to access to Proxy information.	4.3	More Details
CVE-2025-58794	Cross-Site Request Forgery (CSRF) vulnerability in rainafarai Notification for Telegram allows Cross Site Request Forgery. This issue affects Notification for Telegram: from n/a through 3.4.6.	4.3	More Details
CVE-2025-58798	Cross-Site Request Forgery (CSRF) vulnerability in Bjorn Manintveld BCM Duplicate Menu allows Cross Site Request Forgery. This issue affects BCM Duplicate Menu: from n/a through 1.1.2.	4.3	More Details
CVE-2025-58799	Cross-Site Request Forgery (CSRF) vulnerability in themelocation Custom WooCommerce Checkout Fields Editor allows Cross Site Request Forgery. This issue affects Custom WooCommerce Checkout Fields Editor: from n/a through 1.3.4.	4.3	More Details
CVE-2025-58800	Cross-Site Request Forgery (CSRF) vulnerability in Steve Truman WP Email Template allows Cross Site Request Forgery. This issue affects WP Email Template: from n/a through 2.8.3.	4.3	More Details
CVE-2025-27003	Cross-Site Request Forgery (CSRF) vulnerability in fullworks Quick Paypal Payments allows Cross Site Request Forgery. This issue affects Quick Paypal Payments: from n/a through 5.7.46.	4.3	More Details
CVE-2025-58802	Cross-Site Request Forgery (CSRF) vulnerability in michalzagdan TrustMate.io – WooCommerce integration allows Cross Site Request Forgery. This issue affects TrustMate.io – WooCommerce integration: from n/a through 1.14.0.	4.3	More Details
CVE-2025-58804	Cross-Site Request Forgery (CSRF) vulnerability in brijrajs WooCommerce Single Page Checkout allows Cross Site Request Forgery. This issue affects WooCommerce Single Page Checkout: from n/a through 1.2.7.	4.3	More Details
CVE-2025-58813	Missing Authorization vulnerability in ThemeArile Consultstreet allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Consultstreet: from n/a through 3.0.0.	4.3	More Details
CVE-2025-42925	Due to the lack of randomness in assigning Object Identifiers in the SAP NetWeaver AS JAVA IIOP service, an authenticated attacker with low privileges could predict the identifiers by conducting a brute force search. By leveraging knowledge of several identifiers generated close to the same time, the attacker could determine a desired identifier which could enable them to access limited system information. This poses a low risk to confidentiality without impacting the integrity or availability of the service.	4.3	More Details
CVE-2025-42923	Due to insufficient CSRF protection in SAP Fiori App Manage Work Center Groups, an authenticated user could be tricked by an attacker to send unintended request to the web server. This has low impact on integrity and no impact on confidentiality and availability of the application.	4.3	More Details
CVE-2025-42918	SAP NetWeaver Application Server for ABAP allows authenticated users with access to background processing to gain unauthorized read access to profile parameters. This results in a low impact on confidentiality, with no impact on integrity or availability	4.3	More Details
CVE-2025-	Missing Authorization vulnerability in DesertThemes SoftMe allows Exploiting Incorrectly Configured Access Control	4.3	More

58817	Security Levels. This issue affects SoftMe: from n/a through 1.1.24.		Details
CVE-2025-58824	Missing Authorization vulnerability in webriti Shk Corporate allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Shk Corporate: from n/a through 2.4.1.1.	4.3	More Details
CVE-2025-58831	Cross-Site Request Forgery (CSRF) vulnerability in snagysandor Parallax Scrolling Enllax.js allows Cross Site Request Forgery. This issue affects Parallax Scrolling Enllax.js: from n/a through 0.0.6.	4.3	More Details
CVE-2025-3701	Missing Authorization vulnerability in Malcure Web Security Malcure Malware Scanner allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Malcure Malware Scanner: from n/a through 16.8.	4.3	More Details
CVE-2025-58458	In Jenkins Git client Plugin 6.3.2 and earlier, except 6.1.4 and 6.2.1, Git URL field form validation responses differ based on whether the specified file path exists on the controller when specifying `amazon-s3` protocol for use with JGit, allowing attackers with Overall/Read permission to check for the existence of an attacker-specified file path on the Jenkins controller file system.	4.3	More Details
CVE-2025-20287	A vulnerability in the web-based management interface of Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to upload arbitrary files to an affected device. This vulnerability is due to improper validation of files that are uploaded to the web-based management interface. An attacker could exploit this vulnerability by sending a crafted file upload request to a specific API endpoint. A successful exploit could allow the attacker to upload arbitrary files to an affected system. To exploit this vulnerability, an attacker must have at least valid Config Managers credentials on the affected device.	4.3	More Details
CVE-2025-58459	Jenkins global-build-stats Plugin 322.v22f4db_18e2dd and earlier does not perform permission checks in its REST API endpoints, allowing attackers with Overall/Read permission to enumerate graph IDs.	4.3	More Details
CVE-2025-9936	A vulnerability was identified in fuyang_lipengjun platform 1.0.0. This issue affects the function AdController of the file /ad/queryAll. The manipulation leads to improper authorization. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	4.3	More Details
CVE-2025-9931	A vulnerability was detected in Jinher OA 1.0. Affected is an unknown function of the file /jc6/platform/sys/login!changePassWord.action of the component POST Request Handler. The manipulation of the argument Account results in cross site scripting. The attack can be launched remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2025-39553	Missing Authorization vulnerability in andy_moyle Church Admin. This issue affects Church Admin: from n/a through 5.0.9.	4.3	More Details
CVE-2025-10032	A vulnerability was detected in Campcodes Grocery Sales and Inventory System 1.0. The affected element is an unknown function of the file /index.php. The manipulation of the argument page results in cross site scripting. The attack can be executed remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2024-13071	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Akinsoft e-Mutabakat allows Cross-Site Scripting (XSS).This issue affects e-Mutabakat: from 2.02.05 before v2.02.06.	4.3	More Details
CVE-2025-9923	A flaw has been found in Campcodes Sales and Inventory System 1.0. This affects an unknown part of the file /index.php. Executing manipulation of the argument page can lead to cross site scripting. The attack may be launched remotely. The exploit has been published and may be used.	4.3	More Details
CVE-2025-20326	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) Software and Cisco Unified CM Session Management Edition (SME) Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user.	4.3	More Details
CVE-2025-10063	A vulnerability was identified in itsourcecode POS Point of Sale System 1.0. This vulnerability affects unknown code of the file /inventory/main/vendors/datatables/unit_testing/templates/deferred_table.php. The manipulation of the argument scripts leads to cross site scripting. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	4.3	More Details
CVE-2025-10064	A security flaw has been discovered in itsourcecode POS Point of Sale System 1.0. This issue affects some unknown processing of the file /inventory/main/vendors/datatables/unit_testing/templates/dom_data_two_headers.php. The manipulation of the argument scripts results in cross site scripting. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	4.3	More Details
CVE-2025-10065	A weakness has been identified in itsourcecode POS Point of Sale System 1.0. Impacted is an unknown function of the file /inventory/main/vendors/datatables/unit_testing/templates/dom_data_th.php. This manipulation of the argument scripts causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been	4.3	More Details

	made available to the public and could be exploited.		
CVE-2025-10066	A security vulnerability has been detected in itsourcecode POS Point of Sale System 1.0. The affected element is an unknown function of the file /inventory/main/vendors/datatables/unit_testing/templates/dymanic_table.php. Such manipulation of the argument scripts leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2025-20291	A vulnerability in Cisco Webex Meetings could have allowed an unauthenticated, remote attacker to redirect a targeted Webex Meetings user to an untrusted website. Cisco has addressed this vulnerability in the Cisco Webex Meetings service, and no customer action is needed. This vulnerability existed because of insufficient validation of URLs that were included in a meeting-join URL. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by including a URL to a website of their choosing in a specific value of a Cisco Webex Meetings join URL. A successful exploit could have allowed the attacker to redirect a targeted user to a website that was controlled by the attacker, possibly making the user more likely to believe the website was trusted by Webex and perform additional actions as part of phishing attacks.	4.3	More Details
CVE-2025-10067	A vulnerability was detected in itsourcecode POS Point of Sale System 1.0. The impacted element is an unknown function of the file /inventory/main/vendors/datatables/unit_testing/templates/empty_table.php. Performing manipulation of the argument scripts results in cross site scripting. It is possible to initiate the attack remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2025-54107	Improper resolution of path equivalence in Windows MapUrlToZone allows an unauthorized attacker to bypass a security feature over a network.	4.3	More Details
CVE-2025-20270	A vulnerability in the web-based management interface of Cisco Evolved Programmable Network Manager (EPNM) and Cisco Prime Infrastructure could allow an authenticated, remote attacker to obtain sensitive information from an affected system. This vulnerability is due to improper validation of requests to API endpoints. An attacker could exploit this vulnerability by sending a valid request to a specific API endpoint within the affected system. A successful exploit could allow a low-privileged user to view sensitive configuration information on the affected system that should be restricted. To exploit this vulnerability, an attacker must have access as a low-privileged user.	4.3	More Details
CVE-2025-58865	Cross-Site Request Forgery (CSRF) vulnerability in reimund Compact Admin allows Cross Site Request Forgery. This issue affects Compact Admin: from n/a through 1.3.0.	4.3	More Details
CVE-2025-9922	A security vulnerability has been detected in Campcodes Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /index.php. Such manipulation of the argument page leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2025-58594	Missing Authorization vulnerability in themefusecom Brizy allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Brizy: from n/a through 2.7.12.	4.3	More Details
CVE-2025-54917	Protection mechanism failure in Windows MapUrlToZone allows an unauthorized attacker to bypass a security feature over a network.	4.3	More Details
CVE-2025-58597	Authorization Bypass Through User-Controlled Key vulnerability in Tomdever wpForo Forum allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects wpForo Forum: from n/a through 2.4.6.	4.3	More Details
CVE-2025-58599	Missing Authorization vulnerability in tychesoftwares Order Delivery Date for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Order Delivery Date for WooCommerce: from n/a through 4.1.0.	4.3	More Details
CVE-2025-10073	A vulnerability was determined in Portabilis i-Educar up to 2.10. Impacted is an unknown function of the file /module/Api/turma. Executing manipulation can lead to improper authorization. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	4.3	More Details
CVE-2025-58601	Missing Authorization vulnerability in RadiusTheme Classified Listing allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Classified Listing: from n/a through 5.0.6.	4.3	More Details
CVE-2025-58611	Cross-Site Request Forgery (CSRF) vulnerability in Tickera Tickera allows Cross Site Request Forgery. This issue affects Tickera: from n/a through 3.5.5.6.	4.3	More Details
CVE-2025-58617	Missing Authorization vulnerability in FAKTOR VIER F4 Media Taxonomies allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects F4 Media Taxonomies: from n/a through 1.1.4.	4.3	More Details
CVE-2025-58622	Missing Authorization vulnerability in yydevelopment Mobile Contact Line allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Mobile Contact Line: from n/a through 2.4.0.	4.3	More Details

CVE-2025-10044	A flaw was found in Keycloak. Keycloak's account console and other pages accept arbitrary text in the error_description query parameter. This text is directly rendered in error pages without validation or sanitization. While HTML encoding prevents XSS, an attacker can craft URLs with misleading messages (e.g., fake support phone numbers or URLs), which are displayed within the trusted Keycloak UI. This creates a phishing vector, potentially tricking users into contacting malicious actors.	4.3	More Details
CVE-2025-54251	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by an XML Injection vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to manipulate XML queries and gain limited unauthorized write access.	4.3	More Details
CVE-2025-56760	When Memos 0.22 is configured to store objects locally, an attacker can create a file via the CreateResource endpoint containing a path traversal sequence in the name, allowing arbitrary file write on the server.	4.3	More Details
CVE-2025-58460	A missing permission check in Jenkins OpenTelemetry Plugin 3.1543.v8446b_92b_cd64 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	4.2	More Details
CVE-2025-23301	NVIDIA HGX and DGX contain a vulnerability where a misconfiguration of the VBIOS could enable an attacker to set an unsafe debug access level. A successful exploit of this vulnerability might lead to denial of service.	4.2	More Details
CVE-2025-56608	The SourceCodester Android application "Corona Virus Tracker App India" 1.0 uses MD5 for digest authentication in `OkHttpClientWrapper.java`. The `handleDigest()` function employs `MessageDigest.getInstance("MD5")` to hash credentials. MD5 is a broken cryptographic algorithm known to allow hash collisions. This makes the authentication mechanism vulnerable to replay, spoofing, or brute-force attacks, potentially leading to unauthorized access. The vulnerability corresponds to CWE-327 and aligns with OWASP M5: Insufficient Cryptography and MASVS MSTG-CRYPTO-4.	4.2	More Details
CVE-2025-23302	NVIDIA HGX and DGX contain a vulnerability where a misconfiguration of the LS10 could enable an attacker to set an unsafe debug access level. A successful exploit of this vulnerability might lead to denial of service.	4.2	More Details
CVE-2021-26377	Insufficient parameter validation while allocating process space in the Trusted OS (TOS) may allow for a malicious userspace process to trigger an integer overflow, leading to a potential denial of service.	4.1	More Details
CVE-2025-21037	Improper access control in Samsung Notes prior to version 4.4.30.63 allows physical attackers to access data across multiple user profiles. User interaction is required for triggering this vulnerability.	4.1	More Details
CVE-2025-21026	Improper handling of insufficient permission in ImsService prior to SMR Sep-2025 Release 1 allows local attackers to interrupt the call.	4.0	More Details
CVE-2024-49731	In apk-versions.txt, there is a possible corruption of telemetry opt-in settings on other watches when setting up a new Pixel Watch due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	4.0	More Details
CVE-2025-21029	Improper handling of insufficient permission in System UI prior to SMR Sep-2025 Release 1 allows local attackers to send arbitrary replies to messages from the cover display.	4.0	More Details
CVE-2025-54255	Acrobat Reader versions 24.001.30254, 20.005.30774, 25.001.20672 and earlier are affected by a Violation of Secure Design Principles vulnerability that could result in a security feature bypass. Exploitation of this issue does not require user interaction, and scope is unchanged.	4.0	More Details
CVE-2025-21034	Out-of-bounds write in libsavsvc.so prior to SMR Sep-2025 Release 1 allows local attackers to potentially execute arbitrary code.	4.0	More Details
CVE-2024-49739	In MMapVAccess of pmr_os.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	4.0	More Details
CVE-2025-26425	In multiple functions of RoleService.java, there is a possible permission squatting vulnerability due to a logic error in the code. This could lead to local escalation of privilege on versions of Android where android.permission.MANAGE_DEFAULT_APPLICATIONS was not defined with no additional execution privileges needed. User interaction is not needed for exploitation.	4.0	More Details
CVE-2025-26421	In multiple locations, there is a possible lock screen bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	4.0	More Details
CVE-2023-35657	In bta_av_config_ind of bta_av_aact.cc, there is a possible out of bounds read due to type confusion. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	4.0	More Details

CVE-2025-0077	In multiple functions of UserController.java, there is a possible lock screen bypass due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	4.0	More Details
CVE-2025-48528	In multiple locations, there is a possible way to overlay biometrics due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	4.0	More Details
CVE-2025-48526	In createMultiProfilePagerAdapter of ChooserActivity.java , there is a possible way for an app to launch the ChooserActivity in another profile due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	4.0	More Details
CVE-2023-21469	Improper access control vulnerability in SLocation prior to SMR Apr-2022 Release 1 allows local attackers to get device location information using com.samsung.android.wifi.GEOFENCE action.	4.0	More Details
CVE-2023-21470	Improper access control vulnerability in SLocation prior to SMR Apr-2022 Release 1 allows local attackers to get device location information using com.samsung.android.wifi.NETWORK_LOCATION action.	4.0	More Details
CVE-2023-21471	Improper access control vulnerability in SemClipboard prior to SMR Apr-2023 Release 1 allows attackers to read arbitrary files with system permission.	4.0	More Details
CVE-2025-26422	In dump of WindowManagerService.java, there is a possible way of running dumpsys without the required permission due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	4.0	More Details
CVE-2025-21033	Improper access control in ContactProvider prior to SMR Sep-2025 Release 1 allows local attackers to access sensitive information.	4.0	More Details
CVE-2025-26424	In multiple functions of VpnManager.java, there is a possible cross-user data leak due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	4.0	More Details
CVE-2025-22415	In android_app of Android.bp, there is a possible way to launch any activity as a system user. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	4.0	More Details
CVE-2023-31365	An integer overflow in the SMU could allow a privileged attacker to potentially write memory beyond the end of the reserved dRAM area resulting in loss of integrity or availability.	3.9	More Details
CVE-2025-57807	ImageMagick is free and open-source software used for editing and manipulating digital images. ImageMagick versions lower than 14.8.2 include insecure functions: SeekBlob(), which permits advancing the stream offset beyond the current end without increasing capacity, and WriteBlob(), which then expands by quantum + length (amortized) instead of offset + length, and copies to data + offset. When offset ≫ extent, the copy targets memory beyond the allocation, producing a deterministic heap write on 64-bit builds. No 2^{64} arithmetic wrap, external delegates, or policy settings are required. This is fixed in version 14.8.2.	3.8	More Details
CVE-2025-58827	Improper Control of Generation of Code ('Code Injection') vulnerability in PickPlugins Job Board Manager allows Code Injection. This issue affects Job Board Manager: from n/a through 2.1.61.	3.8	More Details
CVE-2025-51586	An issue was discoverd in file controllers/admin/AdminLoginController.php in PrestaShop before 8.2.1 allowing attackers to gain sensitive information via the reset password feature.	3.7	More Details
CVE-2025-7039	A flaw was found in glib. An integer overflow during temporary file creation leads to an out-of-bounds memory access, allowing an attacker to potentially perform path traversal or access private temporary file content by creating symbolic links. This vulnerability allows a local attacker to manipulate file paths and access unauthorized data. The core issue stems from insufficient validation of file path lengths during temporary file operations.	3.7	More Details
CVE-2024-48341	dingfanzu CMS V1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/doAdminAction.php?act=addShop	3.7	More Details
CVE-2025-10117	A weakness has been identified in SourceCodester Simple To-Do List System 1.0. Impacted is an unknown function of the file /fetch_tasks.php of the component Add New Task. Executing manipulation with the input <script>alert('XSS')</script> can lead to cross site scripting. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.	3.5	More Details
CVE-2025-10026	A vulnerability was found in itsourcecode POS Point of Sale System 1.0. Affected by this vulnerability is an unknown functionality of the file /inventory/main/vendors/datatables/unit_testing/templates/-complex_header.php. The manipulation of the argument scripts results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used.	3.5	More Details

CVE-2025-58816	Missing Authorization vulnerability in Plugin Devs Product Carousel Slider for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Product Carousel Slider for Elementor: from n/a through 2.1.3.	3.5	More Details
CVE-2025-9940	A vulnerability was detected in CodeAstro Real Estate Management System 1.0. This affects an unknown function of the file /feature.php. Performing manipulation of the argument msg results in cross site scripting. The attack can be initiated remotely. The exploit is now public and may be used.	3.5	More Details
CVE-2025-9845	A vulnerability has been found in code-projects Fruit Shop Management System 1.0. Affected by this vulnerability is an unknown functionality of the file products.php. Such manipulation of the argument product_code/gen_name/product_name/supplier leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-10028	A vulnerability was identified in itsourcecode POS Point of Sale System 1.0. This affects an unknown part of the file /inventory/main/vendors/datatables/unit_testing/templates/6776.php. Such manipulation of the argument scripts leads to cross site scripting. The attack can be launched remotely. The exploit is publicly available and might be used.	3.5	More Details
CVE-2025-10075	A security flaw has been discovered in SourceCodester Online Polling System 1.0. The impacted element is an unknown function of the file /manage-profile.php. The manipulation of the argument firstname results in cross site scripting. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	3.5	More Details
CVE-2025-10029	A security flaw has been discovered in itsourcecode POS Point of Sale System 1.0. This vulnerability affects unknown code of the file /inventory/main/vendors/datatables/unit_testing/templates/complex_header_2.php. Performing manipulation of the argument scripts results in cross site scripting. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	3.5	More Details
CVE-2025-10074	A vulnerability was identified in Portabilis i-Educar up to 2.10. The affected element is an unknown function of the file /usuarios/tipos/. The manipulation of the argument Tipos de Usuário/Descrição leads to cross site scripting. The attack can be initiated remotely. The exploit is publicly available and might be used.	3.5	More Details
CVE-2025-9939	A security vulnerability has been detected in CodeAstro Real Estate Management System 1.0. The impacted element is an unknown function of the file /propertyview.php. Such manipulation of the argument msg leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	3.5	More Details
CVE-2025-10027	A vulnerability was determined in itsourcecode POS Point of Sale System 1.0. Affected by this issue is some unknown functionality of the file /inventory/main/vendors/datatables/unit_testing/templates/2512.php. This manipulation of the argument scripts causes cross site scripting. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	3.5	More Details
CVE-2025-10088	A vulnerability was detected in SourceCodester Time Tracker 1.0. The affected element is an unknown function of the file /index.html. Performing manipulation of the argument project-name results in cross site scripting. The attack may be initiated remotely. The exploit is now public and may be used.	3.5	More Details
CVE-2025-42927	SAP NetWeaver AS Java application uses Adobe Document Service, installed with a vulnerable version of OpenSSL.Successful exploitation of known vulnerabilities in the outdated OpenSSL library would allow user with high system privileges to access and modify system information.This vulnerability has a low impact on confidentiality and integrity, with no impact on availability.	3.4	More Details
CVE-2023-3666	The Sticky Side Buttons WordPress plugin before 2.0.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	3.3	More Details
CVE-2025-0011	Improper removal of sensitive information before storage or transfer in AMD Crash Defender could allow an attacker to obtain kernel address information potentially resulting in loss of confidentiality.	3.3	More Details
CVE-2025-26461	In Permission Manager, there is a possible way for the microphone privacy indicator to remain activated even after the user attempts to close the app due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2023-20516	Improper handling of insufficiency privileges in the ASP could allow a privileged attacker to modify Translation Map Registers (TMRs) potentially resulting in loss of confidentiality or integrity.	3.3	More Details
CVE-2025-0076	In multiple locations, there is a possible way to view icons belonging to another user due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2023-31306	Improper validation of an array index in the AMD graphics driver software could allow an attacker to pass malformed arguments to the dynamic power management (DPM) functions resulting in an out of bounds read and loss of availability.	3.3	More Details
CVE-2025-26419	In initPhoneSwitch of SystemSettingsFragment.java, there is a possible FRP bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	3.3	More Details

CVE-2025-26428	In startLockTaskMode of LockTaskController.java, there is a possible lock screen bypass due to a logic error in the code. This could lead to physical escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	3.2	More Details
CVE-2024-36331	Improper initialization of CPU cache memory could allow a privileged attacker with hypervisor access to overwrite SEV-SNP guest memory resulting in loss of data integrity.	3.2	More Details
CVE-2024-21977	Incomplete cleanup after loading a CPU microcode patch may allow a privileged attacker to degrade the entropy of the RDRAND instruction, potentially resulting in loss of integrity for SEV-SNP guests.	3.2	More Details
CVE-2025-40802	A vulnerability has been identified in RUGGEDCOM RST2428P (6GK6242-6PA00) (All versions). The affected device may be susceptible to resource exhaustion when subjected to high volumes of query requests. This could allow an attacker to cause a temporary denial of service, with the system recovering once the activity stops.	3.1	More Details
CVE-2025-42914	Due to missing authorization checks, SAP HCM My Timesheet Fiori 2.0 application allows an authenticated attacker with in-depth system knowledge to escalate privileges and perform activities that are otherwise restricted, resulting in a low impact on the integrity of the application. Confidentiality and availability are not impacted.	3.1	More Details
CVE-2025-42913	Due to missing authorization checks, SAP HCM My Timesheet Fiori 2.0 application allows an authenticated attacker with in-depth system knowledge to escalate privileges and perform activities that are otherwise restricted, resulting in a low impact on the integrity of the application. Confidentiality and availability are not impacted.	3.1	More Details
CVE-2025-40803	A vulnerability has been identified in RUGGEDCOM RST2428P (6GK6242-6PA00) (All versions). The affected device exposes certain non-critical information from the device. This could allow an unauthenticated attacker to access sensitive data, potentially leading to a breach of confidentiality.	3.1	More Details
CVE-2025-10080	A vulnerability has been found in running-elephant Datart up to 1.0.0-rc3. Affected by this issue is the function getTokensecret of the file datart/security/src/main/java/datart/security/util/AESUtil.java of the component API. The manipulation leads to use of hard-coded cryptographic key . The attack is possible to be carried out remotely. The attack is considered to have high complexity. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used.	3.1	More Details
CVE-2025-8277	A flaw was found in libssh's handling of key exchange (KEX) processes when a client repeatedly sends incorrect KEX guesses. The library fails to free memory during these rekey operations, which can gradually exhaust system memory. This issue can lead to crashes on the client side, particularly when using libgcrypt, which impacts application stability and availability.	3.1	More Details
CVE-2025-10014	A flaw has been found in elunez eladmin up to 2.7. This impacts the function updateUserEmail of the file /api/users/updateEmail/ of the component Email Address Handler. Executing manipulation of the argument id/email can lead to improper authorization. The attack may be performed from remote. Attacks of this nature are highly complex. The exploitability is said to be difficult. The exploit has been published and may be used. It is required to know the RSA-encrypted password of the attacked user account.	3.1	More Details
CVE-2021-46750	Failure to validate the address and size in TEE (Trusted Execution Environment) may allow a malicious x86 attacker to send malformed messages to the graphics mailbox resulting in an overlap of a TMR (Trusted Memory Region) that was previously allocated by the ASP bootloader leading to a potential loss of integrity.	3.0	More Details
CVE-2023-31326	Use of an uninitialized variable in the ASP could allow an attacker to access leftover data from a trusted execution environment (TEE) driver, potentially leading to loss of confidentiality.	2.8	More Details
CVE-2025-2667	IBM Sterling B2B Integrator 6.0.0.0 through 6.1.2.7_1 and 6.2.0.0 through 6.2.0.4 and IBM Sterling File Gateway 6.0.0.0 through 6.1.2.7_1 and 6.2.0.0 through 6.2.0.4 could disclose sensitive system information about the server to a privileged user that could aid in further attacks against the system.	2.7	More Details
CVE-2025-58866	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Rami Yushuvaev Site Info allows Retrieve Embedded Sensitive Data. This issue affects Site Info: from n/a through 1.1.	2.7	More Details
CVE-2025-9821	SummaryUsers with webhook permissions can conduct SSRF via webhooks. If they have permission to view the webhook logs, the (partial) request response is also disclosed DetailsWhen sending webhooks, the destination is not validated, causing SSRF. ImpactBypass of firewalls to interact with internal services. See https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/ for more potential impact. Resources https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html for more information on SSRF and its fix.	2.7	More Details
CVE-2025-10043	A path traversal validation flaw exists in Keycloak’s vault key handling on Windows. The previous fix for CVE-2024-10492 did not account for the Windows file separator (\). As a result, a high-privilege administrator could probe for the existence of files outside the expected realm context through crafted vault secret lookups. This is a platform-specific variant/incomplete fix of CVE-2024-10492.	2.7	More Details
CVE-2023-	An out-of-bounds read in the ASP could allow a privileged attacker with access to a malicious bootloader to potentially read sensitive memory resulting in loss of confidentiality.	2.5	More Details

