SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 20 August 2025

Generated on 20 August 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-2025-20265	A vulnerability in the RADIUS subsystem implementation of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to inject arbitrary shell commands that are executed by the device. This vulnerability is due to a lack of proper handling of user input during the authentication phase. An attacker could exploit this vulnerability by sending crafted input when entering credentials that will be authenticated at the configured RADIUS server. A successful exploit could allow the attacker to execute commands at a high privilege level. Note: For this vulnerability to be exploited, Cisco Secure FMC Software must be configured for RADIUS authentication for the web-based management interface, SSH management, or both.	10.0	More Details
CVE-2025-50567	Saurus CMS Community Edition 4.7.1 contains a vulnerability in the custom DB::prepare() function, which uses preg_replace() with the deprecated /e (eval) modifier to interpolate SQL query parameters. This leads to injection of user-controlled SQL statements, potentially leading to arbitrary PHP code execution.	10.0	More Details
CVE-2025-25174	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in beeteam368 BeeTeam368 Extensions allows PHP Local File Inclusion. This issue affects BeeTeam368 Extensions: from n/a through 1.9.4.	10.0	More Details
CVE-2025-49887	Improper Control of Generation of Code ('Code Injection') vulnerability in WPFactory Product XML Feed Manager for WooCommerce allows Remote Code Inclusion. This issue affects Product XML Feed Manager for WooCommerce: from n/a through 2.9.3.	9.9	More Details
CVE-2025-24775	Unrestricted Upload of File with Dangerous Type vulnerability in Made I.T. Forms allows Upload a Web Shell to a Web Server. This issue affects Forms: from n/a through 2.9.0.	9.9	More Details
CVE-2025-7384	The Database for Contact Form 7, WPforms, Elementor forms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.4.3 via deserialization of untrusted input in the get_lead_detail function. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain in the Contact Form 7 plugin, which is likely to be used alongside, allows attackers to delete arbitrary files, leading to a denial of service or remote code execution when the wp-config.php file is deleted.	9.8	More Details
CVE-2025-7441	The StoryChief plugin for WordPress is vulnerable to arbitrary file uploads in all versions up to, and including, 1.0.42. This vulnerability occurs through the /wp-json/storychief/webhook REST-API endpoint that does not have sufficient filetype validation. 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-2025-27845	In ESPEC North America Web Controller 3 before 3.3.4, /api/v4/auth/ with any invalid authentication request results in exposing a JWT secret. This allows for elevated permissions to the UI.	9.8	More Details
CVE-2025-50518	A use-after-free vulnerability exists in the coap_delete_pdu_lkd function within coap_pdu.c of the libcoap library. This issue occurs due to improper handling of memory after the freeing of a PDU object, leading to potential memory corruption or the possibility of executing arbitrary code.	9.8	More Details
CVE-2025-6679	The Bit Form builder plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in all versions up to, and including, 2.20.4. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. For this to be exploitable, the PRO version needs to be installed and activated as well. Additionally a form with an advanced file upload element needs to be published.	9.8	More Details
CVE-2025-7778	The Icons Factory plugin for WordPress is vulnerable to Arbitrary File Deletion due to insufficient authorization and improper path validation within the delete_files() function in all versions up to, and including, 1.6.12. This makes it possible for unauthenticated attackers to to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	9.8	More Details

CVE-2025-8995	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal Authenticator Login allows Authentication Bypass.This issue affects Authenticator Login: from 0.0.0 before 2.1.4.	9.8	More Details
CVE-2025-8898	The Taxi Booking Manager for Woocommerce | E-cab plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.3.0. This is due to the plugin not properly validating a user's capabilities prior to updating a plugin setting or their identity prior to updating their details like email address. This makes it possible for unauthenticated attackers to change arbitrary user's email addresses, including administrators, and leverage that to reset the user's password and gain access to their account.	9.8	More Details
CVE-2025-54686	Deserialization of Untrusted Data vulnerability in scriptsbundle Exertio allows Object Injection. This issue affects Exertio: from n/a through 1.3.2.	9.8	More Details
CVE-2025-31715	In vowifi service, there is a possible command injection due to improper input validation. This could lead to remote escalation of privilege with no additional execution privileges needed.	9.8	More Details
CVE-2025-55591	TOTOLINK-A3002R v4.0.0-B20