31330			
CVE-2025-9921	A weakness has been identified in code-projects POS Pharmacy System 1.0. Affected is an unknown function of the file /main/products.php. This manipulation of the argument product_code/gen_name/product_name/supplier causes cross site scripting. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	2.4	More Details
CVE-2025-9929	A weakness has been identified in code-projects Responsive Blog Site 1.0. This affects an unknown function of the file blogs_view.php. Executing manipulation of the argument product_code/gen_name/product_name/supplier can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited.	2.4	More Details
CVE-2025-10099	A weakness has been identified in Portabilis i-Educar up to 2.10. Affected by this vulnerability is an unknown functionality of the file /intranet/educar_usuario_cad.php of the component Editar usuário Page. This manipulation of the argument email/data_inicial/data_expiracao causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.	2.4	More Details
CVE-2025-39696	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda: tas2781: Fix wrong reference of tasdevice_priv During the conversion to unify the calibration data management, the reference to tasdevice_priv was wrongly set to h->hda_priv instead of h->priv. This resulted in memory corruption and crashes eventually. Unfortunately it's a void pointer, hence the compiler couldn't know that it's wrong.	N/A	More Details
CVE-2025-39697	In the Linux kernel, the following vulnerability has been resolved: NFS: Fix a race when updating an existing write After nfs_lock_and_join_requests() tests for whether the request is still attached to the mapping, nothing prevents a call to nfs_inode_remove_request() from succeeding until we actually lock the page group. The reason is that whoever called nfs_inode_remove_request() doesn't necessarily have a lock on the page group head. So in order to avoid races, let's take the page group lock earlier in nfs_lock_and_join_requests(), and hold it across the removal of the request in nfs_inode_remove_request().	N/A	More Details
CVE-2025-39698	In the Linux kernel, the following vulnerability has been resolved: io_uring/futex: ensure io_futex_wait() cleans up properly on failure The io_futex_data is allocated upfront and assigned to the io_kiocb async_data field, but the request isn't marked with REQ_F_ASYNC_DATA at that point. Those two should always go together, as the flag tells io_uring whether the field is valid or not. Additionally, on failure cleanup, the futex handler frees the data but does not clear ->async_data. Clear the data and the flag in the error path as well. Thanks to Trend Micro Zero Day Initiative and particularly ReDress for reporting this.	N/A	More Details
CVE-2025-57064	Tenda G3 v3.0br_V15.11.0.17 was discovered to contain a stack overflow in the bindDhcpIndex parameter in the modifyDhcpRule function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-57069	Tenda G3 v3.0br_V15.11.0.17 was discovered to contain a stack overflow in the pPppUser parameter in the getsinglepppuser function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-57540	A stored cross-site scripting (XSS) vulnerability exists in the WebAuthn Relying Party field within the Datacenter configuration of Proxmox Virtual Environment (PVE) 8.4. Authenticated users can inject JavaScript code that is later executed in the browsers of users who view the configuration page, enabling client-side attacks.	N/A	More Details
CVE-2025-57539	A stored cross-site scripting (XSS) vulnerability in the U2F Origin field of the Datacenter configuration in Proxmox Virtual Environment (PVE) 8.4 allows authenticated users to store malicious input. The payload is rendered unsafely in the Web UI and executed when viewed by other users, potentially leading to session hijacking or other attacks.	N/A	More Details
CVE-2025-57538	A stored cross-site scripting (XSS) vulnerability in the HTTP Proxy field within the Datacenter configuration panel of Proxmox Virtual Environment (PVE) 8.4 allows an authenticated user to inject malicious input. The input is stored and executed in the context of other users' browsers when they view the affected configuration page. This can lead to arbitrary JavaScript execution.	N/A	More Details
CVE-2025-57087	Tenda W30E V16.01.0.19 (5037) was discovered to contain a stack overflow in the countryCode parameter in the werlessAdvancedSet function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-57072	Tenda G3 v3.0br_V15.11.0.17 was discovered to contain a stack overflow in the staticRouteGateway parameter in the formSetStaticRoute function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-57070	Tenda G3 v3.0br_V15.11.0.17 was discovered to contain a stack overflow in the gstUp parameter in the guestWifiRuleRefresh function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-57071	Tenda G3 v3.0br_V15.11.0.17 was discovered to contain a stack overflow in the vpnUsers parameter in the formAddVpnUsers function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-39699	In the Linux kernel, the following vulnerability has been resolved: iommu/riscv: prevent NULL deref in iova_to_phys The riscv_iommu_pte_fetch() function returns either NULL for unmapped/never-mapped iova, or a valid leaf pte pointer that requires no further validation. riscv_iommu_iova_to_phys() failed to handle NULL returns. Prevent null	N/A	More Details

	pointer dereference in riscv_iommu_iova_to_phys(), and remove the pte validation.		
CVE-2025-57063	Tenda G3 v3.0br_V15.11.0.17 was discovered to contain a stack overflow in the portMappingIndex parameter in the formDelPortMapping function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-39709	In the Linux kernel, the following vulnerability has been resolved: media: venus: protect against spurious interrupts during probe Make sure the interrupt handler is initialized before the interrupt is registered. If the IRQ is registered before hfi_create(), it's possible that an interrupt fires before the handler setup is complete, leading to a NULL dereference. This error condition has been observed during system boot on Rb3Gen2.	N/A	More Details
CVE-2025-39711	In the Linux kernel, the following vulnerability has been resolved: media: ivsc: Fix crash at shutdown due to missing mei_cldev_disable() calls Both the ACE and CSI driver are missing a mei_cldev_disable() call in their remove() function. This causes the mei_cl client to stay part of the mei_device->file_list list even though its memory is freed by mei_cl_bus_dev_release() calling kfree(cldev->cl). This leads to a use-after-free when mei_vsc_remove() runs mei_stop() which first removes all mei bus devices calling mei_ace_remove() and mei_csi_remove() followed by mei_cl_bus_dev_release() and then calls mei_cl_all_disconnect() which walks over mei_device->file_list dereferecing the just freed cldev->cl. And mei_vsc_remove() it self is run at shutdown because of the platform_device_unregister(tp->pdev) in vsc_tp_shutdown() When building a kernel with KASAN this leads to the following KASAN report: [106.634504] == [106.634623] BUG: KASAN: slab-use-after-free in mei_cl_set_disconnected (drivers/misc/mei/client.c:783) mei [106.634683] Read of size 4 at addr ffff88819cb62018 by task systemd-shutdow/1 [106.634729] [106.634767] Tainted: [E]=UNSIGNED_MODULE [106.634770] Hardware name: Dell Inc. XPS 16 9640/09CK4V, BIOS 1.12.0 02/10/2025 [106.634773] Call Trace: [106.634777] <TASK> ... [106.634871] kasan_report (mm/kasan/report.c:221 mm/kasan/report.c:636) [106.634901] mei_cl_set_disconnected (drivers/misc/mei/client.c:783) mei [106.634921] mei_cl_all_disconnect (drivers/misc/mei/client.c:2165 (discriminator 4)) mei [106.634941] mei_reset (drivers/misc/mei/init.c:163) mei ... [106.635042] mei_stop (drivers/misc/mei/init.c:348) mei [106.635062] mei_vsc_remove (drivers/misc/mei/mei_dev.h:784 drivers/misc/mei/platform-vsc.c:393) mei_vsc [106.635066] platform_remove (drivers/base/platform.c:1424) Add the missing mei_cldev_disable() calls so that the mei_cl gets removed from mei_device->file_list before it is freed to fix this.	N/A	More Details
CVE-2025-39712	In the Linux kernel, the following vulnerability has been resolved: media: mt9m114: Fix deadlock in get_frame_interval/set_frame_interval Getting / Setting the frame interval using the V4L2 subdev pad ops get_frame_interval/set_frame_interval causes a deadlock, as the subdev state is locked in the [1] but also in the driver itself. In [2] it's described that the caller is responsible to acquire and release the lock in this case. Therefore, acquiring the lock in the driver is wrong. Remove the lock acquisitions/releases from mt9m114_ifp_get_frame_interval() and mt9m114_ifp_set_frame_interval(). [1] drivers/media/v4l2-core/v4l2-subdev.c - line 1129 [2] Documentation/driver-api/media/v4l2-subdev.rst	N/A	More Details
CVE-2025-39713	In the Linux kernel, the following vulnerability has been resolved: media: rainshadow-cec: fix TOCTOU race condition in rain_interrupt() In the interrupt handler rain_interrupt(), the buffer full check on rain->buf_len is performed before acquiring rain->buf_lock. This creates a Time-of-Check to Time-of-Use (TOCTOU) race condition, as rain->buf_len is concurrently accessed and modified in the work handler rain_irq_work_handler() under the same lock. Multiple interrupt invocations can race, with each reading buf_len before it becomes full and then proceeding. This can lead to both interrupts attempting to write to the buffer, incrementing buf_len beyond its capacity (DATA_SIZE) and causing a buffer overflow. Fix this bug by moving the spin_lock() to before the buffer full check. This ensures that the check and the subsequent buffer modification are performed atomically, preventing the race condition. An corresponding spin_unlock() is added to the overflow path to correctly release the lock. This possible bug was found by an experimental static analysis tool developed by our team.	N/A	More Details
CVE-2025-39714	In the Linux kernel, the following vulnerability has been resolved: media: usbtv: Lock resolution while streaming When an program is streaming (ffplay) and another program (qv4l2) changes the TV standard from NTSC to PAL, the kernel crashes due to trying to copy to unmapped memory. Changing from NTSC to PAL increases the resolution in the usbtv struct, but the video plane buffer isn't adjusted, so it overflows. [hverkuil: call vb2_is_busy instead of vb2_is_streaming]	N/A	More Details
CVE-2025-39715	In the Linux kernel, the following vulnerability has been resolved: parisc: Revise gateway LWS calls to probe user read access We use load and stbys,e instructions to trigger memory reference interruptions without writing to memory. Because of the way read access support is implemented, read access interruptions are only triggered at privilege levels 2 and 3. The kernel and gateway page execute at privilege level 0, so this code never triggers a read access interruption. Thus, it is currently possible for user code to execute a LWS compare and swap operation at an address that is read protected at privilege level 3 (PRIV_USER). Fix this by probing read access rights at privilege level 3 and branching to lws_fault if access isn't allowed.	N/A	More Details
CVE-2025-39716	In the Linux kernel, the following vulnerability has been resolved: parisc: Revise __get_user() to probe user read access Because of the way read access support is implemented, read access interruptions are only triggered at privilege levels 2 and 3. The kernel executes at privilege level 0, so __get_user() never triggers a read access interruption (code 26). Thus, it is currently possible for user code to access a read protected address via a system call. Fix this by probing read access rights at privilege level 3 (PRIV_USER) and setting __gu_err to -EFAULT (-14) if access isn't allowed. Note the cmpiclr instruction does a 32-bit compare because COND macro doesn't work inside asm.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: open_tree_attr: do not allow id-mapping changes		

CVE-2025-39717	without OPEN_TREE_CLONE As described in commit 7a54947e727b ('Merge patch series "fs: allow changing idmappings"'), open_tree_attr(2) was necessary in order to allow for a detached mount to be created and have its idmappings changed without the risk of any racing threads operating on it. For this reason, mount_setattr(2) still does not allow for id-mappings to be changed. However, there was a bug in commit 2462651ffa76 ("fs: allow changing idmappings") which allowed users to bypass this restriction by calling open_tree_attr(2) *without* OPEN_TREE_CLONE. can_idmap_mount() prevented this bug from allowing an attached mountpoint's id-mapping from being modified (thanks to an is_anon_ns() check), but this still allows for detached (but visible) mounts to have their be id-mapping changed. This risks the same UAF and locking issues as described in the merge commit, and was likely unintentional.	N/A	More Details
CVE-2025-39718	In the Linux kernel, the following vulnerability has been resolved: vsock/virtio: Validate length in packet header before skb_put() When receiving a vsock packet in the guest, only the virtqueue buffer size is validated prior to virtio_vsock_skb_rx_put(). Unfortunately, virtio_vsock_skb_rx_put() uses the length from the packet header as the length argument to skb_put(), potentially resulting in SKB overflow if the host has gone wonky. Validate the length as advertised by the packet header before calling virtio_vsock_skb_rx_put().	N/A	More Details
CVE-2025-39719	In the Linux kernel, the following vulnerability has been resolved: iio: imu: bno055: fix OOB access of hw_xlate array Fix a potential out-of-bounds array access of the hw_xlate array in bno055.c. In bno055_get_regmask(), hw_xlate was iterated over the length of the vals array instead of the length of the hw_xlate array. In the case of bno055_gyr_scale, the vals array is larger than the hw_xlate array, so this could result in an out-of-bounds access. In practice, this shouldn't happen though because a match should always be found which breaks out of the for loop before it iterates beyond the end of the hw_xlate array. By adding a new hw_xlate_len field to the bno055_sysfs_attr, we can be sure we are iterating over the correct length.	N/A	More Details
CVE-2025-39720	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix refcount leak causing resource not released When ksmbd_conn_releasing(opinfo->conn) returns true,the refcount was not decremented properly, causing a refcount leak that prevents the count from reaching zero and the memory from being released.	N/A	More Details
CVE-2025-39721	In the Linux kernel, the following vulnerability has been resolved: crypto: qat - flush misc workqueue during device shutdown Repeated loading and unloading of a device specific QAT driver, for example qat_4xxx, in a tight loop can lead to a crash due to a use-after-free scenario. This occurs when a power management (PM) interrupt triggers just before the device-specific driver (e.g., qat_4xxx.ko) is unloaded, while the core driver (intel_qat.ko) remains loaded. Since the driver uses a shared workqueue (`qat_misc_wq`) across all devices and owned by intel_qat.ko, a deferred routine from the device-specific driver may still be pending in the queue. If this routine executes after the driver is unloaded, it can dereference freed memory, resulting in a page fault and kernel crash like the following: BUG: unable to handle page fault for address: ffa000002e50a01c #PF: supervisor read access in kernel mode RIP: 0010:pm_bh_handler+0x1d2/0x250 [intel_qat] Call Trace: pm_bh_handler+0x1d2/0x250 [intel_qat] process_one_work+0x171/0x340 worker_thread+0x277/0x3a0 kthread+0xf0/0x120 ret_from_fork+0x2d/0x50 To prevent this, flush the misc workqueue during device shutdown to ensure that all pending work items are completed before the driver is unloaded. Note: This approach may slightly increase shutdown latency if the workqueue contains jobs from other devices, but it ensures correctness and stability.	N/A	More Details
CVE-2025-39722	In the Linux kernel, the following vulnerability has been resolved: crypto: caam - Prevent crash on suspend with iMX8QM / iMX8ULP Since the CAAM on these SoCs is managed by another ARM core, called the SECO (Security Controller) on iMX8QM and Secure Enclave on iMX8ULP, which also reserves access to register page 0 suspend operations cannot touch this page. This is similar to when running OPTEE, where OPTEE will reserve page 0. Track this situation using a new state variable no_page0, reflecting if page 0 is reserved elsewhere, either by other management cores in SoC or by OPTEE. Replace the optee_en check in suspend/resume with the new check. optee_en cannot go away as it's needed elsewhere to gate OPTEE specific situations. Fixes the following splat at suspend: Internal error: synchronous external abort: 0000000096000010 [#1] SMP Hardware name: Freescale i.MX8QXP ACU6C (DT) pstate: 60400005 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : readl+0x0/0x18 lr : rd_reg32+0x18/0x3c sp : ffffffc08192ba20 x29: ffffffc08192ba20 x28: ffffff8025190000 x27: 0000000000000000 x26: ffffffc0808ae808 x25: ffffffc080922338 x24: ffffff8020e89090 x23: 0000000000000000 x22: ffffffc080922000 x21: ffffff8020e89010 x20: ffffffc080387ef8 x19: ffffff8020e89010 x18: 000000005d8000d5 x17: 0000000030f35963 x16: 000000008f785f3f x15: 000000003b8ef57c x14: 00000000c418aef8 x13: 00000000f5fea526 x12: 0000000000000001 x11: 0000000000000002 x10: 0000000000000001 x9 : 0000000000000000 x8 : ffffff8025190870 x7 : ffffff8021726880 x6 : 0000000000000002 x5 : ffffff80217268f0 x4 : ffffff8021726880 x3 : ffffffc081200000 x2 : 0000000000000001 x1 : ffffff8020e89010 x0 : ffffffc081200004 Call trace: readl+0x0/0x18 caam_ctrl_suspend+0x30/0xdc dpm_run_callback.constprop.0+0x24/0x5c device_suspend+0x170/0x2e8 dpm_suspend+0xa0/0x104 dpm_suspend_start+0x48/0x50 suspend_devices_and_enter+0x7c/0x45c pm_suspend+0x148/0x160 state_store+0xb4/0xf8 kobj_attr_store+0x14/0x24 sysfs_kf_write+0x38/0x48 kernfs_fop_write_iter+0xb4/0x178 vfs_write+0x118/0x178 ksys_write+0x6c/0xd0 __arm64_sys_write+0x14/0x1c invoke_syscall.constprop.0+0x64/0xb0 do_el0_svc+0x90/0xb0 el0_svc+0x18/0x44 el0t_64_sync_handler+0x88/0x124 el0t_64_sync+0x150/0x154 Code: 88dffc21 88dffc21 5ac00800 d65f03c0 (b9400000)	N/A	More Details
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: netfs: Fix unbuffered write error handling If all the subrequests in an unbuffered write stream fail, the subrequest collector doesn't update the stream->transferred value and it retains its initial LONG_MAX value. Unfortunately, if all active streams fail, then we take the smallest value of { LONG_MAX, LONG_MAX, ... } as the value to set in wreq->transferred - which is then returned from ->write_iter(). LONG_MAX was chosen as the initial value so that all the streams can be quickly assessed by taking the smallest value of all stream->transferred - but this only works if we've set any of them. Fix this by adding a flag to indicate whether the value in stream->transferred is valid and checking that when we integrate the values. stream->transferred can then be initialised to zero. This was found by running the generic/750 xfstest against cifs with cache=none. It splices data to the target file. Once (if) it has used up all the available scratch space, the writes	N/A	More Details

39723	start failing with ENOSPC. This causes ->write_iter() to fail. However, it was returning wreq->transferred, i.e. LONG_MAX, rather than an error (because it thought the amount transferred was non-zero) and iter_file_splice_write() would then try to clean up that amount of pipe bufferage - leading to an oops when it overran. The kernel log showed: CIFS: VFS: Send error in write = -28 followed by: BUG: kernel NULL pointer dereference, address: 0000000000000008 with: RIP: 0010:iter_file_splice_write+0x3a4/0x520 do_splice+0x197/0x4e0 or: RIP: 0010:pipe_buf_release (include/linux/pipe_fs_i.h:282) iter_file_splice_write (fs/splice.c:755) Also put a warning check into splice to announce if ->write_iter() returned that it had written more than it was asked to.		
CVE-2025-39724	In the Linux kernel, the following vulnerability has been resolved: serial: 8250: fix panic due to PSLVERR When the PSLVERR_RESP_EN parameter is set to 1, the device generates an error response if an attempt is made to read an empty RBR (Receive Buffer Register) while the FIFO is enabled. In serial8250_do_startup(), calling serial_port_out(port, UART_LCR, UART_LCR_WLEN8) triggers dw8250_check_lcr(), which invokes dw8250_force_idle() and serial8250_clear_and_reinit_fifos(). The latter function enables the FIFO via serial_out(p, UART_FCR, p->fcr). Execution proceeds to the serial_port_in(port, UART_RX). This satisfies the PSLVERR trigger condition. When another CPU (e.g., using printk()) is accessing the UART (UART is busy), the current CPU fails the check (value & ~UART_LCR_SPAR) == (lcr & ~UART_LCR_SPAR) in dw8250_check_lcr(), causing it to enter dw8250_force_idle(). Put serial_port_out(port, UART_LCR, UART_LCR_WLEN8) under the port->lock to fix this issue. Panic backtrace: [0.442336] Oops - unknown exception [#1] [0.442343] epc : dw8250_serial_in32+0x1e/0x4a [0.442351] ra : serial8250_do_startup+0x2c8/0x88e ... [0.442416] console_on_rootfs+0x26/0x70	N/A	More Details
CVE-2025-39725	In the Linux kernel, the following vulnerability has been resolved: mm/vmscan: fix hwpoisoned large folio handling in shrink_folio_list In shrink_folio_list(), the hwpoisoned folio may be large folio, which can't be handled by unmap_poisoned_folio(). For THP, try_to_unmap_one() must be passed with TTU_SPLIT_HUGE_PMD to split huge PMD first and then retry. Without TTU_SPLIT_HUGE_PMD, we will trigger null-ptr deref of pvmw.pte. Even we passed TTU_SPLIT_HUGE_PMD, we will trigger a WARN_ON_ONCE due to the page isn't in swapcache. Since UCE is rare in real world, and race with reclaimation is more rare, just skipping the hwpoisoned large folio is enough. memory_failure() will handle it if the UCE is triggered again. This happens when memory reclaim for large folio races with memory_failure(), and will lead to kernel panic. The race is as follows: cpu0 cpu1 shrink_folio_list memory_failure TestSetPageHWPoison unmap_poisoned_folio --> trigger BUG_ON due to unmap_poisoned_folio couldn't handle large folio [tujinjiang@huawei.com: add comment to unmap_poisoned_folio()]	N/A	More Details
CVE-2025-39710	In the Linux kernel, the following vulnerability has been resolved: media: venus: Add a check for packet size after reading from shared memory Add a check to ensure that the packet size does not exceed the number of available words after reading the packet header from shared memory. This ensures that the size provided by the firmware is safe to process and prevent potential out-of-bounds memory access.	N/A	More Details
CVE-2025-39708	In the Linux kernel, the following vulnerability has been resolved: media: iris: Fix NULL pointer dereference A warning reported by smatch indicated a possible null pointer dereference where one of the arguments to API "iris_hfi_gen2_handle_system_error" could sometimes be null. To fix this, add a check to validate that the argument passed is not null before accessing its members.	N/A	More Details
CVE-2025-57062	Tenda G3 v3.0br_V15.11.0.17 was discovered to contain a stack overflow in the delDhcpIndex parameter in the formDelDhcpRule function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-39707	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: check if hubbub is NULL in debugfs/amdgpu_dm_capabilities HUBBUB structure is not initialized on DCE hardware, so check if it is NULL to avoid null dereference while accessing amdgpu_dm_capabilities file in debugfs.	N/A	More Details
CVE-2025-57061	Tenda G3 v3.0br_V15.11.0.17 was discovered to contain multiple stack overflows in the formIPMacBindModify function via the ruleId, ip, mac, v6 and remark parameters. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-57059	Tenda G3 v3.0br_V15.11.0.17 was discovered to contain a stack overflow in the dhcpIndex parameter in the addDhcpRule function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-57058	Tenda G3 v3.0br_V15.11.0.17 was discovered to contain multiple stack overflows in the formSetDebugCfg function via the pEnable, pLevel, and pModule parameters. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-57057	Tenda G3 v3.0br_V15.11.0.17 was discovered to contain a stack overflow in the listStr parameter in the ipMacBindListStore function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-41000	Cross-Frame Scripting (XFS) vulnerability in BoomCMS v9.1.4 from UXB London. XFS is a web attack technique that exploits specific browser bugs to spy on users via JavaScript. This type of attack is based on social engineering and depends entirely on the browser chosen by the user, so it is perceived as a minor threat to web application security. This vulnerability only works in older browsers.	N/A	More Details
CVE-2025-39694	In the Linux kernel, the following vulnerability has been resolved: s390/sclp: Fix SCCB present check Tracing code called by the SCLP interrupt handler contains early exits if the SCCB address associated with an interrupt is NULL. This check is performed after physical to virtual address translation. If the kernel identity mapping does not start at address zero, the resulting virtual address is never zero, so that the NULL checks won't work. Subsequently this may result in incorrect accesses to the first page of the identity mapping. Fix this by introducing a function that handles	N/A	More Details

	the NULL case before address translation.		
CVE-2025-38678	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: reject duplicate device on updates A chain/flowtable update with duplicated devices in the same batch is possible. Unfortunately, netdev event path only removes the first device that is found, leaving unregistered the hook of the duplicated device. Check if a duplicated device exists in the transaction batch, bail out with EEXIST in such case. WARNING is hit when unregistering the hook: [49042.221275] WARNING: CPU: 4 PID: 8425 at net/netfilter/core.c:340 nf_hook_entry_head+0xaa/0x150 [49042.221375] CPU: 4 UID: 0 PID: 8425 Comm: nft Tainted: G S 6.16.0+ #170 PREEMPT(full) [...] [49042.221382] RIP: 0010:nf_hook_entry_head+0xaa/0x150	N/A	More Details
CVE-2025-39700	In the Linux kernel, the following vulnerability has been resolved: mm/damon/ops-common: ignore migration request to invalid nodes damon_migrate_pages() tries migration even if the target node is invalid. If users mistakenly make such invalid requests via DAMOS_MIGRATE_{HOT,COLD} action, the below kernel BUG can happen. [7831.883495] BUG: unable to handle page fault for address: 0000000000001f48 [7831.884160] #PF: supervisor read access in kernel mode [7831.884681] #PF: error_code(0x0000) - not-present page [7831.885203] PGD 0 P4D 0 [7831.885468] Oops: Oops: 0000 [#1] SMP PTI [7831.885852] CPU: 31 UID: 0 PID: 94202 Comm: kdamond.0 Not tainted 6.16.0-rc5-mm-new-damon+ #93 PREEMPT(voluntary) [7831.886913] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-4.el9 04/01/2014 [7831.887777] RIP: 0010:__alloc_frozen_pages_noprof (include/linux/mmzone.h:1724 include/linux/mmzone.h:1750 mm/page_alloc.c:4936 mm/page_alloc.c:5137) [...] [7831.895953] Call Trace: [7831.896195] <TASK> [7831.896397] __folio_alloc_noprof (mm/page_alloc.c:5183 mm/page_alloc.c:5192) [7831.896787] migrate_pages_batch (mm/migrate.c:1189 mm/migrate.c:1851) [7831.897228] ? __pfx_alloc_migration_target (mm/migrate.c:2137) [7831.897735] migrate_pages (mm/migrate.c:2078) [7831.898141] ? __pfx_alloc_migration_target (mm/migrate.c:2137) [7831.898664] damon_migrate_folio_list (mm/damon/ops-common.c:321 mm/damon/ops-common.c:354) [7831.899140] damon_migrate_pages (mm/damon/ops-common.c:405) [...] Add a target node validity check in damon_migrate_pages(). The validity check is stolen from that of do_pages_move(), which is being used for the move_pages() system call.	N/A	More Details
CVE-2025-39701	In the Linux kernel, the following vulnerability has been resolved: ACPI: pfr_update: Fix the driver update version check The security-version-number check should be used rather than the runtime version check for driver updates. Otherwise, the firmware update would fail when the update binary had a lower runtime version number than the current one. [rjw: Changelog edits]	N/A	More Details
CVE-2025-39702	In the Linux kernel, the following vulnerability has been resolved: ipv6: sr: Fix MAC comparison to be constant-time To prevent timing attacks, MACs need to be compared in constant time. Use the appropriate helper function for this.	N/A	More Details
CVE-2025-47421	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability in CRESTRON TOUCHSCREENS x70 allows Argument Injection.This issue affects TOUCHSCREENS x70: from 3.001.0031.001 through 3.001.0034.001. A specially crafted SCP command sent via SSH login string can lead a valid administrator user to gain Privileged Operating System access on the device. Following Products Models are affected: TSW-x70 TSW-x60 TST-1080 AM-3000/3100/3200 Soundbar VB70 HD-PS622/621/402 HD-TXU-RXU-4kZ-211 HD-MDNXM-4KZ-E *Note: additional firmware updates will be published once made available	N/A	More Details
CVE-2025-39703	In the Linux kernel, the following vulnerability has been resolved: net, hsr: reject HSR frame if skb can't hold tag Receiving HSR frame with insufficient space to hold HSR tag in the skb can result in a crash (kernel BUG): [45.390915] skbuff: skb_under_panic: text:ffffffff86f32cac len:26 put:14 head:ffff888042418000 data:ffff888042417ff4 tail:0xe end:0x180 dev:bridge_slave_1 [45.392559] ------------[cut here]------------ [45.392912] kernel BUG at net/core/skbuff.c:211! [45.393276] Oops: invalid opcode: 0000 [#1] SMP DEBUG_PAGEALLOC KASAN NOPTI [45.393809] CPU: 1 UID: 0 PID: 2496 Comm: reproducer Not tainted 6.15.0 #12 PREEMPT(undef) [45.394433] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [45.395273] RIP: 0010:skb_panic+0x15b/0x1d0 <snip registers, remove unreliable trace> [45.402911] Call Trace: [45.403105] <IRQ> [45.404470] skb_push+0xcd/0xf0 [45.404726] br_dev_queue_push_xmit+0x7c/0x6c0 [45.406513] br_forward_finish+0x128/0x260 [45.408483] __br_forward+0x42d/0x590 [45.409464] maybe_deliver+0x2eb/0x420 [45.409763] br_flood+0x174/0x4a0 [45.410030] br_handle_frame_finish+0xc7c/0x1bc0 [45.411618] br_handle_frame+0xac3/0x1230 [45.413674] __netif_receive_skb_core.constprop.0+0x808/0x3df0 [45.422966] __netif_receive_skb_one_core+0xb4/0x1f0 [45.424478] __netif_receive_skb+0x22/0x170 [45.424806] process_backlog+0x242/0x6d0 [45.425116] __napi_poll+0xbb/0x630 [45.425394] net_rx_action+0x4d1/0xcc0 [45.427613] handle_softirqs+0x1a4/0x580 [45.427926] do_softirq+0x74/0x90 [45.428196] </IRQ> This issue was found by syzkaller. The panic happens in br_dev_queue_push_xmit() once it receives a corrupted skb with ETH header already pushed in linear data. When it attempts the skb_push() call, there's not enough headroom and skb_push() panics. The corrupted skb is put on the queue by HSR layer, which makes a sequence of unintended transformations when it receives a specific corrupted HSR frame (with incomplete TAG). Fix it by dropping and consuming frames that are not long enough to contain both ethernet and hsr headers. Alternative fix would be to check for enough headroom before skb_push() in br_dev_queue_push_xmit(). In the reproducer, this is injected via AF_PACKET, but I don't easily see why it couldn't be sent over the wire from adjacent network. Further Details: In the reproducer, the following network interface chain is set up: ┌──────────────┐ ┌──────────────┐ │ veth0_to_hsr ├──┤ hsr_slave0 ┼──┐ └──────────────┘ │ │ ┌──────┐ ├──┤ hsr0 ├──┐ │ └──────┘ │ ┌──────────────┐ ┌──────────────┐ │ │ ┌──────────────┐ │ veth1_to_hsr ┼──┤ hsr_slave1 ├──┘ └┤ │ └──────────────┘ └──────────────┘ ┌┼ bridge │ │ │ └──────────────┘ │ ┌──────┐ │ │ ... ├──────┘ └──────┘ To trigger the events leading up to crash, reproducer sends a corrupted HSR fr ---truncated---	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: LoongArch: KVM: Fix stack protector issue in send_ipi_data() Function kvm_io_bus_read() is called in function send_ipi_data(), buffer size of parameter *val should		

CVE-2025-39704	be at least 8 bytes. Since some emulation functions like loongarch_ipi_readl() and kvm_eiointc_read() will write the buffer *val with 8 bytes signed extension regardless parameter len. Otherwise there will be buffer overflow issue when CONFIG_STACKPROTECTOR is enabled. The bug report is shown as follows: Kernel panic - not syncing: stack-protector: Kernel stack is corrupted in: send_ipi_data+0x194/0x1a0 [kvm] CPU: 11 UID: 107 PID: 2692 Comm: CPU 0/KVM Not tainted 6.17.0-rc1+ #102 PREEMPT(full) Stack : 9000000005901568 0000000000000000 9000000003af371c 900000013c68c000 900000013c68f850 900000013c68f858 0000000000000000 900000013c68f998 900000013c68f990 900000013c68f990 900000013c68f6c0 ffffffffffdb058 ffffffffffdb0e0 900000013c68f858 911e1d4d39cf0ec2 9000000105657a00 0000000000000001 fffffffffffffffe 0000000000000578 282049464555206e 6f73676e6f6f4c20 0000000000000001 00000000086b4000 0000000000000000 0000000000000000 0000000000000000 9000000005709968 90000000058f9000 900000013c68fa68 900000013c68fab4 90000000029279f0 900000010153f940 900000010001f360 0000000000000000 9000000003af3734 000000004390000c 00000000000000b0 0000000000000004 0000000000000000 0000000000071c1d ... Call Trace: [<9000000003af3734>] show_stack+0x5c/0x180 [<9000000003aed168>] dump_stack_lvl+0x6c/0x9c [<9000000003ad0ab0>] vpanic+0x108/0x2c4 [<9000000003ad0ca8>] panic+0x3c/0x40 [<9000000004eb0a1c>] __stack_chk_fail+0x14/0x18 [<ffff8000023473f8>] send_ipi_data+0x190/0x1a0 [kvm] [<ffff8000023313e4>] __kvm_io_bus_write+0xa4/0xe8 [kvm] [<ffff80000233147c>] kvm_io_bus_write+0x54/0x90 [kvm] [<ffff80000233f9f8>] kvm_emu_iocsr+0x180/0x310 [kvm] [<ffff80000233fe08>] kvm_handle_gspr+0x280/0x478 [kvm] [<ffff8000023443e8>] kvm_handle_exit+0xc0/0x130 [kvm]	N/A	More Details
CVE-2025-39705	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: fix a Null pointer dereference vulnerability [Why] A null pointer dereference vulnerability exists in the AMD display driver's (DC module) cleanup function dc_destruct(). When display control context (dc->ctx) construction fails (due to memory allocation failure), this pointer remains NULL. During subsequent error handling when dc_destruct() is called, there's no NULL check before dereferencing the perf_trace member (dc->ctx->perf_trace), causing a kernel null pointer dereference crash. [How] Check if dc->ctx is non-NULL before dereferencing. (Updated commit text and removed unnecessary error message) (cherry picked from commit 9dd8e2ba268c636c240a918e0a31e6feaee19404)	N/A	More Details
CVE-2025-39706	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Destroy KFD debugfs after destroy KFD wq Since KFD proc content was moved to kernel debugfs, we can't destroy KFD debugfs before kfd_process_destroy_wq. Move kfd_process_destroy_wq prior to kfd_debugfs_fini to fix a kernel NULL pointer problem. It happens when /sys/kernel/debug/kfd was already destroyed in kfd_debugfs_fini but kfd_process_destroy_wq calls kfd_debugfs_remove_process. This line debugfs_remove_recursive(entry->proc_dentry); tries to remove /sys/kernel/debug/kfd/proc/<pid> while /sys/kernel/debug/kfd is already gone. It hangs the kernel by kernel NULL pointer. (cherry picked from commit 0333052d90683d88531558dcfdbf2525cc37c233)	N/A	More Details
CVE-2025-39695	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Flush delayed SKBs while releasing RXE resources When skb packets are sent out, these skb packets still depends on the rxe resources, for example, QP, sk, when these packets are destroyed. If these rxe resources are released when the skb packets are destroyed, the call traces will appear. To avoid skb packets hang too long time in some network devices, a timestamp is added when these skb packets are created. If these skb packets hang too long time in network devices, these network devices can free these skb packets to release rxe resources.	N/A	More Details
CVE-2025-39682	In the Linux kernel, the following vulnerability has been resolved: tls: fix handling of zero-length records on the rx_list Each recvmsg() call must process either - only contiguous DATA records (any number of them) - one non-DATA record If the next record has different type than what has already been processed we break out of the main processing loop. If the record has already been decrypted (which may be the case for TLS 1.3 where we don't know type until decryption) we queue the pending record to the rx_list. Next recvmsg() will pick it up from there. Queuing the skb to rx_list after zero-copy decrypt is not possible, since in that case we decrypted directly to the user space buffer, and we don't have an skb to queue (darg.skb points to the ciphertext skb for access to metadata like length). Only data records are allowed zero-copy, and we break the processing loop after each non-data record. So we should never zero-copy and then find out that the record type has changed. The corner case we missed is when the initial record comes from rx_list, and it's zero length.	N/A	More Details
CVE-2025-39693	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Avoid a NULL pointer dereference [WHY] Although unlikely drm_atomic_get_new_connector_state() or drm_atomic_get_old_connector_state() can return NULL. [HOW] Check returns before dereference. (cherry picked from commit 1e5e8d672fec9f2ab352be121be971877bff2af9)	N/A	More Details
CVE-2025-34176	In pfSense CE /suricata/suricata_ip_reputation.php, the value of the iplist parameter is not sanitized of directory traversal-related strings/characters. This value is directly used in a file existence check operation. While the contents of the file cannot be read, the server reveals whether the file exists, which enables an attacker to enumerate files on the target. The attacker must be authenticated with at least "WebCfg - Services: suricata package" permissions.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix vm_bind_ioctl double free bug If the argument check during an array bind fails, the bind_ops are freed twice as seen below. Fix this by setting bind_ops to NULL after freeing. == BUG: KASAN: double-free in xe_vm_bind_ioctl+0x1b2/0x21f0 [xe] Free of addr ffff88813bb9b800 by task xe_vm/14198 CPU: 5 UID: 0 PID: 14198 Comm: xe_vm Not tainted 6.16.0-xe-eudebug-cmanszew+ #520 PREEMPT(full) Hardware name: Intel Corporation Alder Lake Client Platform/AlderLake-P DDR5 RVP, BIOS ADLPFWI1.R00.2411.A02.2110081023 10/08/2021 Call Trace: <TASK> dump_stack_lvl+0x82/0xd0 print_report+0xcb/0x610 ? __virt_addr_valid+0x19a/0x300 ? xe_vm_bind_ioctl+0x1b2/0x21f0 [xe] kasan_report_invalid_free+0xc8/0xf0 ? xe_vm_bind_ioctl+0x1b2/0x21f0 [xe] ? xe_vm_bind_ioctl+0x1b2/0x21f0 [xe]		

CVE-2025-38731	check_slab_allocation+0x102/0x130 kfree+0x10d/0x440 ? should_fail_ex+0x57/0x2f0 ? xe_vm_bind_ioctl+0x1b2/0x21f0 [xe] xe_vm_bind_ioctl+0x1b2/0x21f0 [xe] ? __pfx_xe_vm_bind_ioctl+0x10/0x10 [xe] ? __lock_acquire+0xab9/0x27f0 ? lock_acquire+0x165/0x300 ? drm_dev_enter+0x53/0xe0 [drm] ? find_held_lock+0x2b/0x80 ? drm_dev_exit+0x30/0x50 [drm] ? drm_ioctl_kernel+0x128/0x1c0 [drm] drm_ioctl_kernel+0x128/0x1c0 [drm] ? __pfx_xe_vm_bind_ioctl+0x10/0x10 [xe] ? find_held_lock+0x2b/0x80 ? __pfx_drm_ioctl_kernel+0x10/0x10 [drm] ? should_fail_ex+0x57/0x2f0 ? __pfx_xe_vm_bind_ioctl+0x10/0x10 [xe] drm_ioctl+0x352/0x620 [drm] ? __pfx_drm_ioctl+0x10/0x10 [drm] ? __pfx_rpm_resume+0x10/0x10 ? do_raw_spin_lock+0x11a/0x1b0 ? find_held_lock+0x2b/0x80 ? __pm_runtime_resume+0x61/0xc0 ? rcu_is_watching+0x20/0x50 ? trace_irq_enable.constprop.0+0xac/0xe0 xe_drm_ioctl+0x91/0xc0 [xe] __x64_sys_ioctl+0xb2/0x100 ? rcu_is_watching+0x20/0x50 do_syscall_64+0x68/0x2e0 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7fa9acb24ded (cherry picked from commit a01b704527c28a2fd43a17a85f8996b75ec8492a)	N/A	More Details
CVE-2025-54084	OS Command ('OS Command Injection') vulnerability in Calix GigaCenter ONT (Quantenna SoC modules) allows authenticated attackers with 'super' user credentials to execute arbitrary OS commands through improper input validation, potentially leading to full system compromise.This issue affects GigaCenter ONT: 844E, 844G, 844GE, 854GE.	N/A	More Details
CVE-2025-54083	Insecure Storage of Sensitive Information vulnerability in Calix GigaCenter ONT (Quantenna SoC modules) allows admin access to the web interface.This issue affects GigaCenter ONT: 844E, 844G, 844GE, 854GE.	N/A	More Details
CVE-2025-44595	Halo v2.20.17 and before is vulnerable to Cross Site Scripting (XSS) in /halo_host/archives/{name}.	N/A	More Details
CVE-2025-44593	Halo prior to 2.20.13 allows bypassing file type detection and uploading malicious files such as .exe and .html files. Specifically, .html files can trigger stored XSS vulnerabilities. This vulnerability is fixed in 2.20.13	N/A	More Details
CVE-2025-43491	A vulnerability in the Poly Lens Desktop application running on the Windows platform might allow modifications to the filesystem, which might lead to SYSTEM level privileges being granted.	N/A	More Details
CVE-2025-34178	In pfSense CE /suricata/suricata_app_parsers.php, the value of the policy_name parameter is not sanitized of HTML-related strings/characters before being directly displayed. This can result in stored cross-site scripting. The attacker must be authenticated with at least "WebCfg - Services: suricata package" permissions.	N/A	More Details
CVE-2025-34177	In pfSense CE /suricata/suricata_flow_stream.php, the value of the policy_name parameter is not sanitized of HTML-related strings/characters before being directly displayed. This can result in stored cross-site scripting. The attacker must be authenticated with at least "WebCfg - Services: suricata package" permissions.	N/A	More Details
CVE-2025-38732	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_reject: don't leak dst refcount for loopback packets recent patches to add a WARN() when replacing skb dst entry found an old bug: WARNING: include/linux/skbuff.h:1165 skb_dst_check_unset include/linux/skbuff.h:1164 [inline] WARNING: include/linux/skbuff.h:1165 skb_dst_set include/linux/skbuff.h:1210 [inline] WARNING: include/linux/skbuff.h:1165 nf_reject_fill_skb_dst+0x2a4/0x330 net/ipv4/netfilter/nf_reject_ipv4.c:234 [..] Call Trace: nf_send_unreach+0x17b/0x6e0 net/ipv4/netfilter/nf_reject_ipv4.c:325 nft_reject_inet_eval+0x4bc/0x690 net/netfilter/nft_reject_inet.c:27 expr_call_ops_eval net/netfilter/nf_tables_core.c:237 [inline] .. This is because blamed commit forgot about loopback packets. Such packets already have a dst_entry attached, even at PRE_ROUTING stage. Instead of checking hook just check if the skb already has a route attached to it.	N/A	More Details
CVE-2025-58400	RATOC RAID Monitoring Manager for Windows provided by RATOC Systems, Inc. registers a Windows service with an unquoted file path. A user with the write permission on the root directory of the system drive may execute arbitrary code with SYSTEM privilege.	N/A	More Details
CVE-2025-38733	In the Linux kernel, the following vulnerability has been resolved: s390/mm: Do not map lowcore with identity mapping Since the identity mapping is pinned to address zero the lowcore is always also mapped to address zero, this happens regardless of the relocate_lowcore command line option. If the option is specified the lowcore is mapped twice, instead of only once. This means that NULL pointer accesses will succeed instead of causing an exception (low address protection still applies, but covers only parts). To fix this never map the first two pages of physical memory with the identity mapping.	N/A	More Details
CVE-2025-7635	Unauthenticated Telnet access vulnerability in Calix GigaCenter ONT allows root access.This issue affects GigaCenter ONT: 844E, 844G, 844GE, 854GE.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix UAF on smcsk after smc_listen_out() BPF CI testing report a UAF issue: [16.446633] BUG: kernel NULL pointer dereference, address: 000000000000003 0 [16.447134] #PF: supervisor read access in kernel mod e [16.447516] #PF: error_code(0x0000) - not-present pag e [16.447878] PGD 0 P4D 0 [16.448063] Oops: Oops: 0000 [#1] PREEMPT SMP NOPT I [16.448409] CPU: 0 UID: 0 PID: 9 Comm: kworker/0:1 Tainted: G OE 6.13.0-rc3-g89e8a75fda73-dirty #4 2 [16.449124] Tainted: [O]=OOT_MODULE, [E]=UNSIGNED_MODUL E [16.449502] Hardware name: QEMU Ubuntu 24.04 PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/201 4 [16.450201] Workqueue: smc_hs_wq smc_listen_wor k [16.450531] RIP: 0010:smc_listen_work+0xc02/0x159 0 [16.452158] RSP: 0018:ffffb5ab40053d98 EFLAGS: 0001024		

CVE-2025-38734	6 [16.452526] RAX: 0000000000000001 RBX: 0000000000000002 RCX: 000000000000030 0 [16.452994] RDX: 0000000000000280 RSI: 00003513840053f0 RDI: 000000000000000 0 [16.453492] RBP: ffffa097808e3800 R08: ffffa09782dba1e0 R09: 000000000000000 5 [16.453987] R10: 0000000000000000 R11: 0000000000000000 R12: ffffa0978274640 0 [16.454497] R13: 0000000000000000 R14: 0000000000000000 R15: ffffa09782d4092 0 [16.454996] FS: 0000000000000000(0000) GS:ffffa097bbc00000(0000) knlGS:000000000000000 0 [16.455557] CS: 0010 DS: 0000 ES: 0000 CR0: 000000008005003 3 [16.455961] CR2: 0000000000000030 CR3: 0000000102788004 CR4: 0000000000770ef 0 [16.456459] PKRU: 5555555 4 [16.456654] Call Trace : [16.456832] <TASK > [16.456989] ? __die+0x23/0x7 0 [16.457215] ? page_fault_oops+0x180/0x4c 0 [16.457508] ? __lock_acquire+0x3e6/0x249 0 [16.457801] ? exc_page_fault+0x68/0x20 0 [16.458080] ? asm_exc_page_fault+0x26/0x3 0 [16.458389] ? smc_listen_work+0xc02/0x159 0 [16.458689] ? smc_listen_work+0xc02/0x159 0 [16.458987] ? lock_is_held_type+0x8f/0x10 0 [16.459284] process_one_work+0x1ea/0x6d 0 [16.459570] worker_thread+0x1c3/0x38 0 [16.459839] ? __pfx_worker_thread+0x10/0x1 0 [16.460144] kthread+0xe0/0x11 0 [16.460372] ? __pfx_kthread+0x10/0x1 0 [16.460640] ret_from_fork+0x31/0x5 0 [16.460896] ? __pfx_kthread+0x10/0x1 0 [16.461166] ret_from_fork_asm+0x1a/0x3 0 [16.461453] </TASK > [16.461616] Modules linked in: bpf_testmod(OE) [last unloaded: bpf_testmod(OE)] [16.462134] CR2: 000000000000003 0 [16.462380] ---[end trace 0000000000000000]--- [16.462710] RIP: 0010:smc_listen_work+0xc02/0x1590 The direct cause of this issue is that after smc_listen_out_connected(), newclcsock->sk may be NULL since it will releases the smcsk. Therefore, if the application closes the socket immediately after accept, newclcsock->sk can be NULL. A possible execution order could be as follows: smc_listen_work | userspace ---------- lock_sock(sk) | smc_listen_out_connected() | | \- smc_listen_out | | | \- release_sock | | |- sk->sk_data_ready() | | fd = accept(); | close(fd); | \- socket->sk = NULL; /* newclcsock->sk is NULL now */ SMC_STAT_SERV_SUCC_INC(sock_net(newclcsock->sk)) Since smc_listen_out_connected() will not fail, simply swapping the order of the code can easily fix this issue.	N/A	More Details
CVE-2025-38735	In the Linux kernel, the following vulnerability has been resolved: gve: prevent ethtool ops after shutdown A crash can occur if an ethtool operation is invoked after shutdown() is called. shutdown() is invoked during system shutdown to stop DMA operations without performing expensive deallocations. It is discouraged to unregister the netdev in this path, so the device may still be visible to userspace and kernel helpers. In gve, shutdown() tears down most internal data structures. If an ethtool operation is dispatched after shutdown(), it will dereference freed or NULL pointers, leading to a kernel panic. While graceful shutdown normally quiesces userspace before invoking the reboot syscall, forced shutdowns (as observed on GCP VMs) can still trigger this path. Fix by calling netif_device_detach() in shutdown(). This marks the device as detached so the ethtool ioctl handler will skip dispatching operations to the driver.	N/A	More Details
CVE-2025-38736	In the Linux kernel, the following vulnerability has been resolved: net: usb: asix_devices: Fix PHY address mask in MDIO bus initialization Syzbot reported shift-out-of-bounds exception on MDIO bus initialization. The PHY address should be masked to 5 bits (0-31). Without this mask, invalid PHY addresses could be used, potentially causing issues with MDIO bus operations. Fix this by masking the PHY address with 0x1f (31 decimal) to ensure it stays within the valid range.	N/A	More Details
CVE-2025-38737	In the Linux kernel, the following vulnerability has been resolved: cifs: Fix oops due to uninitialised variable Fix smb3_init_transform_rq() to initialise buffer to NULL before calling netfs_alloc_folioq_buffer() as netfs assumes it can append to the buffer it is given. Setting it to NULL means it should start a fresh buffer, but the value is currently undefined.	N/A	More Details
CVE-2025-58753	Copyparty is a portable file server. In versions prior to 1.19.8, there was a missing permission-check in the shares feature (the `shr` global-option). When a share was created for just one file inside a folder, it was possible to access the other files inside that folder by guessing the filenames. It was not possible to descend into subdirectories in this manner; only the sibling files were accessible. This issue did not affect filekeys or dirkeys. Version 1.19.8 fixes the issue.	N/A	More Details
CVE-2025-39673	In the Linux kernel, the following vulnerability has been resolved: ppp: fix race conditions in ppp_fill_forward_path ppp_fill_forward_path() has two race conditions: 1. The ppp->channels list can change between list_empty() and list_first_entry(), as ppp_lock() is not held. If the only channel is deleted in ppp_disconnect_channel(), list_first_entry() may access an empty head or a freed entry, and trigger a panic. 2. pch->chan can be NULL. When ppp_unregister_channel() is called, pch->chan is set to NULL before pch is removed from ppp->channels. Fix these by using a lockless RCU approach: - Use list_first_or_null_rcu() to safely test and access the first list entry. - Convert list modifications on ppp->channels to their RCU variants and add synchronize_net() after removal. - Check for a NULL pch->chan before dereferencing it.	N/A	More Details
CVE-2025-55671	Uncontrolled search path element issue exists in TkEasyGUI versions prior to v1.0.22. If this vulnerability is exploited, arbitrary code may be executed with the privilege of running the program.	N/A	More Details
CVE-2025-9785	PaperCut Print Deploy is an optional component that integrates with PaperCut NG/MF which simplifies printer deployment and management. When the component is deployed to an environment, the customer has an option to configure the system to use a self-signed certificate. If the customer does not fully configure the system to leverage the trust database on the clients, it opens up the communication between clients and the server to man-in-the-middle attacks. It was discovered that certain parts of the documentation related to the configuration of SSL in Print Deploy were lacking, which could potentially contribute to a misconfiguration of the Print Deploy client installation. PaperCut strongly recommends to use valid certificates to secure installations and to follow the updated documentation to ensure the correct SSL configuration. Those who use private CAs and/or self-signed certificates should make sure to copy their Certification Authority certificate, or their self signed certificate if using only one, to the trust store of their operating system and to the Java key store	N/A	More Details

CVE-2025-39692	In the Linux kernel, the following vulnerability has been resolved: smb: server: split ksmbd_rdma_stop_listening() out of ksmbd_rdma_destroy() We can't call destroy_workqueue(smb_direct_wq); before stop_sessions()! Otherwise already existing connections try to use smb_direct_wq as a NULL pointer.	N/A	More Details
CVE-2025-9999	Some payload elements of the messages sent between two stations in a networking architecture are not properly checked on the receiving station allowing an attacker to execute unauthorized commands in the application.	N/A	More Details
CVE-2025-59042	PyInstaller bundles a Python application and all its dependencies into a single package. Due to a special entry being appended to `sys.path` during the bootstrap process of a PyInstaller-frozen application, and due to the bootstrap script attempting to load an optional module for bytecode decryption while this entry is still present in `sys.path`, an application built with PyInstaller < 6.0.0 may be tricked by an unprivileged attacker into executing arbitrary python code when **all** of the following conditions are met. First, the application is built with PyInstaller < 6.0.0; both onedir and onefile mode are affected. Second, the optional bytecode encryption code feature was not enabled during the application build. Third, the attacker can create files/directories in the same directory where the executable is located. Fourth, the filesystem supports creation of files/directories that contain `?` in their name (i.e., non-Windows systems). Fifth, the attacker is able to determine the offset at which the PYZ archive is embedded in the executable. The attacker can create a directory (or a zip archive) next to the executable, with the name that matches the format used by PyInstaller's bootloader to transmit information about the location of PYZ archive to the bootstrap script. If this directory (or zip archive) contains a python module whose name matches the name used by the optional bytecode encryption feature, this module will be loaded and executed by the bootstrap script (in the absence of the real, built-in module that is available when the bytecode-encryption feature is enabled). This results in arbitrary code execution that requires no modification of the executable itself. If the executable is running with elevated privileges (for example, due to having the `setuid` bit set), the code in the injected module is also executed with the said elevated privileges, resulting in a local privilege escalation. PyInstaller 6.0.0 (f5adf291c8b832d5aff7632844f7e3ddf7ad4923) removed support for bytecode encryption; this effectively removes the described attack vector, due to the bootstrap script not attempting to load the optional module for bytecode-decryption anymore. PyInstaller 6.10.0 (cfd60b510f95f92cb81fc42735c399bb781a4739) reworked the bootstrap process to avoid (ab)using `sys.path` for transmitting location of the PYZ archive, which further eliminates the possibility of described injection procedure. If upgrading PyInstaller is not feasible, this issue can be worked around by ensuring proper permissions on directories containing security-sensitive executables (i.e., executables with `setuid` bit set) should mitigate the issue.	N/A	More Details
CVE-2025-59039	Prebid Universal Creative (PUC) is a JavaScript API to render multiple formats. Npm users of PUC 1.17.3 or PUC latest were briefly affected by crypto-related malware. This includes the extremely popular jsdelivr hosting of this file. The maintainers of PUC unpublished version 1.17.3. Users should see Prebid.js 9 release notes for suggestions on moving off the deprecated workflow of using the PUC or pointing to a dynamic version of it. PUC users pointing to latest should transition to 1.17.2 as soon as possible to avoid similar attacks in the future.	N/A	More Details
CVE-2025-59038	Prebid.js is a free and open source library for publishers to quickly implement header bidding. NPM users of prebid 10.9.2 may have been briefly compromised by a malware campaign. The malicious code attempts to redirect crypto transactions on the site to the attackers' wallet. Version 10.10.0 fixes the issue. As a workaround, it is also possible to downgrade to 10.9.1.	N/A	More Details
CVE-2025-57806	Local Deep Research is an AI-powered research assistant for deep, iterative research. Versions 0.2.0 through 0.6.7 stored confidential information, including API keys, in a local SQLite database without encryption. This behavior was not clearly documented outside of the database architecture page. Users were not given the ability to configure the database location, allowing anyone with access to the container or host filesystem to retrieve sensitive data in plaintext by accessing the .db file. This is fixed in version 1.0.0.	N/A	More Details
CVE-2025-9997	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that could cause command injection in BLMon that is executed in the operating system console when in a SSH session.	N/A	More Details
CVE-2025-58440	Rejected reason: The unisharp/laravel-filemanager is a separate project, unrelated to laravel-filemanager.	N/A	More Details
CVE-2025-58164	Rejected reason: This CVE is a duplicate of another CVE, CVE-2025-58163.	N/A	More Details
CVE-2025-9998	The sequence of packets received by a Networking server are not correctly checked. An attacker could exploit this vulnerability to send specially crafted messages to force the application to stop.	N/A	More Details
CVE-2025-58165	Rejected reason: This CVE is a duplicate of another CVE, CVE-2025-58163.	N/A	More Details
CVE-2025-58170	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-			More

2025-58166	Rejected reason: This CVE is a duplicate of another CVE.	N/A	Details
CVE-2025-58167	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2025-9996	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that could cause the execution of any shell command when executing a netstat command using BLMon Console in an SSH session.	N/A	More Details
CVE-2025-7746	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause an unvalidated data injected by a malicious user potentially leading to modify or read data in a victim’s browser.	N/A	More Details
CVE-2025-59037	DuckDB is an analytical in-process SQL database management system. On 08 September 2025, the DuckDB distribution for Node.js on npm was compromised with malware (along with several other packages). An attacker published new versions of four of DuckDB's packages that included malicious code to interfere with cryptocoin transactions* According to the npm statistics, nobody has downloaded these packages before they were deprecated. The packages and versions `@duckdb/node-api@1.3.3`, `@duckdb/node-bindings@1.3.3`, `duckdb@1.3.3`, and `@duckdb/duckdb-wasm@1.29.2` were affected. DuckDB immediately deprecated the specific versions, engaged npm support to delete the affected verions, and re-released the node packages with higher version numbers (1.3.4/1.30.0). Users may upgrade to versions 1.3.4, 1.30.0, or a higher version to protect themselves. As a workaround, they may also downgrade to 1.3.2 or 1.29.1.	N/A	More Details
CVE-2025-58168	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2025-58169	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2025-57633	A command injection vulnerability in FTP-Flask-python through 5173b68 allows unauthenticated remote attackers to execute arbitrary OS commands. The /ftp.html endpoint's "Upload File" action constructs a shell command from the ftp_file parameter and executes it using os.system() without sanitization or escaping.	N/A	More Details
CVE-2025-58435	Open OnDemand is an open-source HPC portal. Prior to versions 3.1.15 and 4.0.7, noVNC interactive applications did not correctly rotate the password when TurboVNC was higher than version 3.1.2. The likelihood of exploitation is low as a user would need to share their link to an active desktop session and the other user would need to be authenticated to the portal. But obtaining the link would allow that user to perform any actions as the original user and access their data. Open OnDemand 3.1.15 and 4.0.7 have patched this vulnerability and correctly rotate passwords for any version of TurboVNC. As a workaround, downgrade TurboVNC to a version lower than 3.1.2.	N/A	More Details
CVE-2025-58430	listmonk is a standalone, self-hosted, newsletter and mailing list manager. In versions up to and including 1.1.0, every http request in addition to the session cookie `session` there included `nonce`. The value is not checked and validated by the backend, removing `nonce` allows the requests to be processed correctly. This may seem harmless, but if chained to other vulnerabilities it can become a critical vulnerability. Cross-site request forgery and cross-site scripting chained together can result in improper admin account creation. As of time of publication, no patched versions are available.	N/A	More Details
CVE-2025-58180	OctoPrint provides a web interface for controlling consumer 3D printers. OctoPrint versions up until and including 1.11.2 contain a vulnerability that allows an authenticated attacker to upload a file under a specially crafted filename that will allow arbitrary command execution if said filename becomes included in a command defined in a system event handler and said event gets triggered. If no event handlers executing system commands with uploaded filenames as parameters have been configured, this vulnerability does not have an impact. The vulnerability is patched in version 1.11.3. As a workaround, OctoPrint administrators who have event handlers configured that include any kind of filename based placeholders should disable those by setting their `enabled` property to `False` or unchecking the "Enabled" checkbox in the GUI based Event Manager. Alternatively, OctoPrint administrators should set `feature.enforceReallyUniversalFilenames` to `true` in `config.yaml` and restart OctoPrint, then vet the existing uploads and make sure to delete any suspicious looking files. As always, OctoPrint administrators are advised to not expose OctoPrint on hostile networks like the public internet, and to vet who has access to their instance.	N/A	More Details
CVE-2025-39683	In the Linux kernel, the following vulnerability has been resolved: tracing: Limit access to parser->buffer when trace_get_user failed When the length of the string written to set_ftrace_filter exceeds FTRACE_BUFF_MAX, the following KASAN alarm will be triggered: BUG: KASAN: slab-out-of-bounds in strsep+0x18c/0x1b0 Read of size 1 at addr ffff0000d00bd5ba by task ash/165 CPU: 1 UID: 0 PID: 165 Comm: ash Not tainted 6.16.0-g6bcdbd62bd56-dirty Hardware name: linux,dummy-virt (DT) Call trace: show_stack+0x34/0x50 (C) dump_stack_lvl+0xa0/0x158 print_address_description.constprop.0+0x88/0x398 print_report+0xb0/0x280 kasan_report+0xa4/0xf0 __asan_report_load1_noabort+0x20/0x30 strsep+0x18c/0x1b0 ftrace_process_regex.isra.0+0x100/0x2d8 ftrace_regex_release+0x484/0x618 __fput+0x364/0xa58 ____fput+0x28/0x40 task_work_run+0x154/0x278 do_notify_resume+0x1f0/0x220 el0_svc+0xec/0xf0 el0t_64_sync_handler+0xa0/0xe8 el0t_64_sync+0x1ac/0x1b0 The reason is that trace_get_user will fail when processing a string longer than FTRACE_BUFF_MAX, but not set the end of parser->buffer to 0. Then an OOB access will be triggered in ftrace_regex_release-> ftrace_process_regex-	N/A	More Details

	>strsep->strpbrk. We can solve this problem by limiting access to parser->buffer when trace_get_user failed.		
CVE-2025-57665	Element Plus Link component (el-link) through 2.10.6 implements insufficient input validation for the href attribute, creating a security abstraction gap that obscures URL-based attack vectors. The component passes user-controlled href values directly to underlying anchor elements without protocol validation, URL sanitization, or security headers. This allows attackers to inject malicious URLs using dangerous protocols (javascript:, data:, file:) or redirect users to external malicious sites. While native HTML anchor elements present similar risks, UI component libraries bear additional responsibility for implementing security safeguards and providing clear risk documentation. The vulnerability enables XSS attacks, phishing campaigns, and open redirect exploits affecting applications that use Element Plus Link components with user-controlled or untrusted URL inputs.	N/A	More Details
CVE-2025-57086	Tenda W30E V16.01.0.19 (5037) was discovered to contain a stack overflow in the String parameter in the formDeleteMeshNode function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-57085	Tenda W30E V16.01.0.19 (5037) was discovered to contain a stack overflow in the v17 parameter in the UploadCfg function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-57078	Tenda G3 v3.0br_V15.11.0.17 was discovered to contain a stack overflow in the pppoeServerWhiteMacIndex parameter in the formModifyPppAuthWhiteMac function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-10199	A local privilege escalation vulnerability exists in Sunshine for Windows (version v2025.122.141614 and likely prior versions) due to an unquoted service path.	N/A	More Details
CVE-2025-10198	Sunshine for Windows, version v2025.122.141614, contains a DLL search-order hijacking vulnerability, allowing attackers to insert a malicious DLL in user-writeable PATH directories.	N/A	More Details
CVE-2025-39681	In the Linux kernel, the following vulnerability has been resolved: x86/cpu/hygon: Add missing resctrl_cpu_detect() in bsp_init helper Since 923f3a2b48bd ("x86/resctrl: Query LLC monitoring properties once during boot") resctrl_cpu_detect() has been moved from common CPU initialization code to the vendor-specific BSP init helper, while Hygon didn't put that call in their code. This triggers a division by zero fault during early booting stage on our machines with X86_FEATURE_CQM* supported, where get_rdt_mon_resources() tries to calculate mon_l3_config with uninitialized boot_cpu_data.x86_cache_occ_scale. Add the missing resctrl_cpu_detect() in the Hygon BSP init helper. [bp: Massage commit message.]	N/A	More Details
CVE-2025-9709	On-Chip Debug and Test Interface With Improper Access Control and Improper Protection against Electromagnetic Fault Injection (EM-FI) in Nordic Semiconductor nRF52810 allow attacker to perform EM Fault Injection and bypass APPROTECT at runtime, requiring the least amount of modification to the hardware system possible.	N/A	More Details
CVE-2025-39684	In the Linux kernel, the following vulnerability has been resolved: comedi: Fix use of uninitialized memory in do_insn_ioctl() and do_insnlist_ioctl() syzbot reports a KMSAN kernel-infoleak in `do_insn_ioctl()`. A kernel buffer is allocated to hold `insn->n` samples (each of which is an `unsigned int`). For some instruction types, `insn->n` samples are copied back to user-space, unless an error code is being returned. The problem is that not all the instruction handlers that need to return data to userspace fill in the whole `insn->n` samples, so that there is an information leak. There is a similar syzbot report for `do_insnlist_ioctl()`, although it does not have a reproducer for it at the time of writing. One culprit is `insn_rw_emulate_bits()` which is used as the handler for `INSN_READ` or `INSN_WRITE` instructions for subdevices that do not have a specific handler for that instruction, but do have an `INSN_BITS` handler. For `INSN_READ` it only fills in at most 1 sample, so if `insn->n` is greater than 1, the remaining `insn->n - 1` samples copied to userspace will be uninitialized kernel data. Another culprit is `vm80xx_ai_insn_read()` in the "vm80xx" driver. It never returns an error, even if it fails to fill the buffer. Fix it in `do_insn_ioctl()` and `do_insnlist_ioctl()` by making sure that uninitialized parts of the allocated buffer are zeroed before handling each instruction. Thanks to Arnaud Lecomte for their fix to `do_insn_ioctl()`. That fix replaced the call to `kmalloc_array()` with `kcalloc()`, but it is not always necessary to clear the whole buffer.	N/A	More Details
CVE-2025-39674	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: ufs-qcom: Fix ESI null pointer dereference ESI/MSI is a performance optimization feature that provides dedicated interrupts per MCQ hardware queue. This is optional feature and UFS MCQ should work with and without ESI feature. Commit e46a28cea29a ("scsi: ufs: qcom: Remove the MSI descriptor abuse") brings a regression in ESI (Enhanced System Interrupt) configuration that causes a null pointer dereference when Platform MSI allocation fails. The issue occurs in when platform_device_msi_init_and_alloc_irqs() in ufs_qcom_config_esi() fails (returns -EINVAL) but the current code uses __free() macro for automatic cleanup free MSI resources that were never successfully allocated. Unable to handle kernel NULL pointer dereference at virtual address 0000000000000008 Call trace: mutex_lock+0xc/0x54 (P) platform_device_msi_free_irqs_all+0x1c/0x40 ufs_qcom_config_esi+0x1d0/0x220 [ufs_qcom] ufshcd_config_mcq+0x28/0x104 ufshcd_init+0xa3c/0xf40 ufshcd_pltfrm_init+0x504/0x7d4 ufs_qcom_probe+0x20/0x58 [ufs_qcom] Fix by restructuring the ESI configuration to try MSI allocation first, before any other resource allocation and instead use explicit cleanup instead of __free() macro to avoid cleanup of unallocated resources. Tested on SM8750 platform with MCQ enabled, both with and without Platform ESI support.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: comedi: pcl726: Prevent invalid irq number The reproducer passed in an irq number(0x80008000) that was too large, which triggered the oob. Added an interrupt number check to prevent users from passing in an irq number that was too large. If `it->options[1]` is 31, then `1		

2025-39685	<< it->options[1]` is still invalid because it shifts a 1-bit into the sign bit (which is UB in C). Possible solutions include reducing the upper bound on the `it->options[1]` value to 30 or lower, or using `1U << it->options[1]`. The old code would just not attempt to request the IRQ if the `options[1]` value were invalid. And it would still configure the device without interrupts even if the call to `request_irq` returned an error. So it would be better to combine this test with the test below.	N/A	More Details
CVE-2025-39686	In the Linux kernel, the following vulnerability has been resolved: comedi: Make insn_rw_emulate_bits() do insn->n samples The `insn_rw_emulate_bits()` function is used as a default handler for `INSN_READ` instructions for subdevices that have a handler for `INSN_BITS` but not for `INSN_READ`. Similarly, it is used as a default handler for `INSN_WRITE` instructions for subdevices that have a handler for `INSN_BITS` but not for `INSN_WRITE`. It works by emulating the `INSN_READ` or `INSN_WRITE` instruction handling with a constructed `INSN_BITS` instruction. However, `INSN_READ` and `INSN_WRITE` instructions are supposed to be able read or write multiple samples, indicated by the `insn->n` value, but `insn_rw_emulate_bits()` currently only handles a single sample. For `INSN_READ`, the comedi core will copy `insn->n` samples back to user-space. (That triggered KASAN kernel-infoleak errors when `insn->n` was greater than 1, but that is being fixed more generally elsewhere in the comedi core.) Make `insn_rw_emulate_bits()` either handle `insn->n` samples, or return an error, to conform to the general expectation for `INSN_READ` and `INSN_WRITE` handlers.	N/A	More Details
CVE-2025-39687	In the Linux kernel, the following vulnerability has been resolved: iio: light: as73211: Ensure buffer holes are zeroed Given that the buffer is copied to a kfifo that ultimately user space can read, ensure we zero it.	N/A	More Details
CVE-2025-58272	Cross-site request forgery vulnerability exists in Web Caster V130 versions 1.08 and earlier. If a logged-in user views a malicious page created by an attacker, the settings of the product may be unintentionally changed.	N/A	More Details
CVE-2025-39689	In the Linux kernel, the following vulnerability has been resolved: ftrace: Also allocate and copy hash for reading of filter files Currently the reader of set_ftrace_filter and set_ftrace_notrace just adds the pointer to the global tracer hash to its iterator. Unlike the writer that allocates a copy of the hash, the reader keeps the pointer to the filter hashes. This is problematic because this pointer is static across function calls that release the locks that can update the global tracer hashes. This can cause UAF and similar bugs. Allocate and copy the hash for reading the filter files like it is done for the writers. This not only fixes UAF bugs, but also makes the code a bit simpler as it doesn't have to differentiate when to free the iterator's hash between writers and readers.	N/A	More Details
CVE-2025-8663	Insertion of Sensitive Information into Log File vulnerability in upKeeper Solutions upKeeper Manager allows Use of Known Domain Credentials.This issue affects upKeeper Manager: from 5.0.0 before 5.2.12.	N/A	More Details
CVE-2025-39690	In the Linux kernel, the following vulnerability has been resolved: iio: accel: sca3300: fix uninitialized iio scan data Fix potential leak of uninitialized stack data to userspace by ensuring that the `channels` array is zeroed before use.	N/A	More Details
CVE-2025-39691	In the Linux kernel, the following vulnerability has been resolved: fs/buffer: fix use-after-free when call bh_read() helper There's issue as follows: BUG: KASAN: stack-out-of-bounds in end_buffer_read_sync+0xe3/0x110 Read of size 8 at addr ffffc9000168f7f8 by task swapper/3/0 CPU: 3 UID: 0 PID: 0 Comm: swapper/3 Not tainted 6.16.0-862.14.0.6.x86_64 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996) Call Trace: <IRQ> dump_stack_lvl+0x55/0x70 print_address_description.constprop.0+0x2c/0x390 print_report+0xb4/0x270 kasan_report+0xb8/0xf0 end_buffer_read_sync+0xe3/0x110 end_bio_bh_io_sync+0x56/0x80 blk_update_request+0x30a/0x720 scsi_end_request+0x51/0x2b0 scsi_io_completion+0xe3/0x480 ? scsi_device_unbusy+0x11e/0x160 blk_complete_reqs+0x7b/0x90 handle_softirqs+0xef/0x370 irq_exit_rcu+0xa5/0xd0 sysvec_apic_timer_interrupt+0x6e/0x90 </IRQ> Above issue happens when do ntfs3 filesystem mount, issue may happens as follows: mount IRQ ntfs_fill_super read_cache_page do_read_cache_folio filemap_read_folio mpage_read_folio do_mpage_readpage ntfs_get_block_vbo bh_read submit_bh wait_on_buffer(bh); blk_complete_reqs scsi_io_completion scsi_end_request blk_update_request end_bio_bh_io_sync end_buffer_read_sync __end_buffer_read_notouch unlock_buffer wait_on_buffer(bh);--> return will return to caller put_bh --> trigger stack-out-of-bounds In the mpage_read_folio() function, the stack variable 'map_bh' is passed to ntfs_get_block_vbo(). Once unlock_buffer() unlocks and wait_on_buffer() returns to continue processing, the stack variable is likely to be reclaimed. Consequently, during the end_buffer_read_sync() process, calling put_bh() may result in stack overrun. If the bh is not allocated on the stack, it belongs to a folio. Freeing a buffer head which belongs to a folio is done by drop_buffers() which will fail to free buffers which are still locked. So it is safe to call put_bh() before __end_buffer_read_notouch().	N/A	More Details
CVE-2025-9269	A Server-Side Request Forgery (SSRF) vulnerability has been identified in the embedded web server in various Lexmark devices. This vulnerability can be leveraged by an attacker to force the device to send an arbitrary HTTP request to a third-party server. Successful exploitation of this vulnerability can lead to internal network access / potential data disclosure from a device.	N/A	More Details
CVE-2025-29089	An issue in TP-Link AX10 Ax1500 v.1.3.10 Build (20230130) allows a remote attacker to obtain sensitive information	N/A	More Details
CVE-2025-43775	Stored cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.0 through 7.4.3.128, and Liferay DXP 2024.Q3.0 through 2024.Q3.5, 2024.Q2.0 through 2024.Q2.12, 2024.Q1.1 through 2024.Q1.12, and 7.4 GA through update 92 allows remote attackers to inject arbitrary web script or HTML via remote app title field.	N/A	More Details

CVE-2025-43781	Reflected cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.3.110 through 7.4.3.128, and Liferay DXP 2024.Q3.1 through 2024.Q3.8, 2024.Q2.0 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.12 allows remote attackers to inject arbitrary web script or HTML via the URL in search bar portlet	N/A	More Details
CVE-2025-39675	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null pointer check in mod_hdcp_hdcp1_create_session() The function mod_hdcp_hdcp1_create_session() calls the function get_first_active_display(), but does not check its return value. The return value is a null pointer if the display list is empty. This will lead to a null pointer dereference. Add a null pointer check for get_first_active_display() and return MOD_HDCP_STATUS_DISPLAY_NOT_FOUND if the function return null. This is similar to the commit c3e9826a2202 ("drm/amd/display: Add null pointer check for get_first_active_display()"). (cherry picked from commit 5e43eb3cd731649c4f8b9134f857be62a416c893)	N/A	More Details
CVE-2025-53914	Excessive Privileges vulnerability in Calix GigaCenter ONT (Broadcom SoC modules) allows Privilege Abuse.This issue affects GigaCenter ONT: 844E, 844G, 844GE, 854GE, 812G, 813G, 818G.	N/A	More Details
CVE-2025-53913	Excessive Privileges vulnerability in Calix GigaCenter ONT (Quantenna SoC modules) allows Privilege Abuse.This issue affects GigaCenter ONT: 844E, 844G, 844GE, 854GE, 812G, 813G, 818G.	N/A	More Details
CVE-2025-47415	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in CRESTRON TOUCHSCREENS x70 allows Relative Path Traversal.This issue affects TOUCHSCREENS x70: from 3.000.0110.001 before 3.001.0031.001. Confirmed Affected Hardware: TSW-760, TSW-1060 Confirmed Affected Firmware: 3.002.1061 - (no fix released, product discontinued) For x70 The Affected Firmware:- 3.000.0110.001 and versions below The Fixed Firmware:- 3.001.0031.001	N/A	More Details
CVE-2025-44594	halo v2.20.17 and before is vulnerable to server-side request forgery (SSRF) in /apis/uc.api.storage.halo.run/v1alpha1/attachments/-/upload-from-url.	N/A	More Details
CVE-2025-43786	Enumeration of ERC from object entry in Liferay Portal 7.4.0 through 7.4.3.128, and Liferay DXP 2024.Q3.0 through 2024.Q3.1, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12, 2023.Q4.0 and 7.4 GA through update 92 allow attackers to determine existent ERC in the application by exploit the time response.	N/A	More Details
CVE-2025-39676	In the Linux kernel, the following vulnerability has been resolved: scsi: qla4xxx: Prevent a potential error pointer dereference The qla4xxx_get_ep_fwdb() function is supposed to return NULL on error, but qla4xxx_ep_connect() returns error pointers. Propagating the error pointers will lead to an Oops in the caller, so change the error pointers to NULL.	N/A	More Details
CVE-2025-39677	In the Linux kernel, the following vulnerability has been resolved: net/sched: Fix backlog accounting in qdisc_dequeue_internal This issue applies for the following qdiscs: hhf, fq, fq_codel, and fq_pie, and occurs in their change handlers when adjusting to the new limit. The problem is the following in the values passed to the subsequent qdisc_tree_reduce_backlog call given a tbf parent: When the tbf parent runs out of tokens, skbs of these qdiscs will be placed in gso_skb. Their peek handlers are qdisc_peek_dequeued, which accounts for both qlen and backlog. However, in the case of qdisc_dequeue_internal, ONLY qlen is accounted for when pulling from gso_skb. This means that these qdiscs are missing a qdisc_qstats_backlog_dec when dropping packets to satisfy the new limit in their change handlers. One can observe this issue with the following (with tc patched to support a limit of 0): export TARGET=fq tc qdisc del dev lo root tc qdisc add dev lo root handle 1: tbf rate 8bit burst 100b latency 1ms tc qdisc replace dev lo handle 3: parent 1:1 $TARGET limit 1000 echo ''; echo 'add child'; tc -s -d qdisc show dev lo ping -I lo -f -c2 -s32 -W0.001 127.0.0.1 2>&1 >/dev/null echo ''; echo 'after ping'; tc -s -d qdisc show dev lo tc qdisc change dev lo handle 3: parent 1:1 $TARGET limit 0 echo ''; echo 'after limit drop'; tc -s -d qdisc show dev lo tc qdisc replace dev lo handle 2: parent 1:1 sfq echo ''; echo 'post graft'; tc -s -d qdisc show dev lo The second to last show command shows 0 packets but a positive number (74) of backlog bytes. The problem becomes clearer in the last show command, where qdisc_purge_queue triggers qdisc_tree_reduce_backlog with the positive backlog and causes an underflow in the tbf parent's backlog (4096 Mb instead of 0). To fix this issue, the codepath for all clients of qdisc_dequeue_internal has been simplified: codel, pie, hhf, fq, fq_pie, and fq_codel. qdisc_dequeue_internal handles the backlog adjustments for all cases that do not directly use the dequeue handler. The old fq_codel_change limit adjustment loop accumulated the arguments to the subsequent qdisc_tree_reduce_backlog call through the cstats field. However, this is confusing and error prone as fq_codel_dequeue could also potentially mutate this field (which qdisc_dequeue_internal calls in the non gso_skb case), so we have unified the code here with other qdiscs.	N/A	More Details
CVE-2025-34175	In pfSense CE /usr/local/www/suricata/suricata_filecheck.php, the value of the filehash parameter is directly displayed without sanitizing for HTML-related characters/strings. This can result in reflected cross-site scripting if the victim is authenticated.	N/A	More Details
CVE-2025-34174	In pfSense CE /usr/local/www/status_traffic_totals.php, the value of the start-day parameter is not ensured to be a numeric value or sanitized of HTML-related characters/strings before being directly displayed in the input box. This value can be saved as the default value to be displayed to all users when visiting the Status Traffic Totals page, resulting in stored cross-site scripting. The attacker must be authenticated with at least "WebCfg - Status: Traffic Totals" permissions.	N/A	More Details
CVE-2025-34173	In pfSense CE /usr/local/www/snort/snort_ip_reputation.php, the value of the iplist parameter is not sanitized of directory traversal-related characters/strings before being used to check if a file exists. While the contents of the file cannot be read, the server reveals whether a file exists, which allows an attacker to enumerate files on the target. The attacker must be authenticated with at least "WebCfg - Services: Snort package" permissions.	N/A	More Details

CVE-2025-34172	In pfSense CE /usr/local/www/haproxy/haproxy_stats.php, the value of the showsticktablecontent parameter is displayed after being read from HTTP GET requests. This can enable reflected cross-site scripting when the victim is authenticated.	N/A	More Details
CVE-2025-57278	The LB-Link BL-CPE300M AX300 4G LTE Router firmware version BL-R8800_B10_ALK_SL_V01.01.02P42U14_06 does not implement proper session handling. After a user authenticates from a specific IP address, the router grants access to any other client using that same IP, without requiring credentials or verifying client identity. There are no session tokens, cookies, or unique identifiers in place. This flaw allows an attacker to obtain full administrative access simply by configuring their device to use the same IP address as a previously authenticated user. This results in a complete authentication bypass.	N/A	More Details
CVE-2025-57060	Tenda G3 v3.0br_V15.11.0.17 was discovered to contain a stack overflow in the rules parameter in the dns_forward_rule_store function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-39678	In the Linux kernel, the following vulnerability has been resolved: platform/x86/amd/hsmp: Ensure sock->metric_tbl_addr is non-NULL If metric table address is not allocated, accessing metrics_bin will result in a NULL pointer dereference, so add a check.	N/A	More Details
CVE-2025-39679	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau/nvif: Fix potential memory leak in nvif_vmm_ctor(). When the nvif_vmm_type is invalid, we will return error directly without freeing the args in nvif_vmm_ctor(), which leading a memory leak. Fix it by setting the ret -EINVAL and goto done.	N/A	More Details
CVE-2025-39680	In the Linux kernel, the following vulnerability has been resolved: i2c: rtl9300: Fix out-of-bounds bug in rtl9300_i2c_smbus_xfer The data->block[0] variable comes from user. Without proper check, the variable may be very large to cause an out-of-bounds bug. Fix this bug by checking the value of data->block[0] first. 1. commit 39244cc75482 ("i2c: ismt: Fix an out-of-bounds bug in ismt_access()") 2. commit 92fbb6d1296f ("i2c: xgene-slimpro: Fix out-of-bounds bug in xgene_slimpro_i2c_xfer()")	N/A	More Details
CVE-2025-39726	In the Linux kernel, the following vulnerability has been resolved: s390/ism: fix concurrency management in ism_cmd() The s390x ISM device data sheet clearly states that only one request-response sequence is allowable per ISM function at any point in time. Unfortunately as of today the s390/ism driver in Linux does not honor that requirement. This patch aims to rectify that. This problem was discovered based on Aliaksei's bug report which states that for certain workloads the ISM functions end up entering error state (with PEC 2 as seen from the logs) after a while and as a consequence connections handled by the respective function break, and for future connection requests the ISM device is not considered -- given it is in a dysfunctional state. During further debugging PEC 3A was observed as well. A kernel message like [1211.244319] zpci: 061a:00:00.0: Event 0x2 reports an error for PCI function 0x61a is a reliable indicator of the stated function entering error state with PEC 2. Let me also point out that a kernel message like [1211.244325] zpci: 061a:00:00.0: The ism driver bound to the device does not support error recovery is a reliable indicator that the ISM function won't be auto-recovered because the ISM driver currently lacks support for it. On a technical level, without this synchronization, commands (inputs to the FW) may be partially or fully overwritten (corrupted) by another CPU trying to issue commands on the same function. There is hard evidence that this can lead to DMB token values being used as DMB IOVAs, leading to PEC 2 PCI events indicating invalid DMA. But this is only one of the failure modes imaginable. In theory even completely losing one command and executing another one twice and then trying to interpret the outputs as if the command we intended to execute was actually executed and not the other one is also possible. Frankly, I don't feel confident about providing an exhaustive list of possible consequences.	N/A	More Details
CVE-2025-38707	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Add sanity check for file name The length of the file name should be smaller than the directory entry size.	N/A	More Details
CVE-2025-55037	Improper neutralization of special elements used in an OS command ('OS Command Injection') issue exists in TkEasyGUI versions prior to v1.0.22. If this vulnerability is exploited, an arbitrary OS command may be executed by a remote unauthenticated attacker if the settings are configured to construct messages from external sources.	N/A	More Details
CVE-2025-38709	In the Linux kernel, the following vulnerability has been resolved: loop: Avoid updating block size under exclusive owner Syzbot came up with a reproducer where a loop device block size is changed underneath a mounted filesystem. This causes a mismatch between the block device block size and the block size stored in the superblock causing confusion in various places such as fs/buffer.c. The particular issue triggered by syzbot was a warning in __getblk_slow() due to requested buffer size not matching block device block size. Fix the problem by getting exclusive hold of the loop device to change its block size. This fails if somebody (such as filesystem) has already an exclusive ownership of the block device and thus prevents modifying the loop device under some exclusive owner which doesn't expect it.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: hfsplus: fix slab-out-of-bounds read in hfsplus_uni2asc() The hfsplus_readdir() method is capable to crash by calling hfsplus_uni2asc(): [667.121659][T9805] == [667.122651][T9805] BUG: KASAN: slab-out-of-bounds in hfsplus_uni2asc+0x902/0xa10 [667.123627][T9805] Read of size 2 at addr ffff88802592f40c by task repro/9805 [667.124578][T9805] [667.124876][T9805] CPU: 3 UID: 0 PID: 9805 Comm: repro Not tainted 6.16.0-rc3 #1 PREEMPT(full) [667.124886][T9805] Hardware name: QEMU Ubuntu 24.04 PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [667.124890][T9805] Call Trace: [667.124893][T9805] <TASK> [667.124896][T9805] dump_stack_lvl+0x10e/0x1f0 [667.124911][T9805] print_report+0xd0/0x660 [667.124920][T9805] ? __virt_addr_valid+0x81/0x610 [667.124928][T9805] ?		

CVE-2025-38713	__phys_addr+0xe8/0x180 [667.124934][T9805] ? hfsplus_uni2asc+0x902/0xa10 [667.124942][T9805] kasan_report+0xc6/0x100 [667.124950][T9805] ? hfsplus_uni2asc+0x902/0xa10 [667.124959][T9805] hfsplus_uni2asc+0x902/0xa10 [667.124966][T9805] ? hfsplus_bnode_read+0x14b/0x360 [667.124974][T9805] hfsplus_readdir+0x845/0xfc0 [667.124984][T9805] ? __pfx_hfsplus_readdir+0x10/0x10 [667.124994][T9805] ? stack_trace_save+0x8e/0xc0 [667.125008][T9805] ? iterate_dir+0x18b/0xb20 [667.125015][T9805] ? trace_lock_acquire+0x85/0xd0 [667.125022][T9805] ? lock_acquire+0x30/0x80 [667.125029][T9805] ? iterate_dir+0x18b/0xb20 [667.125037][T9805] ? down_read_killable+0x1ed/0x4c0 [667.125044][T9805] ? putname+0x154/0x1a0 [667.125051][T9805] ? __pfx_down_read_killable+0x10/0x10 [667.125058][T9805] ? apparmor_file_permission+0x239/0x3e0 [667.125069][T9805] iterate_dir+0x296/0xb20 [667.125076][T9805] __x64_sys_getdents64+0x13c/0x2c0 [667.125084][T9805] ? __pfx___x64_sys_getdents64+0x10/0x10 [667.125091][T9805] ? __x64_sys_openat+0x141/0x200 [667.125126][T9805] ? __pfx_filldir64+0x10/0x10 [667.125134][T9805] ? do_user_addr_fault+0x7fe/0x12f0 [667.125143][T9805] do_syscall_64+0xc9/0x480 [667.125151][T9805] entry_SYSCALL_64_after_hwframe+0x77/0x7f [667.125158][T9805] RIP: 0033:0x7fa8753b2fc9 [667.125164][T9805] Code: 00 c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 48 [667.125172][T9805] RSP: 002b:00007ffe96f8e0f8 EFLAGS: 00000217 ORIG_RAX: 00000000000000d9 [667.125181][T9805] RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007fa8753b2fc9 [667.125185][T9805] RDX: 0000000000000400 RSI: 00002000000063c0 RDI: 0000000000000004 [667.125190][T9805] RBP: 00007ffe96f8e110 R08: 00007ffe96f8e110 R09: 00007ffe96f8e110 [667.125195][T9805] R10: 0000000000000000 R11: 0000000000000217 R12: 0000556b1e3b4260 [667.125199][T9805] R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 [667.125207][T9805] </TASK> [667.125210][T9805] [667.145632][T9805] Allocated by task 9805: [667.145991][T9805] kasan_save_stack+0x20/0x40 [667.146352][T9805] kasan_save_track+0x14/0x30 [667.146717][T9805] __kasan_kmalloc+0xaa/0xb0 [667.147065][T9805] __kmalloc_noprof+0x205/0x550 [667.147448][T9805] hfsplus_find_init+0x95/0x1f0 [667.147813][T9805] hfsplus_readdir+0x220/0xfc0 [667.148174][T9805] iterate_dir+0x296/0xb20 [667.148549][T9805] __x64_sys_getdents64+0x13c/0x2c0 [667.148937][T9805] do_syscall_64+0xc9/0x480 [667.149291][T9805] entry_SYSCALL_64_after_hwframe+0x77/0x7f [667.149809][T9805] [667.150030][T9805] The buggy address belongs to the object at ffff88802592f000 [667.150030][T9805] which belongs to the cache kmalloc-2k of size 2048 [667.151282][T9805] The buggy address is located 0 bytes to the right of [667.151282][T9805] allocated 1036-byte region [ffff88802592f000, ffff88802592f40c) [667.1 ---truncated---	N/A	More Details
CVE-2022-50238	The on-endpoint Microsoft vulnerable driver blocklist is not fully synchronized with the online Microsoft recommended driver block rules. Some entries present on the online list have been excluded from the on-endpoint blocklist longer than the expected periodic monthly Windows updates. It is possible to fully synchronize the driver blocklist using WDAC policies. NOTE: The vendor explains that Windows Update provides a smaller, compatibility-focused driver blocklist for general users, while the full XML list is available for advanced users and organizations to customize at the risk of usability issues.	N/A	More Details
CVE-2025-6785	Securing externally available CAN wires can easily allow physical access to the CAN bus, allowing possible injection of specially formed CAN messages to control remote start functions of the vehicle. Testing completed on Tesla Model 3 vehicles with software version v11.1 (2023.20.9 ee6de92ddac5). This issue affects Model 3: With software versions from 2023.Xx before 2023.44.	N/A	More Details
CVE-2025-38712	In the Linux kernel, the following vulnerability has been resolved: hfsplus: don't use BUG_ON() in hfsplus_create_attributes_file() When the volume header contains erroneous values that do not reflect the actual state of the filesystem, hfsplus_fill_super() assumes that the attributes file is not yet created, which later results in hitting BUG_ON() when hfsplus_create_attributes_file() is called. Replace this BUG_ON() with -EIO error with a message to suggest running fsck tool.	N/A	More Details
CVE-2025-8311	dotCMS versions 24.03.22 and after, identified a Boolean-based blind SQLi vulnerability in the /api/v1/contenttype endpoint. This endpoint uses the sites query parameter, which accepts a comma-separated list of site identifiers or keys. The vulnerability was triggered via the sites parameter, which was directly concatenated into a SQL query without proper sanitization. Exploitation allowed an authenticated attacker with low privileges to extract data from database, perform privilege escalation, or trigger denial-of-service conditions. The vulnerability was verified using tools such as SQLMap and confirmed to allow full database exfiltration and potential denial-of-service conditions via crafted payloads. The vulnerability is fixed in the following versions of dotCMS stack: 25.08.14 / 25.07.10-1v2 LTS / 24.12.27v10 LTS / 24.04.24v21 LTS	N/A	More Details
CVE-2025-38711	In the Linux kernel, the following vulnerability has been resolved: smb/server: avoid deadlock when linking with ReplaceIfExists If smb2_create_link() is called with ReplaceIfExists set and the name does exist then a deadlock will happen. ksmbd_vfs_kern_path_locked() will return with success and the parent directory will be locked. ksmbd_vfs_remove_file() will then remove the file. ksmbd_vfs_link() will then be called while the parent is still locked. It will try to lock the same parent and will deadlock. This patch moves the ksmbd_vfs_kern_path_unlock() call to *before* ksmbd_vfs_link() and then simplifies the code, removing the file_present flag variable.	N/A	More Details
CVE-2025-38710	In the Linux kernel, the following vulnerability has been resolved: gfs2: Validate i_depth for exhash directories A fuzzer test introduced corruption that ends up with a depth of 0 in dir_e_read(), causing an undefined shift by 32 at: index = hash >> (32 - dip->i_depth); As calculated in an open-coded way in dir_make_exhash(), the minimum depth for an exhash directory is ilog2(sdp->sd_hash_ptrs) and 0 is invalid as sdp->sd_hash_ptrs is fixed as sdp->bsize / 16 at mount time. So we can avoid the undefined behaviour by checking for depth values lower than the minimum in gfs2_dinode_in(). Values greater than the maximum are already being checked for there. Also switch the calculation in dir_make_exhash() to use ilog2() to clarify how the depth is calculated. Tested with the syzkaller repro.c and xfstests '-g quick'.	N/A	More Details

CVE-2025-7709	An integer overflow exists in the FTS5 https://sqlite.org/fts5.html extension. It occurs when the size of an array of tombstone pointers is calculated and truncated into a 32-bit integer. A pointer to partially controlled data can then be written out of bounds.	N/A	More Details
CVE-2025-38715	In the Linux kernel, the following vulnerability has been resolved: hfs: fix slab-out-of-bounds in hfs_bnode_read() This patch introduces is_bnode_offset_valid() method that checks the requested offset value. Also, it introduces check_and_correct_requested_length() method that checks and correct the requested length (if it is necessary). These methods are used in hfs_bnode_read(), hfs_bnode_write(), hfs_bnode_clear(), hfs_bnode_copy(), and hfs_bnode_move() with the goal to prevent the access out of allocated memory and triggering the crash.	N/A	More Details
CVE-2025-38708	In the Linux kernel, the following vulnerability has been resolved: drbd: add missing kref_get in handle_write_conflicts With `two-primaries` enabled, DRBD tries to detect "concurrent" writes and handle write conflicts, so that even if you write to the same sector simultaneously on both nodes, they end up with the identical data once the writes are completed. In handling "superseeded" writes, we forgot a kref_get, resulting in a premature drbd_destroy_device and use after free, and further to kernel crashes with symptoms. Relevance: No one should use DRBD as a random data generator, and apparently all users of "two-primaries" handle concurrent writes correctly on layer up. That is cluster file systems use some distributed lock manager, and live migration in virtualization environments stops writes on one node before starting writes on the other node. Which means that other than for "test cases", this code path is never taken in real life. FYI, in DRBD 9, things are handled differently nowadays. We still detect "write conflicts", but no longer try to be smart about them. We decided to disconnect hard instead: upper layers must not submit concurrent writes. If they do, that's their fault.	N/A	More Details
CVE-2025-38679	In the Linux kernel, the following vulnerability has been resolved: media: venus: Fix OOB read due to missing payload bound check Currently, The event_seq_changed() handler processes a variable number of properties sent by the firmware. The number of properties is indicated by the firmware and used to iterate over the payload. However, the payload size is not being validated against the actual message length. This can lead to out-of-bounds memory access if the firmware provides a property count that exceeds the data available in the payload. Such a condition can result in kernel crashes or potential information leaks if memory beyond the buffer is accessed. Fix this by properly validating the remaining size of the payload before each property access and updating bounds accordingly as properties are parsed. This ensures that property parsing is safely bounded within the received message buffer and protects against malformed or malicious firmware behavior.	N/A	More Details
CVE-2025-38680	In the Linux kernel, the following vulnerability has been resolved: media: uvcvideo: Fix 1-byte out-of-bounds read in uvc_parse_format() The buffer length check before calling uvc_parse_format() only ensured that the buffer has at least 3 bytes (buflen > 2), buf the function accesses buffer[3], requiring at least 4 bytes. This can lead to an out-of-bounds read if the buffer has exactly 3 bytes. Fix it by checking that the buffer has at least 4 bytes in uvc_parse_format().	N/A	More Details
CVE-2025-38681	In the Linux kernel, the following vulnerability has been resolved: mm/ptdump: take the memory hotplug lock inside ptdump_walk_pgd() Memory hot remove unmaps and tears down various kernel page table regions as required. The ptdump code can race with concurrent modifications of the kernel page tables. When leaf entries are modified concurrently, the dump code may log stale or inconsistent information for a VA range, but this is otherwise not harmful. But when intermediate levels of kernel page table are freed, the dump code will continue to use memory that has been freed and potentially reallocated for another purpose. In such cases, the ptdump code may dereference bogus addresses, leading to a number of potential problems. To avoid the above mentioned race condition, platforms such as arm64, riscv and s390 take memory hotplug lock, while dumping kernel page table via the sysfs interface /sys/kernel/debug/kernel_page_tables. Similar race condition exists while checking for pages that might have been marked W+X via /sys/kernel/debug/kernel_page_tables/check_wx_pages which in turn calls ptdump_check_wx(). Instead of solving this race condition again, let's just move the memory hotplug lock inside generic ptdump_check_wx() which will benefit both the scenarios. Drop get_online_mems() and put_online_mems() combination from all existing platform ptdump code paths.	N/A	More Details
CVE-2025-43774	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.17 allows a remote authenticated user to inject JavaScript code via Style Book theme name. This malicious payload is then reflected and executed within the user's browser.	N/A	More Details
CVE-2025-38682	In the Linux kernel, the following vulnerability has been resolved: i2c: core: Fix double-free of fwnode in i2c_unregister_device() Before commit df6d7277e552 ("i2c: core: Do not dereference fwnode in struct device"), i2c_unregister_device() only called fwnode_handle_put() on of_node-s in the form of calling of_node_put(client->dev.of_node). But after this commit the i2c_client's fwnode now unconditionally gets fwnode_handle_put() on it. When the i2c_client has no primary (ACPI / OF) fwnode but it does have a software fwnode, the software-node will be the primary node and fwnode_handle_put() will put() it. But for the software fwnode device_remove_software_node() will also put() it leading to a double free: [82.665598] ------------[cut here]------------ [82.665609] refcount_t: underflow; use-after-free. [82.665808] WARNING: CPU: 3 PID: 1502 at lib/refcount.c:28 refcount_warn_saturate+0xba/0x11 ... [82.666830] RIP: 0010:refcount_warn_saturate+0xba/0x110 ... [82.666962] <TASK> [82.666971] i2c_unregister_device+0x60/0x90 Fix this by not calling fwnode_handle_put() when the primary fwnode is a software-node.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: hv_netvsc: Fix panic during namespace deletion with VF The existing code move the VF NIC to new namespace when NETDEV_REGISTER is received on netvsc NIC. During deletion of the namespace, default_device_exit_batch() >> default_device_exit_net() is called. When netvsc NIC is moved back and registered to the default namespace, it automatically brings VF NIC back to the default namespace. This will cause the default_device_exit_net() >> for_each_netdev_safe loop unable to detect the list end, and hit NULL ptr: [231.449420] mana 7870:00:00.0 enP30832s1: Moved VF to namespace with: eth0 [		

CVE-2025-38683	231.449656] BUG: kernel NULL pointer dereference, address: 0000000000000010 [231.450246] #PF: supervisor read access in kernel mode [231.450579] #PF: error_code(0x0000) - not-present page [231.450916] PGD 17b8a8067 P4D 0 [231.451163] Oops: Oops: 0000 [#1] SMP NOPTI [231.451450] CPU: 82 UID: 0 PID: 1394 Comm: kworker/u768:1 Not tainted 6.16.0-rc4+ #3 VOLUNTARY [231.452042] Hardware name: Microsoft Corporation Virtual Machine/Virtual Machine, BIOS Hyper-V UEFI Release v4.1 11/21/2024 [231.452692] Workqueue: netns cleanup_net [231.452947] RIP: 0010:default_device_exit_batch+0x16c/0x3f0 [231.453326] Code: c0 0c f5 b3 e8 d5 db fe ff 48 85 c0 74 15 48 c7 c2 f8 fd ca b2 be 10 00 00 00 48 8d 7d c0 e8 7b 77 25 00 49 8b 86 28 01 00 00 <48> 8b 50 10 4c 8b 2a 4c 8d 62 f0 49 83 ed 10 4c 39 e0 0f 84 d6 00 [231.454294] RSP: 0018:ff75fc7c9bf9fd00 EFLAGS: 00010246 [231.454610] RAX: 0000000000000000 RBX: 0000000000000002 RCX: 61c8864680b583eb [231.455094] RDX: ff1fa9f71462d800 RSI: ff75fc7c9bf9fd38 RDI: 0000000030766564 [231.455686] RBP: ff75fc7c9bf9fd78 R08: 0000000000000000 R09: 0000000000000000 [231.456126] R10: 0000000000000001 R11: 0000000000000004 R12: ff1fa9f70088e340 [231.456621] R13: ff1fa9f70088e340 R14: ffffffffb3f50c20 R15: ff1fa9f7103e6340 [231.457161] FS: 0000000000000000(0000) GS:ff1faa6783a08000(0000) knlGS:0000000000000000 [231.457707] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [231.458031] CR2: 0000000000000010 CR3: 0000000179ab2006 CR4: 0000000000b73ef0 [231.458434] Call Trace: [231.458600] <TASK> [231.458777] ops_undo_list+0x100/0x220 [231.459015] cleanup_net+0x1b8/0x300 [231.459285] process_one_work+0x184/0x340 To fix it, move the ns change to a workqueue, and take rtnl_lock to avoid changing the netdev list when default_device_exit_net() is using it.	N/A	More Details
CVE-2025-38714	In the Linux kernel, the following vulnerability has been resolved: hfsplus: fix slab-out-of-bounds in hfsplus_bnode_read() The hfsplus_bnode_read() method can trigger the issue: [174.852007][T9784] == [174.852709][T9784] BUG: KASAN: slab-out-of-bounds in hfsplus_bnode_read+0x2f4/0x360 [174.853412][T9784] Read of size 8 at addr ffff88810b5fc6c0 by task repro/9784 [174.854059][T9784] [174.854272][T9784] CPU: 1 UID: 0 PID: 9784 Comm: repro Not tainted 6.16.0-rc3 #7 PREEMPT(full) [174.854281][T9784] Hardware name: QEMU Ubuntu 24.04 PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [174.854286][T9784] Call Trace: [174.854289][T9784] <TASK> [174.854292][T9784] dump_stack_lvl+0x10e/0x1f0 [174.854305][T9784] print_report+0xd0/0x660 [174.854315][T9784] ? __virt_addr_valid+0x81/0x610 [174.854323][T9784] ? __phys_addr+0xe8/0x180 [174.854330][T9784] ? hfsplus_bnode_read+0x2f4/0x360 [174.854337][T9784] kasan_report+0xc6/0x100 [174.854346][T9784] ? hfsplus_bnode_read+0x2f4/0x360 [174.854354][T9784] hfsplus_bnode_read+0x2f4/0x360 [174.854362][T9784] hfsplus_bnode_dump+0x2ec/0x380 [174.854370][T9784] ? __pfx_hfsplus_bnode_dump+0x10/0x10 [174.854377][T9784] ? hfsplus_bnode_write_u16+0x83/0xb0 [174.854385][T9784] ? srcu_gp_start+0xd0/0x310 [174.854393][T9784] ? __mark_inode_dirty+0x29e/0xe40 [174.854402][T9784] hfsplus_brec_remove+0x3d2/0x4e0 [174.854411][T9784] __hfsplus_delete_attr+0x290/0x3a0 [174.854419][T9784] ? __pfx_hfs_find_1st_rec_by_cnid+0x10/0x10 [174.854427][T9784] ? __pfx___hfsplus_delete_attr+0x10/0x10 [174.854436][T9784] ? __asan_memset+0x23/0x50 [174.854450][T9784] hfsplus_delete_all_attrs+0x262/0x320 [174.854459][T9784] ? __pfx_hfsplus_delete_all_attrs+0x10/0x10 [174.854469][T9784] ? rcu_is_watching+0x12/0xc0 [174.854476][T9784] ? __mark_inode_dirty+0x29e/0xe40 [174.854483][T9784] hfsplus_delete_cat+0x845/0xde0 [174.854493][T9784] ? __pfx_hfsplus_delete_cat+0x10/0x10 [174.854507][T9784] hfsplus_unlink+0x1ca/0x7c0 [174.854516][T9784] ? __pfx_hfsplus_unlink+0x10/0x10 [174.854525][T9784] ? down_write+0x148/0x200 [174.854532][T9784] ? __pfx_down_write+0x10/0x10 [174.854540][T9784] vfs_unlink+0x2fe/0x9b0 [174.854549][T9784] do_unlinkat+0x490/0x670 [174.854557][T9784] ? __pfx_do_unlinkat+0x10/0x10 [174.854565][T9784] ? __might_fault+0xbc/0x130 [174.854576][T9784] ? getname_flags.part.0+0x1c5/0x550 [174.854584][T9784] __x64_sys_unlink+0xc5/0x110 [174.854592][T9784] do_syscall_64+0xc9/0x480 [174.854600][T9784] entry_SYSCALL_64_after_hwframe+0x77/0x7f [174.854608][T9784] RIP: 0033:0x7f6fdf4c3167 [174.854614][T9784] Code: f0 ff ff 73 01 c3 48 8b 0d 26 0d 0e 00 f7 d8 64 89 01 48 83 c8 ff c3 66 2e 0f 1f 84 00 00 00 00 08 [174.854622][T9784] RSP: 002b:00007ffcb948bca8 EFLAGS: 00000206 ORIG_RAX: 0000000000000057 [174.854630][T9784] RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007f6fdf4c3167 [174.854636][T9784] RDX: 00007ffcb948bcc0 RSI: 00007ffcb948bcc0 RDI: 00007ffcb948bd50 [174.854641][T9784] RBP: 00007ffcb948cd90 R08: 0000000000000001 R09: 00007ffcb948bb40 [174.854645][T9784] R10: 00007f6fdf564fc0 R11: 0000000000000206 R12: 0000561e1bc9c2d0 [174.854650][T9784] R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 [174.854658][T9784] </TASK> [174.854661][T9784] [174.879281][T9784] Allocated by task 9784: [174.879664][T9784] kasan_save_stack+0x20/0x40 [174.880082][T9784] kasan_save_track+0x14/0x30 [174.880500][T9784] __kasan_kmalloc+0xaa/0xb0 [174.880908][T9784] __kmalloc_noprof+0x205/0x550 [174.881337][T9784] __hfs_bnode_create+0x107/0x890 [174.881779][T9784] hfsplus_bnode_find+0x2d0/0xd10 [174.882222][T9784] hfsplus_brec_find+0x2b0/0x520 [174.882659][T9784] hfsplus_delete_all_attrs+0x23b/0x3 ---truncated---	N/A	More Details
CVE-2025-7385	Input from search query parameter in GOV CMS is not sanitized properly, leading to a Blind SQL injection vulnerability, which might be exploited by an unauthenticated remote attacker. Versions 4.0 and above are not affected.	N/A	More Details
CVE-2025-41408	Improper authorization in handler for custom URL scheme issue in "Yahoo! Shopping" App for Android versions prior to 14.15.0 allows a remote unauthenticated attacker may lead a user to access an arbitrary website on the vulnerable App. As a result, the user may become a victim of a phishing attack.	N/A	More Details
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: net: hibmcge: fix rtnl deadlock issue Currently, the hibmcge netdev acquires the rtnl_lock in pci_error_handlers.reset_prepare() and releases it in pci_error_handlers.reset_done(). However, in the PCI framework: pci_reset_bus - __pci_reset_slot - pci_slot_save_and_disable_locked - pci_dev_save_and_disable - err_handler->reset_prepare(dev); In pci_slot_save_and_disable_locked(): list_for_each_entry(dev, &slot->bus->devices, bus_list) { if (!dev->slot || dev->slot!= slot) continue; pci_dev_save_and_disable(dev); if (dev->subordinate) pci_bus_save_and_disable_locked(dev->subordinate); } This will iterate through all devices under the current bus and execute err_handler-	N/A	More Details

38720	>reset_prepare(), causing two devices of the hibmcge driver to sequentially request the rtnl_lock, leading to a deadlock. Since the driver now executes netif_device_detach() before the reset process, it will not concurrently with other netdev APIs, so there is no need to hold the rtnl_lock now. Therefore, this patch removes the rtnl_lock during the reset process and adjusts the position of HBG_NIC_STATE_RESETTING to ensure that multiple resets are not executed concurrently.		
CVE-2025-38727	In the Linux kernel, the following vulnerability has been resolved: netlink: avoid infinite retry looping in netlink_unicast() netlink_attachskb() checks for the socket's read memory allocation constraints. Firstly, it has: rmem < READ_ONCE(sk->sk_rcvbuf) to check if the just increased rmem value fits into the socket's receive buffer. If not, it proceeds and tries to wait for the memory under: rmem + skb->truesize > READ_ONCE(sk->sk_rcvbuf) The checks don't cover the case when skb->truesize + sk->sk_rmem_alloc is equal to sk->sk_rcvbuf. Thus the function neither successfully accepts these conditions, nor manages to reschedule the task - and is called in retry loop for indefinite time which is caught as: rcu: INFO: rcu_sched self-detected stall on CPU rcu: 0-....: (25999 ticks this GP) idle=ef2/1/0x4000000000000000 softirq=262269/262269 fqs=6212 (t=26000 jiffies g=230833 q=259957) NMI backtrace for cpu 0 CPU: 0 PID: 22 Comm: kauditd Not tainted 5.10.240 #68 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.17.0-4.fc42 04/01/2014 Call Trace: <IRQ> dump_stack lib/dump_stack.c:120 nmi_cpu_backtrace.cold lib/nmi_backtrace.c:105 nmi_trigger_cpumask_backtrace lib/nmi_backtrace.c:62 rcu_dump_cpu_stacks kernel/rcu/tree_stall.h:335 rcu_sched_clock_irq.cold kernel/rcu/tree.c:2590 update_process_times kernel/time/timer.c:1953 tick_sched_handle kernel/time/tick-sched.c:227 tick_sched_timer kernel/time/tick-sched.c:1399 __hrtimer_run_queues kernel/time/hrtimer.c:1652 hrtimer_interrupt kernel/time/hrtimer.c:1717 __sysvec_apic_timer_interrupt arch/x86/kernel/apic/apic.c:1113 asm_call_irq_on_stack arch/x86/entry/entry_64.S:808 </IRQ> netlink_attachskb net/netlink/af_netlink.c:1234 netlink_unicast net/netlink/af_netlink.c:1349 kauditd_send_queue kernel/audit.c:776 kauditd_thread kernel/audit.c:897 kthread kernel/kthread.c:328 ret_from_fork arch/x86/entry/entry_64.S:304 Restore the original behavior of the check which commit in Fixes accidentally missed when restructuring the code. Found by Linux Verification Center (linuxtesting.org).	N/A	More Details
CVE-2025-38726	In the Linux kernel, the following vulnerability has been resolved: net: ftgmac100: fix potential NULL pointer access in ftgmac100_phy_disconnect After the call to phy_disconnect() netdev->phydev is reset to NULL. So fixed_phy_unregister() would be called with a NULL pointer as argument. Therefore cache the phy_device before this call.	N/A	More Details
CVE-2025-38725	In the Linux kernel, the following vulnerability has been resolved: net: usb: asix_devices: add phy_mask for ax88772 mdio bus Without setting phy_mask for ax88772 mdio bus, current driver may create at most 32 mdio phy devices with phy address range from 0x00 ~ 0x1f. DLink DUB-E100 H/W Ver B1 is such a device. However, only one main phy device will bind to net phy driver. This is creating issue during system suspend/resume since phy_polling_mode() in phy_state_machine() will directly deference member of phydev->drv for non-main phy devices. Then NULL pointer dereference issue will occur. Due to only external phy or internal phy is necessary, add phy_mask for ax88772 mdio bus to workarnoud the issue.	N/A	More Details
CVE-2025-38724	In the Linux kernel, the following vulnerability has been resolved: nfsd: handle get_client_locked() failure in nfsd4_setclientid_confirm() Lei Lu recently reported that nfsd4_setclientid_confirm() did not check the return value from get_client_locked(). a SETCLIENTID_CONFIRM could race with a confirmed client expiring and fail to get a reference. That could later lead to a UAF. Fix this by getting a reference early in the case where there is an extant confirmed client. If that fails then treat it as if there were no confirmed client found at all. In the case where the unconfirmed client is expiring, just fail and return the result from get_client_locked().	N/A	More Details
CVE-2025-38723	In the Linux kernel, the following vulnerability has been resolved: LoongArch: BPF: Fix jump offset calculation in tailcall The extra pass of bpf_int_jit_compile() skips JIT context initialization which essentially skips offset calculation leaving out_offset = -1, so the jmp_offset in emit_bpf_tail_call is calculated by "#define jmp_offset (out_offset - (cur_offset))" is a negative number, which is wrong. The final generated assembly are as follow. 54: bgeu $a2, $t1, -8 # 0x0000004c 58: addi.d $a6, $s5, -1 5c: bltz $a6, -16 # 0x0000004c 60: alsl.d $t2, $a2, $a1, 0x3 64: ld.d $t2, $t2, 264 68: beq $t2, $zero, -28 # 0x0000004c Before apply this patch, the follow test case will reveal soft lock issues. cd tools/testing/selftests/bpf/ ./test_progs --allow=tailcalls/tailcall_bpf2bpf_1 dmesg: watchdog: BUG: soft lockup - CPU#2 stuck for 26s! [test_progs:25056]	N/A	More Details
CVE-2025-38722	In the Linux kernel, the following vulnerability has been resolved: habanalabs: fix UAF in export_dmabuf() As soon as we'd inserted a file reference into descriptor table, another thread could close it. That's fine for the case when all we are doing is returning that descriptor to userland (it's a race, but it's a userland race and there's nothing the kernel can do about it). However, if we follow fd_install() with any kind of access to objects that would be destroyed on close (be it the struct file itself or anything destroyed by its ->release()), we have a UAF. dma_buf_fd() is a combination of reserving a descriptor and fd_install(). habanalabs export_dmabuf() calls it and then proceeds to access the objects destroyed on close. In particular, it grabs an extra reference to another struct file that will be dropped as part of ->release() for ours; that "will be" is actually "might have already been". Fix that by reserving descriptor before anything else and do fd_install() only when everything had been set up. As a side benefit, we no longer have the failure exit with file already created, but reference to underlying file (as well as ->dmabuf_export_cnt, etc.) not grabbed yet; unlike dma_buf_fd(), fd_install() can't fail.	N/A	More Details
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: netfilter: ctnetlink: fix refcount leak on table dump There is a reference count leak in ctnetlink_dump_table(): if (res < 0) { nf_conntrack_get(&ct->ct_general); // HERE cb->args[1] = (unsigned long)ct; ... While its very unlikely, its possible that ct == last. If this happens, then the refcount of ct was already incremented. This 2nd increment is never undone. This prevents the conntrack object from being released, which in turn keeps prevents cnet->count from dropping back to 0. This will then block the netns dismantle (or conntrack rmmod) as nf_conntrack_cleanup_net_list() will wait forever. This can be reproduced	N/A	More

38721	by running conntrack_resize.sh selftest in a loop. It takes ~20 minutes for me on a preemptible kernel on average before I see a runaway kworker spinning in nf_conntrack_cleanup_net_list. One fix would to change this to: if (res < 0) { if (ct != last) nf_conntrack_get(&ct->ct_general); But this reference counting isn't needed in the first place. We can just store a cookie value instead. A followup patch will do the same for ctnetlink_exp_dump_table, it looks to me as if this has the same problem and like ctnetlink_dump_table, we only need a 'skip hint', not the actual object so we can apply the same cookie strategy there as well.		Details
CVE-2025-38719	In the Linux kernel, the following vulnerability has been resolved: net: hibmcge: fix the division by zero issue When the network port is down, the queue is released, and ring->len is 0. In debugfs, hbg_get_queue_used_num() will be called, which may lead to a division by zero issue. This patch adds a check, if ring->len is 0, hbg_get_queue_used_num() directly returns 0.	N/A	More Details
CVE-2025-40642	Reflected Cross-Site Scripting (XSS) vulnerability in WebWork, which allows remote attackers to execute arbitrary code through the 'q' and 'engine' request parameters in /search.	N/A	More Details
CVE-2025-38718	In the Linux kernel, the following vulnerability has been resolved: sctp: linearize cloned gso packets in sctp_rcv A cloned head skb still shares these frag skbs in fraglist with the original head skb. It's not safe to access these frag skbs. syzbot reported two use-of-uninitialized-memory bugs caused by this: BUG: KMSAN: uninit-value in sctp_inq_pop+0x15b7/0x1920 net/sctp/inqueue.c:211 sctp_inq_pop+0x15b7/0x1920 net/sctp/inqueue.c:211 sctp_assoc_bh_rcv+0x1a7/0xc50 net/sctp/associola.c:998 sctp_inq_push+0x2ef/0x380 net/sctp/inqueue.c:88 sctp_backlog_rcv+0x397/0xdb0 net/sctp/input.c:331 sk_backlog_rcv+0x13b/0x420 include/net/sock.h:1122 __release_sock+0x1da/0x330 net/core/sock.c:3106 release_sock+0x6b/0x250 net/core/sock.c:3660 sctp_wait_for_connect+0x487/0x820 net/sctp/socket.c:9360 sctp_sendmsg_to_asoc+0x1ec1/0x1f00 net/sctp/socket.c:1885 sctp_sendmsg+0x32b9/0x4a80 net/sctp/socket.c:2031 inet_sendmsg+0x25a/0x280 net/ipv4/af_inet.c:851 sock_sendmsg_nosec net/socket.c:718 [inline] and BUG: KMSAN: uninit-value in sctp_assoc_bh_rcv+0x34e/0xbc0 net/sctp/associola.c:987 sctp_assoc_bh_rcv+0x34e/0xbc0 net/sctp/associola.c:987 sctp_inq_push+0x2a3/0x350 net/sctp/inqueue.c:88 sctp_backlog_rcv+0x3c7/0xda0 net/sctp/input.c:331 sk_backlog_rcv+0x142/0x420 include/net/sock.h:1148 __release_sock+0x1d3/0x330 net/core/sock.c:3213 release_sock+0x6b/0x270 net/core/sock.c:3767 sctp_wait_for_connect+0x458/0x820 net/sctp/socket.c:9367 sctp_sendmsg_to_asoc+0x223a/0x2260 net/sctp/socket.c:1886 sctp_sendmsg+0x3910/0x49f0 net/sctp/socket.c:2032 inet_sendmsg+0x269/0x2a0 net/ipv4/af_inet.c:851 sock_sendmsg_nosec net/socket.c:712 [inline] This patch fixes it by linearizing cloned gso packets in sctp_rcv().	N/A	More Details
CVE-2025-38717	In the Linux kernel, the following vulnerability has been resolved: net: kcm: Fix race condition in kcm_unattach() syzbot found a race condition when kcm_unattach(psock) and kcm_release(kcm) are executed at the same time. kcm_unattach() is missing a check of the flag kcm->tx_stopped before calling queue_work(). If the kcm has a reserved psock, kcm_unattach() might get executed between cancel_work_sync() and unreserve_psock() in kcm_release(), requeuing kcm->tx_work right before kcm gets freed in kcm_done(). Remove kcm->tx_stopped and replace it by the less error-prone disable_work_sync().	N/A	More Details
CVE-2025-5993	ITCube CRM in versions from 2023.2 through 2025.2 is vulnerable to path traversal. Unauthenticated remote attacker is able to exploit vulnerable parameter fileName and construct payloads that allow to download any file accessible by the the web server process.	N/A	More Details
CVE-2025-43777	Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.9, 2025.Q1.0 through 2025.Q1.16, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.19 exposes "Internal Server Error" in the response body when a login attempt is made with a deleted Client Secret.	N/A	More Details
CVE-2025-38716	In the Linux kernel, the following vulnerability has been resolved: hfs: fix general protection fault in hfs_find_init() The hfs_find_init() method can trigger the crash if tree pointer is NULL: [45.746290][T9787] Oops: general protection fault, probably for non-canonical address 0xdfffffc0000000008: 0000 [#1] SMP KAI [45.747287][T9787] KASAN: null-ptr-deref in range [0x0000000000000040-0x0000000000000047] [45.748716][T9787] CPU: 2 UID: 0 PID: 9787 Comm: repro Not tainted 6.16.0-rc3 #10 PREEMPT(full) [45.750250][T9787] Hardware name: QEMU Ubuntu 24.04 PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [45.751983][T9787] RIP: 0010:hfs_find_init+0x86/0x230 [45.752834][T9787] Code: c1 ea 03 80 3c 02 00 0f 85 9a 01 00 00 4c 8d 6b 40 48 c7 45 18 00 00 00 00 48 b8 00 00 00 00 00 fc [45.755574][T9787] RSP: 0018:ffffc90015157668 EFLAGS: 00010202 [45.756432][T9787] RAX: dfffffc0000000000 RBX: 0000000000000000 RCX: ffffffff819a4d09 [45.757457][T9787] RDX: 0000000000000008 RSI: ffffffff819acd3a RDI: ffffc900151576e8 [45.758282][T9787] RBP: ffffc900151576d0 R08: 0000000000000005 R09: 0000000000000000 [45.758943][T9787] R10: 0000000080000000 R11: 0000000000000001 R12: 0000000000000004 [45.759619][T9787] R13: 0000000000000040 R14: ffff88802c50814a R15: 0000000000000000 [45.760293][T9787] FS: 00007ffb72734540(0000) GS:ffff8880cec64000(0000) knlGS:0000000000000000 [45.761050][T9787] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [45.761606][T9787] CR2: 00007f9bd8225000 CR3: 000000010979a000 CR4: 00000000000006f0 [45.762286][T9787] Call Trace: [45.762570][T9787] <TASK> [45.762824][T9787] hfs_ext_read_extent+0x190/0x9d0 [45.763269][T9787] ? submit_bio_noacct_nocheck+0x2dd/0xce0 [45.763766][T9787] ? __pfx_hfs_ext_read_extent+0x10/0x10 [45.764250][T9787] hfs_get_block+0x55f/0x830 [45.764646][T9787] block_read_full_folio+0x36d/0x850 [45.765105][T9787] ? __pfx_hfs_get_block+0x10/0x10 [45.765541][T9787] ? const_folio_flags+0x5b/0x100 [45.765972][T9787] ? __pfx_hfs_read_folio+0x10/0x10 [45.766415][T9787] filemap_read_folio+0xbe/0x290 [45.766840][T9787] ? __pfx_filemap_read_folio+0x10/0x10 [45.767325][T9787] ? __filemap_get_folio+0x32b/0xbf0 [45.767780][T9787] do_read_cache_folio+0x263/0x5c0 [45.768223][T9787] ? __pfx_hfs_read_folio+0x10/0x10 [45.768666][T9787] read_cache_page+0x5b/0x160 [45.769070][T9787] hfs_btree_open+0x491/0x1740 [45.769481][T9787] hfs_mdb_get+0x15e2/0x1fb0 [45.769877][T9787] ? __pfx_hfs_mdb_get+0x10/0x10 [45.770316][T9787] ? find_held_lock+0x2b/0x80 [45.770731][T9787] ?	N/A	More Details

	lockdep_init_map_type+0x5c/0x280 [45.771200][T9787] ? lockdep_init_map_type+0x5c/0x280 [45.771674][T9787] hfs_fill_super+0x38e/0x720 [45.772092][T9787] ? __pfx_hfs_fill_super+0x10/0x10 [45.772549][T9787] ? snprintf+0xbe/0x100 [45.772931][T9787] ? __pfx_snprintf+0x10/0x10 [45.773350][T9787] ? do_raw_spin_lock+0x129/0x2b0 [45.773796][T9787] ? find_held_lock+0x2b/0x80 [45.774215][T9787] ? set_blocksize+0x40a/0x510 [45.774636][T9787] ? sb_set_blocksize+0x176/0x1d0 [45.775087][T9787] ? setup_bdev_super+0x369/0x730 [45.775533][T9787] get_tree_bdev_flags+0x384/0x620 [45.775985][T9787] ? __pfx_hfs_fill_super+0x10/0x10 [45.776453][T9787] ? __pfx_get_tree_bdev_flags+0x10/0x10 [45.776950][T9787] ? bpf_lsm_capable+0x9/0x10 [45.777365][T9787] ? security_capable+0x80/0x260 [45.777803][T9787] vfs_get_tree+0x8e/0x340 [45.778203][T9787] path_mount+0x13de/0x2010 [45.778604][T9787] ? kmem_cache_free+0x2b0/0x4c0 [45.779052][T9787] ? __pfx_path_mount+0x10/0x10 [45.779480][T9787] ? getname_flags.part.0+0x1c5/0x550 [45.779954][T9787] ? putname+0x154/0x1a0 [45.780335][T9787] __x64_sys_mount+0x27b/0x300 [45.780758][T9787] ? __pfx___x64_sys_mount+0x10/0x10 [45.781232][T9787] ---truncated---		
CVE-2025-40641	Cross-site Scripting (XSS) vulnerability stored in Multi-Purpose Inventory Management System, consisting of a stored XSS due to lack of proper validation of user input by sending a POST request using the product_name parameter in /Controller_Products/update. This vulnerability could allow a remote user to send a specially crafted query to an authenticated user and steal their cookie session details.	N/A	More Details
CVE-2025-43778	A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.11, 2025.Q1.0 through 2025.Q1.16, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.20 allows an remote authenticated attacker to inject JavaScript through the name of a fieldset in Kaleo Forms Admin. The malicious payload is stored and executed without proper sanitization or escaping.	N/A	More Details
CVE-2025-38684	In the Linux kernel, the following vulnerability has been resolved: net/sched: ets: use old 'nbands' while purging unused classes Shuang reported sch_ets test-case [1] crashing in ets_class_qlen_notify() after recent changes from Lion [2]. The problem is: in ets_qdisc_change() we purge unused DWRR queues; the value of 'q->nbands' is the new one, and the cleanup should be done with the old one. The problem is here since my first attempts to fix ets_qdisc_change(), but it surfaced again after the recent qdisc len accounting fixes. Fix it purging idle DWRR queues before assigning a new value of 'q->nbands', so that all purge operations find a consistent configuration: - old 'q->nbands' because it's needed by ets_class_find() - old 'q->nstrict' because it's needed by ets_class_is_strict() BUG: kernel NULL pointer dereference, address: 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: 62 UID: 0 PID: 39457 Comm: tc Kdump: loaded Not tainted 6.12.0-116.el10.x86_64 #1 PREEMPT(voluntary) Hardware name: Dell Inc. PowerEdge R640/06DKY5, BIOS 2.12.2 07/09/2021 RIP: 0010:__list_del_entry_valid_or_report+0x4/0x80 Code: ff 4c 39 c7 0f 84 39 19 8e ff b8 01 00 00 00 c3 cc cc cc cc 66 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa <48> 8b 17 48 8b 4f 08 48 85 d2 0f 84 56 19 8e ff 48 85 c9 0f 84 ab RSP: 0018:ffffba186009f400 EFLAGS: 00010202 RAX: 00000000000000d6 RBX: 0000000000000000 RCX: 0000000000000004 RDX: ffff9f0fa29b69c0 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffffffc12c2400 R08: 0000000000000008 R09: 0000000000000004 R10: ffffffffffffffff R11: 0000000000000004 R12: 0000000000000000 R13: ffff9f0f8cfe0000 R14: 0000000000100005 R15: 0000000000000000 FS: 00007f2154f37480(0000) GS:ffff9f269c1c0000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 00000001530be001 CR4: 00000000007726f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ets_class_qlen_notify+0x65/0x90 [sch_ets] qdisc_tree_reduce_backlog+0x74/0x110 ets_qdisc_change+0x630/0xa40 [sch_ets] __tc_modify_qdisc.constprop.0+0x216/0x7f0 tc_modify_qdisc+0x7c/0x120 rtnetlink_rcv_msg+0x145/0x3f0 netlink_rcv_skb+0x53/0x100 netlink_unicast+0x245/0x390 netlink_sendmsg+0x21b/0x470 ____sys_sendmsg+0x39d/0x3d0 ___sys_sendmsg+0x9a/0xe0 __sys_sendmsg+0x7a/0xd0 do_syscall_64+0x7d/0x160 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7f2155114084 Code: 89 02 b8 ff ff ff ff eb bb 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 f3 0f 1e fa 80 3d 25 f0 0c 00 00 74 13 b8 2e 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 54 c3 0f 1f 00 48 83 ec 28 89 54 24 1c 48 89 RSP: 002b:00007fff1fd7a988 EFLAGS: 00000202 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 0000560ec063e5e0 RCX: 00007f2155114084 RDX: 0000000000000000 RSI: 00007fff1fd7a9f0 RDI: 0000000000000003 RBP: 00007fff1fd7aa60 R08: 0000000000000010 R09: 000000000000003f R10: 0000560ee9b3a010 R11: 0000000000000202 R12: 00007fff1fd7aae0 R13: 000000006891ccde R14: 0000560ec063e5e0 R15: 00007fff1fd7aad0 </TASK> [1] https://lore.kernel.org/netdev/e08c7f4a6882f260011909a868311c6e9b54f3e4.1639153474.git.dcaratti@redhat.com/ [2] https://lore.kernel.org/netdev/d912cbd7-193b-4269-9857-525bee8bbb6a@gmail.com/	N/A	More Details
CVE-2025-38685	In the Linux kernel, the following vulnerability has been resolved: fbdev: Fix vmalloc out-of-bounds write in fast_imageblit This issue triggers when a userspace program does an ioctl FBIOPUT_CON2FBMAP by passing console number and frame buffer number. Ideally this maps console to frame buffer and updates the screen if console is visible. As part of mapping it has to do resize of console according to frame buffer info. if this resize fails and returns from vc_do_resize() and continues further. At this point console and new frame buffer are mapped and sets display vars. Despite failure still it continue to proceed updating the screen at later stages where vc_data is related to previous frame buffer and frame buffer info and display vars are mapped to new frame buffer and eventully leading to out-of-bounds write in fast_imageblit(). This bheviour is excepted only when fg_console is equal to requested console which is a visible console and updates screen with invalid struct references in fbcon_putcs().	N/A	More Details
CVE-2025-38686	In the Linux kernel, the following vulnerability has been resolved: userfaultfd: fix a crash in UFFDIO_MOVE when PMD is a migration entry When UFFDIO_MOVE encounters a migration PMD entry, it proceeds with obtaining a folio and accessing it even though the entry is swp_entry_t. Add the missing check and let split_huge_pmd() handle migration	N/A	More Details

	entries. While at it also remove unnecessary folio check. [surenb@google.com: remove extra folio check, per David]		
CVE-2025-38697	In the Linux kernel, the following vulnerability has been resolved: jfs: upper bound check of tree index in dbAllocAG When computing the tree index in dbAllocAG, we never check if we are out of bounds realative to the size of the stree. This could happen in a scenario where the filesystem metadata are corrupted.	N/A	More Details
CVE-2025-57766	Fides is an open-source privacy engineering platform. Prior to version 2.69.1, admin UI user password changes in Fides do not invalidate active user sessions, creating a vulnerability chaining opportunity where attackers who have obtained session tokens through other attack vectors (such as XSS) can maintain access even after password reset. This issue is not directly exploitable on its own and requires a prerequisite vulnerability to obtain valid session tokens in the first place. Version 2.69.1 fixes the issue. No known workarounds are available.	N/A	More Details
CVE-2025-38693	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: w7090p: fix null-ptr-deref in w7090p_tuner_write_serpar and w7090p_tuner_read_serpar In w7090p_tuner_write_serpar, msg is controlled by user. When msg[0].buf is null and msg[0].len is zero, former checks on msg[0].buf would be passed. If accessing msg[0].buf[2] without sanity check, null pointer deref would happen. We add check on msg[0].len to prevent crash. Similar commit: commit 0ed554fd769a ("media: dvb-usb: az6027: fix null-ptr-deref in az6027_i2c_xfer()")	N/A	More Details
CVE-2025-38694	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: dib7090p: fix null-ptr-deref in dib7090p_rw_on_apb() In dib7090p_rw_on_apb, msg is controlled by user. When msg[0].buf is null and msg[0].len is zero, former checks on msg[0].buf would be passed. If accessing msg[0].buf[2] without sanity check, null pointer deref would happen. We add check on msg[0].len to prevent crash. Similar issue occurs when access msg[1].buf[0] and msg[1].buf[1]. Similar commit: commit 0ed554fd769a ("media: dvb-usb: az6027: fix null-ptr-deref in az6027_i2c_xfer()")	N/A	More Details
CVE-2025-38695	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Check for hdwq null ptr when cleaning up lpfc_vport structure If a call to lpfc_sli4_read_rev() from lpfc_sli4_hba_setup() fails, the resultant cleanup routine lpfc_sli4_vport_delete_fcp_xri_aborted() may occur before sli4_hba.hdwqs are allocated. This may result in a null pointer dereference when attempting to take the abts_io_buf_list_lock for the first hardware queue. Fix by adding a null ptr check on phba->sli4_hba.hdwq and early return because this situation means there must have been an error during port initialization.	N/A	More Details
CVE-2025-38696	In the Linux kernel, the following vulnerability has been resolved: MIPS: Don't crash in stack_top() for tasks without ABI or vDSO Not all tasks have an ABI associated or vDSO mapped, for example kthreads never do. If such a task ever ends up calling stack_top(), it will derefence the NULL ABI pointer and crash. This can for example happen when using kunit: mips_stack_top+0x28/0xc0 arch_pick_mmap_layout+0x190/0x220 kunit_vm_mmap_init+0xf8/0x138 __kunit_add_resource+0x40/0xa8 kunit_vm_mmap+0x88/0xd8 usercopy_test_init+0xb8/0x240 kunit_try_run_case+0x5c/0x1a8 kunit_generic_run_threadfn_adapter+0x28/0x50 kthread+0x118/0x240 ret_from_kernel_thread+0x14/0x1c Only dereference the ABI point if it is set. The GIC page is also included as it is specific to the vDSO. Also move the randomization adjustment into the same conditional.	N/A	More Details
CVE-2025-54994	@akoskm/create-mcp-server-stdio is an MCP server starter kit that uses the StdioServerTransport. Prior to version 0.0.13, the MCP Server is written in a way that is vulnerable to command injection vulnerability attacks as part of some of its MCP Server tool definition and implementation. The MCP Server exposes the tool `which-app-on-port` which relies on Node.js child process API `exec` which is an unsafe and vulnerable API if concatenated with untrusted user input. Version 0.0.13 contains a fix for the issue.	N/A	More Details
CVE-2025-53838	LinkAce is a self-hosted archive to collect website links. A stored cross-site scripting (XSS) vulnerability was discovered in versions prior to 2.1.9 that allows an attacker to inject arbitrary JavaScript, which is then executed in the context of a user's browser when the malicious link is clicked. This is a one-click XSS, meaning the victim only needs to click a crafted link — no further interaction is required. The application contains a stored XSS vulnerability due to insufficient filtering and escaping of user-supplied data inserted into link attributes. Malicious JavaScript code can be saved in the database along with the link and executed in the user's browser when clicking the link, leading to arbitrary script execution within the context of the site. Version 2.1.9 fixes the issue.	N/A	More Details
CVE-2025-38698	In the Linux kernel, the following vulnerability has been resolved: jfs: Regular file corruption check The reproducer builds a corrupted file on disk with a negative i_size value. Add a check when opening this file to avoid subsequent operation failures.	N/A	More Details
CVE-2025-43763	A server-side request forgery (SSRF) vulnerability exist in the Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.20 that affects custom object attachment fields. This flaw allows an attacker to manipulate the application into making unauthorized requests to other instances, creating new object entries that link to external resources.	N/A	More Details
CVE-2025-38699	In the Linux kernel, the following vulnerability has been resolved: scsi: bfa: Double-free fix When the bfad_im_probe() function fails during initialization, the memory pointed to by bfad->im is freed without setting bfad->im to NULL. Subsequently, during driver uninstallation, when the state machine enters the bfad_sm_stopping state and calls the bfad_im_probe_undo() function, it attempts to free the memory pointed to by bfad->im again, thereby triggering a double-free vulnerability. Set bfad->im to NULL if probing fails.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: scsi: libiscsi: Initialize iscsi_conn->dd_data only if memory is allocated In case of an ib_fast_reg_mr allocation failure during iSER setup, the machine hits a panic because iscsi_conn->dd_data is initialized unconditionally, even when no memory is allocated (dd_size == 0). This leads invalid pointer dereference during connection teardown. Fix by setting iscsi_conn->dd_data only if memory is actually allocated. Panic trace: ---------- iser: iser_create_fastreg_desc: Failed to allocate ib_fast_reg_mr err=-12 iser:		More

2025-38700	iser_alloc_rx_descriptors: failed allocating rx descriptors / data buffers BUG: unable to handle page fault for address: ffffffffffffffff8 RIP: 0010:swake_up_locked.part.5+0xa/0x40 Call Trace: complete+0x31/0x40 iscsi_iser_conn_stop+0x88/0xb0 [ib_iser] iscsi_stop_conn+0x66/0xc0 [scsi_transport_iscsi] iscsi_if_stop_conn+0x14a/0x150 [scsi_transport_iscsi] iscsi_if_rx+0x1135/0x1834 [scsi_transport_iscsi] ? netlink_lookup+0x12f/0x1b0 ? netlink_deliver_tap+0x2c/0x200 netlink_unicast+0x1ab/0x280 netlink_sendmsg+0x257/0x4f0 ? _copy_from_user+0x29/0x60 sock_sendmsg+0x5f/0x70	N/A	Details
CVE-2025-38701	In the Linux kernel, the following vulnerability has been resolved: ext4: do not BUG when INLINE_DATA_FL lacks system.data xattr A syzbot fuzzed image triggered a BUG_ON in ext4_update_inline_data() when an inode had the INLINE_DATA_FL flag set but was missing the system.data extended attribute. Since this can happen due to a maiciouly fuzzed file system, we shouldn't BUG, but rather, report it as a corrupted file system. Add similar replacements of BUG_ON with EXT4_ERROR_INODE() ii ext4_create_inline_data() and ext4_inline_data_truncate().	N/A	More Details
CVE-2025-38702	In the Linux kernel, the following vulnerability has been resolved: fbdev: fix potential buffer overflow in do_register_framebuffer() The current implementation may lead to buffer overflow when: 1. Unregistration creates NULL gaps in registered_fb[] 2. All array slots become occupied despite num_registered_fb < FB_MAX 3. The registration loop exceeds array bounds Add boundary check to prevent registered_fb[FB_MAX] access.	N/A	More Details
CVE-2025-38703	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Make dma-fences compliant with the safe access rules Xe can free some of the data pointed to by the dma-fences it exports. Most notably the timeline name can get freed if userspace closes the associated submit queue. At the same time the fence could have been exported to a third party (for example a sync_fence fd) which will then cause an use- after-free on subsequent access. To make this safe we need to make the driver compliant with the newly documented dma-fence rules. Driver has to ensure a RCU grace period between signalling a fence and freeing any data pointed to by said fence. For the timeline name we simply make the queue be freed via kfree_rcu and for the shared lock associated with multiple queues we add a RCU grace period before freeing the per GT structure holding the lock.	N/A	More Details
CVE-2025-38704	In the Linux kernel, the following vulnerability has been resolved: rcu/nocb: Fix possible invalid rdp's->nocb_cb_kthread pointer access In the preparation stage of CPU online, if the corresponding the rdp's->nocb_cb_kthread does not exist, will be created, there is a situation where the rdp's rcuop kthreads creation fails, and then de-offload this CPU's rdp, does not assign this CPU's rdp->nocb_cb_kthread pointer, but this rdp's->nocb_gp_rdp and rdp's->rdp_gp->nocb_gp_kthread is still valid. This will cause the subsequent re-offload operation of this offline CPU, which will pass the conditional check and the kthread_unpark() will access invalid rdp's->nocb_cb_kthread pointer. This commit therefore use rdp's->nocb_gp_kthread instead of rdp_gp's->nocb_gp_kthread for safety check.	N/A	More Details
CVE-2025-38705	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: fix null pointer access Writing a string without delimiters (' ', '\n', '\0') to the under gpu_od/fan_ctrl sysfs or pp_power_profile_mode for the CUSTOM profile will result in a null pointer dereference.	N/A	More Details
CVE-2025-57815	Fides is an open-source privacy engineering platform. Prior to version 2.69.1, the Fides Admin UI login endpoint relies on a general IP-based rate limit for all API traffic and lacks specific anti-automation controls designed to protect against brute-force attacks. This could allow attackers to conduct credential testing attacks, such as credential stuffing or password spraying, which poses a risk to accounts with weak or previously compromised passwords. Version 2.69.1 fixes the issue. For organizations with commercial Fides Enterprise licenses, configuring Single Sign-On (SSO) through an OIDC provider (like Azure, Google, or Okta) is an effective workaround. When OIDC SSO is enabled, username/password authentication can be disabled entirely, which eliminates this attack vector. This functionality is not available for Fides Open Source users.	N/A	More Details
CVE-2025-57816	Fides is an open-source privacy engineering platform. Prior to version 2.69.1, the Fides Webserver API's built-in IP-based rate limiting is ineffective in environments with CDNs, proxies or load balancers. The system incorrectly applies rate limits based on directly connected infrastructure IPs rather than client IPs, and stores counters in-memory rather than in a shared store. This allows attackers to bypass intended rate limits and potentially cause denial of service. This vulnerability only affects deployments relying on Fides's built-in rate limiting for protection. Deployments using external rate limiting solutions (WAFs, API gateways, etc.) are not affected. Version 2.69.1 fixes the issue. There are no application-level workarounds. However, rate limiting may instead be implemented externally at the infrastructure level using a WAF, API Gateway, or similar technology.	N/A	More Details
CVE-2025-57817	Fides is an open-source privacy engineering platform. Prior to version 2.69.1, the OAuth client creation and update endpoints of the Fides Webserver API do not properly authorize scope assignment. This allows highly privileged users with `client:create` or `client:update` permissions to escalate their privileges to owner-level. Version 2.69.1 fixes the issue. No known workarounds are available.	N/A	More Details
CVE-2025-58365	The XWiki blog application allows users of the XWiki platform to create and manage blog posts. Prior to version 9.14, the blog application in XWiki allowed remote code execution for any user who has edit right on any page. Normally, these are all logged-in users as they can edit their own user profile. For an exploit, it is sufficient to add an object of type `Blog.BlogPostClass` to any page and to add some script macro with the exploit code to the "Content" field of that object. The vulnerability has been patched in the blog application version 9.14 by executing the content of blog posts with the rights of the appropriate author. No known workarounds are available.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: comedi: fix race between polling and detaching syzbot reports a use-after-free in comedi in the below link, which is due to comedi gladly removing the allocated async area even though poll requests are still active on the wait_queue_head inside of it. This can cause a use-after-free when the poll entries are later triggered or removed, as the memory for the wait_queue_head has been freed. We need to check there are no tasks queued on any of the subdevices' wait queues before allowing the device to be		

CVE-2025-38687	detached by the `COMEDI_DEVCONFIG` ioctl. Tasks will read-lock `dev->attach_lock` before adding themselves to the subdevice wait queue, so fix the problem in the `COMEDI_DEVCONFIG` ioctl handler by write-locking `dev->attach_lock` before checking that all of the subdevices are safe to be deleted. This includes testing for any sleepers on the subdevices' wait queues. It remains locked until the device has been detached. This requires the `comedi_device_detach()` function to be refactored slightly, moving the bulk of it into new function `comedi_device_detach_locked()`. Note that the refactor of `comedi_device_detach()` results in `comedi_device_cancel_all()` now being called while `dev->attach_lock` is write-locked, which wasn't the case previously, but that does not matter. Thanks to Jens Axboe for diagnosing the problem and co-developing this patch.	N/A	More Details
CVE-2025-38688	In the Linux kernel, the following vulnerability has been resolved: iommufd: Prevent ALIGN() overflow When allocating IOVA the candidate range gets aligned to the target alignment. If the range is close to ULONG_MAX then the ALIGN() can wrap resulting in a corrupted iova. Open code the ALIGN() using get_add_overflow() to prevent this. This simplifies the checks as we don't need to check for length earlier either. Consolidate the two copies of this code under a single helper. This bug would allow userspace to create a mapping that overlaps with some other mapping or a reserved range.	N/A	More Details
CVE-2025-58752	Vite is a frontend tooling framework for JavaScript. Prior to versions 7.1.5, 7.0.7, 6.3.6, and 5.4.20, any HTML files on the machine were served regardless of the `server.fs` settings. Only apps that explicitly expose the Vite dev server to the network (using --host or server.host config option) and use `appType: 'spa'` (default) or `appType: 'mpa'` are affected. This vulnerability also affects the preview server. The preview server allowed HTML files not under the output directory to be served. Versions 7.1.5, 7.0.7, 6.3.6, and 5.4.20 fix the issue.	N/A	More Details
CVE-2025-58751	Vite is a frontend tooling framework for JavaScript. Prior to versions 7.1.5, 7.0.7, 6.3.6, and 5.4.20, files starting with the same name with the public directory were served bypassing the `server.fs` settings. Only apps that explicitly expose the Vite dev server to the network (using --host or `server.host` config option), use the public directory feature (enabled by default), and have a symlink in the public directory are affected. Versions 7.1.5, 7.0.7, 6.3.6, and 5.4.20 fix the issue.	N/A	More Details
CVE-2025-58454	WeGIA is a Web manager for charitable institutions. A SQL Injection vulnerability was identified in WeGIA versions 3.4.10 and prior inthe endpoint /WeGIA/html/memorando/listar_despachos.php, in the id_memorando parameter. This vulnerability allow an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. Version 3.4.11 contains a patch.	N/A	More Details
CVE-2025-58453	WeGIA is a Web manager for charitable institutions. A SQL Injection vulnerability was identified in WeGIA versions 3.4.10 and prior in the endpoint /WeGIA/html/memorando/exibe_anexo.php, in the id_anexo parameter. This vulnerability allow an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. Version 3.4.11 contains a patch.	N/A	More Details
CVE-2025-58452	WeGIA is a Web manager for charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the listar_despachos.php endpoint of the WeGIA application prior to version 3.4.11. This vulnerability allows attackers to inject malicious scripts in the id_memorando parameter. Version 3.4.11 contains a patch.	N/A	More Details
CVE-2025-38689	In the Linux kernel, the following vulnerability has been resolved: x86/fpu: Fix NULL dereference in avx512_status() Problem ------- With CONFIG_X86_DEBUG_FPU enabled, reading /proc/[kthread]/arch_status causes a warning and a NULL pointer dereference. This is because the AVX-512 timestamp code uses x86_task_fpu() but doesn't check it for NULL. CONFIG_X86_DEBUG_FPU addles that function for kernel threads (PF_KTHREAD specifically), making it return NULL. The point of the warning was to ensure that kernel threads only access task->fpu after going through kernel_fpu_begin()/_end(). Note: all kernel tasks exposed in /proc have a valid task->fpu. Solution -------- One option is to silence the warning and check for NULL from x86_task_fpu(). However, that warning is fairly fresh and seems like a defense against misuse of the FPU state in kernel threads. Instead, stop outputting AVX-512_elapsed_ms for kernel threads altogether. The data was garbage anyway because avx512_timestamp is only updated for user threads, not kernel threads. If anyone ever wants to track kernel thread AVX-512 use, they can come back later and do it properly, separate from this bug fix. [dhansen: mostly rewrite changelog]	N/A	More Details
CVE-2025-38690	In the Linux kernel, the following vulnerability has been resolved: drm/xe/migrate: prevent infinite recursion If the buf + offset is not aligned to XE_CAHELINE_BYTES we fallback to using a bounce buffer. However the bounce buffer here is allocated on the stack, and the only alignment requirement here is that it's naturally aligned to u8, and not XE_CACHELINE_BYTES. If the bounce buffer is also misaligned we then recurse back into the function again, however the new bounce buffer might also not be aligned, and might never be until we eventually blow through the stack, as we keep recursing. Instead of using the stack use kmalloc, which should respect the power-of-two alignment request here. Fixes a kernel panic when triggering this path through eudebug. v2 (Stuart): - Add build bug check for power-of-two restriction - s/EINVAL/ENOMEM/ (cherry picked from commit 38b34e928a08ba594c4bbf7118aa3aadacd62fff)	N/A	More Details
CVE-2025-38691	In the Linux kernel, the following vulnerability has been resolved: pNFS: Fix uninited ptr deref in block/scsi layout The error occurs on the third attempt to encode extents. When function ext_tree_prepare_commit() reallocates a larger buffer to retry encoding extents, the "layoutupdate_pages" page array is initialized only after the retry loop. But ext_tree_free_commitdata() is called on every iteration and tries to put pages in the array, thus dereferencing uninitialized pointers. An additional problem is that there is no limit on the maximum possible buffer_size. When there are too many extents, the client may create a layoutcommit that is larger than the maximum possible RPC size accepted by the server. During testing, we observed two typical scenarios. First, one memory page for extents is enough when we work with small files, append data to the end of the file, or preallocate extents before writing. But when we fill a new large file without preallocating, the number of extents can be huge, and counting the number of written extents in ext_tree_encode_commit() does not help much. Since this number increases even more between unlocking and locking of ext_tree, the reallocated buffer may not be large enough again and again.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: exfat: add cluster chain loop check for dir An		

CVE-2025-38692	infinite loop may occur if the following conditions occur due to file system corruption. (1) Condition for exfat_count_dir_entries() to loop infinitely. - The cluster chain includes a loop. - There is no UNUSED entry in the cluster chain. (2) Condition for exfat_create_upcase_table() to loop infinitely. - The cluster chain of the root directory includes a loop. - There are no UNUSED entry and up-case table entry in the cluster chain of the root directory. (3) Condition for exfat_load_bitmap() to loop infinitely. - The cluster chain of the root directory includes a loop. - There are no UNUSED entry and bitmap entry in the cluster chain of the root directory. (4) Condition for exfat_find_dir_entry() to loop infinitely. - The cluster chain includes a loop. - The unused directory entries were exhausted by some operation. (5) Condition for exfat_check_dir_empty() to loop infinitely. - The cluster chain includes a loop. - The unused directory entries were exhausted by some operation. - All files and sub-directories under the directory are deleted. This commit adds checks to break the above infinite loop.	N/A	More Details
CVE-2025-58451	Cattown is a JavaScript markdown parser. Versions prior to 1.0.2 used regular expressions with inefficient, potentially exponential worst-case complexity. This could cause excessive CPU usage due to excessive backtracking on crafted inputs. In turn, the excessive CPU usage could lead to resource exhaustion, where processing malicious inputs could cause high CPU or memory usage, potentially leading to denial of service. Version 1.0.2 contains a patch. Additionally, users should review and restrict input sources if untrusted inputs are processed.	N/A	More Details
CVE-2025-58450	pREST (PostgreSQL REST), is an API that delivers an application on top of a Postgres database. SQL injection is possible in versions prior to 2.0.0-rc3. The validation present in versions prior to 2.0.0-rc3 does not provide adequate protection from injection attempts. Version 2.0.0-rc3 contains a patch to mitigate such attempts.	N/A	More Details
CVE-2025-58449	Maho is a free and open source ecommerce platform. In Maho prior to 25.9.0, an authenticated staff user with access to the `Dashboard` and `Catalog\Manage Products` permissions can create a custom option on a listing with a file input field. By allowing file uploads with a `.php` extension, the user can use the filed to upload malicious PHP files, gaining remote code execution. Version 25.9.0 fixes the issue.	N/A	More Details
CVE-2025-58444	The MCP inspector is a developer tool for testing and debugging MCP servers. A cross-site scripting issue was reported in versions of the MCP Inspector local development tool prior to 0.16.6 when connecting to untrusted remote MCP servers with a malicious redirect URI. This could be leveraged to interact directly with the inspector proxy to trigger arbitrary command execution. Users are advised to update to 0.16.6 to resolve this issue.	N/A	More Details
CVE-2025-59013	An open-redirect vulnerability in GeneralUtility::sanitizeLocalUrl of TYPO3 CMS 9.0.0–9.5.54, 10.0.0–10.4.53, 11.0.0–11.5.47, 12.0.0–12.4.36, and 13.0.0–13.4.17 allows an attacker to redirect users to arbitrary external sites, enabling phishing attacks by supplying a manipulated, sanitized URL.	N/A	More Details
CVE-2025-59014	An uncaught exception in the Bookmark Toolbar of TYPO3 CMS versions 11.0.0–11.5.47, 12.0.0–12.4.36, and 13.0.0–13.4.17 lets administrator-level backend users trigger a denial-of-service condition in the backend user interface by saving manipulated data in the bookmark toolbar.	N/A	More Details
CVE-2025-59015	A deterministic three-character prefix in the Password Generation component of TYPO3 CMS versions 12.0.0–12.4.36 and 13.0.0–13.4.17 reduces entropy, allowing attackers to carry out brute-force attacks more quickly.	N/A	More Details
CVE-2025-58695	Rejected reason: Not used	N/A	More Details
CVE-2025-58912	Rejected reason: Not used	N/A	More Details
CVE-2025-55747	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In versions 6.1-milestone-2 through 16.10.6, configuration files are accessible through the webjars API. This is fixed in version 16.10.7.	N/A	More Details
CVE-2025-55748	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In versions 4.2-milestone-2 through 16.10.6, configuration files are accessible through jsx and sx endpoints. It's possible to access and read configuration files by using URLs such as `http://localhost:8080/bin/ssx/Main/WebHome?resource=../../WEB-INF/xwiki.cfg&minify=false`. This is fixed in version 16.10.7.	N/A	More Details
CVE-2025-43772	Kaleo Forms Admin in Liferay Portal 7.0.0 through 7.4.3.4, and Liferay DXP 7.4 GA, 7.3 GA through update 27, and older unsupported versions does not restrict the saving of request parameters in the portlet session, which allows remote attackers to consume system memory leading to denial-of-service (DoS) conditions via crafted HTTP request.	N/A	More Details
CVE-2025-58064	CKEditor 5 is a modern JavaScript rich-text editor with an MVC architecture. ckeditor5 and ckeditor5-clipboard versions 46.0.0 through 46.0.2 and 44.2.0 through 45.2.1 contain a Cross-Site Scripting (XSS) vulnerability. Ability to exploit could be triggered by a specific user action (leading to unauthorized JavaScript code execution) if the attacker managed to insert a malicious content into the editor, which might happen with a very specific editor configuration. This vulnerability affects installations where the editor configuration meets one of the following criteria: the HTML embed plugin is enabled, or there is a custom plugin introducing an editable element where view RawElement is enabled. This issue is fixed in versions 45.2.2 and 46.0.3 of both ckeditor5 and ckeditor5-clipboard.	N/A	More Details
CVE-2025-58171	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details

CVE-2025-58694	Rejected reason: Not used	N/A	More Details
CVE-2025-58696	Rejected reason: Not used	N/A	More Details
CVE-2025-58438	internetarchive is a Python and Command-Line Interface to Archive.org In versions 5.5.0 and below, there is a directory traversal (path traversal) vulnerability in the File.download() method of the internetarchive library. The file.download() method does not properly sanitize user-supplied filenames or validate the final download path. A maliciously crafted filename could contain path traversal sequences (e.g., ../../../../windows/system32/file.txt) or illegal characters that, when processed, would cause the file to be written outside of the intended target directory. An attacker could potentially overwrite critical system files or application configuration files, leading to a denial of service, privilege escalation, or remote code execution, depending on the context in which the library is used. The vulnerability is particularly critical for users on Windows systems, but all operating systems are affected. This issue is fixed in version 5.5.1.	N/A	More Details
CVE-2025-58697	Rejected reason: Not used	N/A	More Details
CVE-2025-9961	An authenticated attacker may remotely execute arbitrary code via the CWMP binary on the devices AX10 and AX1500. The exploit can only be conducted via a Man-In-The-Middle (MITM) attack. This issue affects AX10 V1/V1.2/V2/V2.6/V3/V3.6: before 1.2.1; AX1500 V1/V1.20/V1.26/V1.60/V1.80/V2.60/V3.6: before 1.3.11.	N/A	More Details
CVE-2025-58698	Rejected reason: Not used	N/A	More Details
CVE-2025-58699	Rejected reason: Not used	N/A	More Details
CVE-2025-58700	Rejected reason: Not used	N/A	More Details
CVE-2025-58701	Rejected reason: Not used	N/A	More Details
CVE-2025-6984	The langchain-ai/langchain project, specifically the EverNoteLoader component, is vulnerable to XML External Entity (XXE) attacks due to insecure XML parsing. The affected version is 0.3.63. The vulnerability arises from the use of etree.iterparse() without disabling external entity references, which can lead to sensitive information disclosure. An attacker could exploit this by crafting a malicious XML payload that references local files, potentially exposing sensitive data such as /etc/passwd.	N/A	More Details
CVE-2025-58911	Rejected reason: Not used	N/A	More Details
CVE-2025-58910	Rejected reason: Not used	N/A	More Details
CVE-2025-58909	Rejected reason: Not used	N/A	More Details
CVE-2025-58908	Rejected reason: Not used	N/A	More Details
CVE-2025-9823	SummaryA Cross-Site Scripting (XSS) vulnerability allows an attacker to execute arbitrary JavaScript in the context of another user’s session. This occurs because user-supplied input is reflected back in the server’s response without proper sanitization or escaping, potentially enabling malicious actions such as session hijacking, credential theft, or unauthorized actions in the application. DetailsThe vulnerability resides in the “Tags” input field on the /s/ajax?action=lead:addLeadTags endpoint. Although the server applies sanitization before storing the data or returning it later, the payload is executed immediately in the victim’s browser upon reflection, allowing an attacker to run arbitrary JavaScript in the user’s session. ImpactA Reflected XSS attack can have a significant impact, allowing attackers to steal sensitive user data like cookies, redirect users to malicious websites, manipulate the web page content, and essentially take control of a user's session within an application by executing malicious JavaScript code within the victim's browser, even if the server-side code is secure; essentially enabling them to perform actions as if they were the logged-in user. References * Web Security Academy: Cross-site scripting https://portswigger.net/web-security/cross-site-scripting * Web Security Academy: Reflected cross-site scripting https://portswigger.net/web-	N/A	More Details

	security/cross-site-scripting/reflected		
CVE-2025-48876	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2025-58401	Obsidian GitHub Copilot Plugin versions prior to 1.1.7 store Github API token in cleartext form. As a result, an attacker may perform unauthorized operations on the linked Github account.	N/A	More Details
CVE-2025-58359	ZF FROST is a Rust implementation of FROST (Flexible Round-Optimised Schnorr Threshold signatures). In versions 2.0.0 through 2.1.0, refresh shares with smaller min_signers will reduce security of group. The inability to change min_signers (i.e. the threshold) with the refresh share functionality (frost_core::keys::refresh module) was not made clear to users. Using a smaller value would not decrease the threshold, and attempts to sign using a smaller threshold would fail. Additionally, after refreshing the shares with a smaller threshold, it would still be possible to sign with the original threshold, potentially causing a security loss to the participant's shares. This issue is fixed in version 2.2.0.	N/A	More Details
CVE-2025-58352	Weblate is a web based localization tool. Versions lower than 5.13.1 contain a vulnerability that causes long session expiry during the second factor verification. The long session expiry could be used to circumvent rate limiting of the second factor. This issue is fixed in version 5.13.1.	N/A	More Details
CVE-2025-55739	api is a module for FreePBX@, which is an open source GUI that controls and manages Asterisk© (PBX). In versions lower than 15.0.13, 16.0.2 through 16.0.14, 17.0.1 and 17.0.2, there is an identical OAuth private key used across multiple systems that installed the same FreePBX RPM or DEB package. An attacker with access to the shared OAuth private key could forge JWT tokens, bypass authentication, and potentially gain full access to both REST and GraphQL APIs. Systems with the "api" module enabled, configured and previously activated by an administrator for remote inbound connections may be affected. This issue is fixed in versions 15.0.13, 16.0.15 and 17.0.3.	N/A	More Details
CVE-2025-58366	Onyxia is a data science environment for kubernetes. In versions 4.6.0 through 4.8.0, Onyxia-API leaked the credentials of private helm repositories in the public (unauthenticated) /public/catalogs endpoint.vOnly instances using private helm repositories (i.e setting username & password in the catalogs configuration) are affected. This is fixed in version 4.9.0.	N/A	More Details
CVE-2025-58367	DeepDiff is a project focused on Deep Difference and search of any Python data. Versions 5.0.0 through 8.6.0 are vulnerable to class pollution via the Delta class constructor, and when combined with a gadget available in DeltaDiff, it can lead to Denial of Service and Remote Code Execution (via insecure Pickle deserialization) exploitation. The gadget available in DeepDiff allows `deepdiff.serialization.SAFE_TO_IMPORT` to be modified to allow dangerous classes such as posix.system, and then perform insecure Pickle deserialization via the Delta class. This potentially allows any Python code to be executed, given that the input to Delta is user-controlled. Depending on the application where DeepDiff is used, this can also lead to other vulnerabilities. This is fixed in version 8.6.1.	N/A	More Details
CVE-2025-55209	contactmanager is a module for FreePBX@, which is an open source GUI that controls and manages Asterisk© (PBX). In versions 15.0.14 and below, 16.0.0 through 16.0.26.4 and 17.0.0 through 17.0.5, a stored cross-site scripting (XSS) vulnerability in FreePBX allows a low-privileged User Control Panel (UCP) user to inject malicious JavaScript into the system. The malicious code executes in the context of an administrator when they interact with the affected component, leading to session hijacking and potential privilege escalation. This issue is fixed in versions 15.0.14, 16.0.27 and 17.0.6.	N/A	More Details
CVE-2025-58371	Roo Code is an AI-powered autonomous coding agent that lives in users' editors. In versions 3.26.6 and below, a Github workflow used unsanitized pull request metadata in a privileged context, allowing an attacker to craft malicious input and achieve Remote Code Execution (RCE) on the Actions runner. The workflow runs with broad permissions and access to repository secrets. It is possible for an attacker to execute arbitrary commands on the runner, push or modify code in the repository, access secrets, and create malicious releases or packages, resulting in a complete compromise of the repository and its associated services. This is fixed in version 3.26.7.	N/A	More Details
CVE-2025-58375	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2025-58904	Rejected reason: Not used	N/A	More Details
CVE-2025-58905	Rejected reason: Not used	N/A	More Details
CVE-2025-58906	Rejected reason: Not used	N/A	More Details
CVE-2025-38706	In the Linux kernel, the following vulnerability has been resolved: ASoC: core: Check for rtd == NULL in snd_soc_remove_pcm_runtime() snd_soc_remove_pcm_runtime() might be called with rtd == NULL which will leads to null pointer dereference. This was reproduced with topology loading and marking a link as ignore due to missing hardware component on the system. On module removal the soc_tplg_remove_link() would call	N/A	More Details

	snd_soc_remove_pcm_runtime() with rtd == NULL since the link was ignored, no runtime was created.		
CVE-2025-9467	When the Vaadin Upload's start listener is used to validate metadata about an incoming upload, it is possible to bypass the upload validation. Users of affected versions should apply the following mitigation or upgrade. Releases that have fixed this issue include: Product version Vaadin 7.0.0 - 7.7.47 Vaadin 8.0.0 - 8.28.1 Vaadin 14.0.0 - 14.13.0 Vaadin 23.0.0 - 23.6.1 Vaadin 24.0.0 - 24.7.6 Mitigation Upgrade to 7.7.48 Upgrade to 8.28.2 Upgrade to 14.13.1 Upgrade to 23.6.2 Upgrade to 24.7.7 or newer Please note that Vaadin versions 10-13 and 15-22 are no longer supported and you should update either to the latest 14, 23, 24 version. Artifacts Maven coordinatesVulnerable versionsFixed versioncom.vaadin:vaadin-server 7.0.0 - 7.7.47 ≥7.7.48 com.vaadin:vaadin-server 8.0.0 - 8.28.1 ≥8.28.2 com.vaadin:vaadin 14.0.0 - 14.13.0 ≥14.13.1 com.vaadin:vaadin23.0.0 - 23.6.1 ≥23.6.2 com.vaadin:vaadin24.0.0 - 24.7.6 ≥24.7.7com.vaadin:vaadin-upload-flow 2.0.0 - 14.13.0 ≥14.13.1 com.vaadin:vaadin-upload-flow 23.0.0 - 23.6.1 ≥23.6.2 com.vaadin:vaadin-upload-flow 24.0.0 - 24.7.6 ≥24.7.7	N/A	More Details
CVE-2025-58446	xgrammar is an open-source library for efficient, flexible, and portable structured generation. A grammar optimizer introduced in 0.1.23 processes large grammars (>100k characters) at very low rates, and can be used for DOS of model providers. This issue is fixed in version 0.1.24.	N/A	More Details
CVE-2025-59016	Error messages containing sensitive information in the File Abstraction Layer in TYPO3 CMS versions 9.0.0-9.5.54, 10.0.0-10.4.53, 11.0.0-11.5.47, 12.0.0-12.4.36, and 13.0.0-13.4.17 allow backend users to disclose full file paths via failed low-level file-system operations.	N/A	More Details
CVE-2025-8007	A security issue exists in the protected mode of 1756-EN4TR and 1756-EN2TR communication modules, where a Concurrent Forward Close operation can trigger a Major Non-Recoverable (MNFR) fault. This condition may lead to unexpected system crashes and loss of device availability.	N/A	More Details
CVE-2025-58422	RICOH Streamline NX versions 3.5.1 to 24R3 are vulnerable to tampering with operation history. If an attacker can perform a man-in-the-middle attack, they may alter the values of HTTP requests, which could result in tampering with the operation history of the product’s management tool.	N/A	More Details
CVE-2025-9364	An open database issue exists in the affected product and version. The security issue stems from an over permissive Redis instance. This could result in an attacker on the intranet accessing sensitive data and potential alteration of data.	N/A	More Details
CVE-2025-9166	A denial-of-service security issue exists in the affected product and version. The security issue stems from the controller repeatedly attempting to forward messages. The issue could result in a major nonrecoverable fault on the controller.	N/A	More Details
CVE-2025-9161	A security issue exists within FactoryTalk Optix MQTT broker due to the lack of URI sanitization. This flaw enables the loading of remote Mosquito plugins, which can be used to achieve remote code execution.	N/A	More Details
CVE-2025-9160	A code execution security issue exists in the affected product. An attacker with physical access could abuse the maintenance menu of the controller with a crafted payload. The security issue can result in arbitrary code execution.	N/A	More Details
CVE-2025-9065	A server-side request forgery security issue exists within Rockwell Automation ThinManager® software due to the lack of input sanitization. Authenticated attackers can exploit this vulnerability by specifying external SMB paths, exposing the ThinServer® service account NTLM hash.	N/A	More Details
CVE-2025-8008	A security issue exists in the protected mode of EN4TR devices, where sending specifically crafted messages during a Forward Close operation can cause the device to crash.	N/A	More Details
CVE-2025-7970	A security issue exists within FactoryTalk Activation Manager. An error in the implementation of cryptography within the software could allow attackers to decrypt traffic. This could result in data exposure, session hijacking, or full communication compromise.	N/A	More Details
CVE-2025-58443	FOG is a free open-source cloning/imaging/rescue suite/inventory management system. Versions 1.5.10.1673 and below contain an authentication bypass vulnerability. It is possible for an attacker to perform an unauthenticated DB dump where they could pull a full SQL DB without credentials. A fix is expected to be released 9/15/2025. To address this vulnerability immediately, upgrade to the latest version of either the dev-branch or working-1.6 branch. This will patch the issue for users concerned about immediate exposure. See the FOG Project documentation for step-by-step upgrade instructions: https://docs.fogproject.org/en/latest/install-fog-server#choosing-a-fog-version.	N/A	More Details
CVE-2025-7350	A security issue affecting multiple Cisco devices also directly impacts Stratix® 5410, 5700, and 8000 devices. This can lead to remote code execution by uploading and running malicious configurations without authentication.	N/A	More Details
CVE-2025-48208	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') vulnerability in Apache HertzBeat . The attacker needs to have an authenticated account with access, and the attack can only be triggered by crafting custom commands. A successful attack would result in arbitrary script execution. This issue affects Apache HertzBeat: through 1.7.2. Users are recommended to upgrade to version [1.7.3], which fixes the issue.	N/A	More Details
CVE-2025-24404	XML Injection RCE by parse http sitemap xml response vulnerability in Apache HertzBeat. The attacker needs to have an authenticated account with access, and add monitor parsed by xml, returned special content can trigger the XML parsing vulnerability. This issue affects Apache HertzBeat (incubating): before 1.7.0. Users are recommended to upgrade to version 1.7.0, which fixes the issue.	N/A	More Details

CVE-2025-10095	A SQL injection vulnerability has been identified in the SMPP server component of the SMSEagle firmware, specifically affecting the handling of certain parameters within the server's database interactions. The vulnerability is isolated to the SMPP server, which operates with its own dedicated database, separate from the main software's database. This isolation limits the scope of the vulnerability to the SMPP server's operations. The vulnerability arises from improper sanitization of user input in the SMPP server's scripts. This issue has been fixed in version 6.11.	N/A	More Details
CVE-2025-59019	Missing authorization checks in the CSV download feature of TYPO3 CMS versions 11.0.0-11.5.47, 12.0.0-12.4.36, and 13.0.0-13.4.17 allow backend users to disclose information from arbitrary database tables stored within the users' web mounts without having access to them.	N/A	More Details
CVE-2025-59018	Missing authorization checks in the Workspace Module of TYPO3 CMS versions 9.0.0-9.5.54, 10.0.0-10.4.53, 11.0.0-11.5.47, 12.0.0-12.4.36, and 13.0.0-13.4.17 allow backend users to directly invoke the corresponding AJAX backend route to disclose sensitive information without having access.	N/A	More Details
CVE-2025-59017	Missing authorization checks in the Backend Routing of TYPO3 CMS versions 9.0.0-9.5.54, 10.0.0-10.4.53, 11.0.0-11.5.47, 12.0.0-12.4.36, and 13.0.0-13.4.17 allow backend users to directly invoke AJAX backend routes without having access to the corresponding backend modules.	N/A	More Details
CVE-2025-38728	In the Linux kernel, the following vulnerability has been resolved: smb3: fix for slab out of bounds on mount to ksmbd With KASAN enabled, it is possible to get a slab out of bounds during mount to ksmbd due to missing check in parse_server_interfaces() (see below): BUG: KASAN: slab-out-of-bounds in parse_server_interfaces+0x14ee/0x1880 [cifs] Read of size 4 at addr ffff8881433dba98 by task mount/9827 CPU: 5 UID: 0 PID: 9827 Comm: mount Tainted: G OE 6.16.0-rc2-kasan #2 PREEMPT(voluntary) Tainted: [O]=OOT_MODULE, [E]=UNSIGNED_MODULE Hardware name: Dell Inc. Precision Tower 3620/0MWYPT, BIOS 2.13.1 06/14/2019 Call Trace: <TASK> dump_stack_lvl+0x9f/0xf0 print_report+0xd1/0x670 __virt_addr_valid+0x22c/0x430 ? parse_server_interfaces+0x14ee/0x1880 [cifs] ? kasan_complete_mode_report_info+0x2a/0x1f0 ? parse_server_interfaces+0x14ee/0x1880 [cifs] kasan_report+0xd6/0x110 parse_server_interfaces+0x14ee/0x1880 [cifs] __asan_report_load_n_noabort+0x13/0x20 parse_server_interfaces+0x14ee/0x1880 [cifs] ? __pfx_parse_server_interfaces+0x10/0x10 [cifs] ? trace_hardirqs_on+0x51/0x60 SMB3_request_interfaces+0x1ad/0x3f0 [cifs] ? __pfx_SMB3_request_interfaces+0x10/0x10 [cifs] ? SMB2_tcon+0x23c/0x15d0 [cifs] smb3_qfs_tcon+0x173/0x2b0 [cifs] ? __pfx_smb3_qfs_tcon+0x10/0x10 [cifs] ? cifs_get_tcon+0x105d/0x2120 [cifs] ? do_raw_spin_unlock+0x5d/0x200 ? cifs_get_tcon+0x105d/0x2120 [cifs] ? __pfx_smb3_qfs_tcon+0x10/0x10 [cifs] cifs_mount_get_tcon+0x369/0xb90 [cifs] ? dfs_cache_find+0xe7/0x150 [cifs] dfs_mount_share+0x985/0x2970 [cifs] ? check_path.constprop.0+0x28/0x50 ? save_trace+0x54/0x370 ? __pfx_dfs_mount_share+0x10/0x10 [cifs] ? __lock_acquire+0xb82/0x2ba0 ? __kasan_check_write+0x18/0x20 cifs_mount+0xbc/0x9e0 [cifs] ? __pfx_cifs_mount+0x10/0x10 [cifs] ? do_raw_spin_unlock+0x5d/0x200 ? cifs_setup_cifs_sb+0x29d/0x810 [cifs] cifs_smb3_do_mount+0x263/0x1990 [cifs]	N/A	More Details
CVE-2025-47416	A vulnerability exists in the ConsoleFindCommandMatchList function in libsymproc. so imported by ctpd that may lead to unauthorized execution of an attacker-defined file that gets prioritized by the ConsoleFindCommandMatchList. A third-party researcher discovered that the ConsoleFindCommandMatchList enumerates the /dev/shm/symproc/c directory in alphabetical order to identify console commands. Permission levels are inferred from the integer values present in each command's file name. Confirmed Affected Hardware: TSW-760, TSW-1060 Confirmed Affected Firmware: 3.002.1061 Fixed Firmware: no fixed released (product is discontinued and end of life) For x70 The Affected Firmware:- 3.000.0110.001 and versions below The Fixed Firmware:- 3.001.0031.001	N/A	More Details
CVE-2025-38729	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Validate UAC3 power domain descriptors, too UAC3 power domain descriptors need to be verified with its variable bLength for avoiding the unexpected OOB accesses by malicious firmware, too.	N/A	More Details
CVE-2025-9951	A heap-buffer-overflow write exists in jpeg2000dec FFmpeg which allows an attacker to potentially gain remote code execution or cause denial of service via the channel definition cdef atom of JPEG2000.	N/A	More Details
CVE-2025-58445	Atlantis is a self-hosted golang application that listens for Terraform pull request events via webhooks. All versions of Atlantis publicly expose detailed version information through its /status endpoint. This information disclosure could allow attackers to identify and target known vulnerabilities associated with the specific versions, potentially compromising the service's security posture. This issue does not currently have a fix.	N/A	More Details
CVE-2025-39727	In the Linux kernel, the following vulnerability has been resolved: mm: swap: fix potential buffer overflow in setup_clusters() In setup_swap_map(), we only ensure badpages are in range (0, last_page]. As maxpages might be < last_page, setup_clusters() will encounter a buffer overflow when a badpage is >= maxpages. Only call inc_cluster_info_page() for badpage which is < maxpages to fix the issue.	N/A	More Details
CVE-2025-39729	In the Linux kernel, the following vulnerability has been resolved: crypto: ccp - Fix dereferencing uninitialized error pointer Fix below smatch warnings: drivers/crypto/ccp/sev-dev.c:1312 __sev_platform_init_locked() error: we previously assumed 'error' could be null	N/A	More Details
CVE-2025-39730	In the Linux kernel, the following vulnerability has been resolved: NFS: Fix filehandle bounds checking in nfs_fh_to_dentry() The function needs to check the minimal filehandle length before it can access the embedded filehandle.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: f2fs: vm_unmap_ram() may be called from an invalid context When testing F2FS with xfstests using UFS backed virtual disks the kernel complains sometimes that		

CVE-2025-39731	f2fs_release_decomp_mem() calls vm_unmap_ram() from an invalid context. Example trace from f2fs/007 test: f2fs/007 5s ... [12:59:38][8.902525] run fstests f2fs/007 [11.468026] BUG: sleeping function called from invalid context at mm/vmalloc.c:2978 [11.471849] in_atomic(): 1, irqs_disabled(): 1, non_block: 0, pid: 68, name: irq/22-ufshcd [11.475357] preempt_count: 1, expected: 0 [11.476970] RCU nest depth: 0, expected: 0 [11.478531] CPU: 0 UID: 0 PID: 68 Comm: irq/22-ufshcd Tainted: G W 6.16.0-rc5-xfstests-ufs-g40f92e79b0aa #9 PREEMPT(none) [11.478535] Tainted: [W]=WARN [11.478536] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [11.478537] Call Trace: [11.478543] <TASK> [11.478545] dump_stack_lvl+0x4e/0x70 [11.478554] __might_resched.cold+0xaf/0xbe [11.478557] vm_unmap_ram+0x21/0xb0 [11.478560] f2fs_release_decomp_mem+0x59/0x80 [11.478563] f2fs_free_dic+0x18/0x1a0 [11.478565] f2fs_finish_read_bio+0xd7/0x290 [11.478570] blk_update_request+0xec/0x3b0 [11.478574] ? sbitmap_queue_clear+0x3b/0x60 [11.478576] scsi_end_request+0x27/0x1a0 [11.478582] scsi_io_completion+0x40/0x300 [11.478583] ufshcd_mcq_poll_cqe_lock+0xa3/0xe0 [11.478588] ufshcd_sl_intr+0x194/0x1f0 [11.478592] ufshcd_threaded_intr+0x68/0xb0 [11.478594] ? __pfx_irq_thread_fn+0x10/0x10 [11.478599] irq_thread_fn+0x20/0x60 [11.478602] ? __pfx_irq_thread_fn+0x10/0x10 [11.478603] irq_thread+0xb9/0x180 [11.478605] ? __pfx_irq_thread_dtor+0x10/0x10 [11.478607] ? __pfx_irq_thread+0x10/0x10 [11.478609] kthread+0x10a/0x230 [11.478614] ? __pfx_kthread+0x10/0x10 [11.478615] ret_from_fork+0x7e/0xd0 [11.478619] ? __pfx_kthread+0x10/0x10 [11.478621] ret_from_fork_asm+0x1a/0x30 [11.478623] </TASK> This patch modifies in_task() check inside f2fs_read_end_io() to also check if interrupts are disabled. This ensures that pages are unmapped asynchronously in an interrupt handler.	N/A	More Details
CVE-2025-39732	In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: fix sleeping-in-atomic in ath11k_mac_op_set_bitrate_mask() ath11k_mac_disable_peer_fixed_rate() is passed as the iterator to ieee80211_iterate_stations_atomic(). Note in this case the iterator is required to be atomic, however ath11k_mac_disable_peer_fixed_rate() does not follow it as it might sleep. Consequently below warning is seen: BUG: sleeping function called from invalid context at wmi.c:304 Call Trace: <TASK> dump_stack_lvl __might_resched.cold ath11k_wmi_cmd_send ath11k_wmi_set_peer_param ath11k_mac_disable_peer_fixed_rate ieee80211_iterate_stations_atomic ath11k_mac_op_set_bitrate_mask.cold Change to ieee80211_iterate_stations_mtx() to fix this issue. Tested-on: WCN6855 hw2.0 PCI WLAN.HSP.1.1-03125-QCAHSPSWPL_V1_V2_SILICONZ_LITE-3.6510.30	N/A	More Details
CVE-2025-39733	In the Linux kernel, the following vulnerability has been resolved: team: replace team lock with rtnl lock syszbot reports various ordering issues for lower instance locks and team lock. Switch to using rtnl lock for protecting team device, similar to bonding. Based on the patch by Tetsuo Handa.	N/A	More Details
CVE-2025-39734	In the Linux kernel, the following vulnerability has been resolved: Revert "fs/ntfs3: Replace inode_trylock with inode_lock" This reverts commit 69505fe98f198ee813898cbcaf6770949636430b. Initially, conditional lock acquisition was removed to fix an xfstest bug that was observed during internal testing. The deadlock reported by syzbot is resolved by reintroducing conditional acquisition. The xfstest bug no longer occurs on kernel version 6.16-rc1 during internal testing. I assume that changes in other modules may have contributed to this.	N/A	More Details
CVE-2025-48042	Incorrect Authorization vulnerability in ash-project ash allows Exploiting Incorrectly Configured Access Control Security Levels. This vulnerability is associated with program files lib/ash/actions/create/bulk.ex, lib/ash/actions/destroy/bulk.ex, lib/ash/actions/update/bulk.ex and program routines 'Elixir.Ash.Actions.Create.Bulk':run/5, 'Elixir.Ash.Actions.Destroy.Bulk':run/6, 'Elixir.Ash.Actions.Update.Bulk:run'/6. This issue affects ash: from pkg:hex/ash before pkg:hex/ash@3.5.39, before 3.5.39, before 5d1b6a5d00771fd468a509778637527b5218be9a.	N/A	More Details
CVE-2025-38730	In the Linux kernel, the following vulnerability has been resolved: io_uring/net: commit partial buffers on retry Ring provided buffers are potentially only valid within the single execution context in which they were acquired. io_uring deals with this and invalidates them on retry. But on the networking side, if MSG_WAITALL is set, or if the socket is of the streaming type and too little was processed, then it will hang on to the buffer rather than recycle or commit it. This is problematic for two reasons: 1) If someone unregisters the provided buffer ring before a later retry, then the req->buf_list will no longer be valid. 2) If multiple sockers are using the same buffer group, then multiple receives can consume the same memory. This can cause data corruption in the application, as either receive could land in the same userspace buffer. Fix this by disallowing partial retries from pinning a provided buffer across multiple executions, if ring provided buffers are used.	N/A	More Details
CVE-2025-52915	K7RKScan.sys 23.0.0.10, part of the K7 Security Anti-Malware suite, allows an admin-privileged user to send crafted IOCTL requests to terminate processes that are protected through a third-party implementation. This is caused by insufficient caller validation in the driver's IOCTL handler, enabling unauthorized processes to perform those actions in kernel space. Successful exploitation can lead to denial of service by disrupting critical third-party services or applications.	N/A	More Details
CVE-2025-52322	An issue in Open5GS v2.7.2 and before allows a remote attacker to cause a denial of service via a crafted Create Session Request message to the SMF (PGW-C), using the IP address of a legitimate UE in the PDN Address Allocation (PAA) field	N/A	More Details
CVE-2025-52277	Cross Site Scripting vulnerability in YesWiki v.4.54 allows a remote attacker to execute arbitrary code via a crafted payload to the meta configuration robots field	N/A	More Details
CVE-2025-	A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.9, 2025.Q1.0 through 2025.Q1.16, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.19 and 7.4 GA through update 92 allows an remote	N/A	More Details

43776	authenticated attacker to inject JavaScript through Custom Object field label. The malicious payload is stored and executed through Process Builder's Configuration tab without proper escaping.		
CVE-2025-9994	The Amp’ed RF BT-AP 111 Bluetooth access point's HTTP admin interface does not have an authentication feature, allowing unauthorized access to anyone with network access.	N/A	More Details
CVE-2025-58907	Rejected reason: Not used	N/A	More Details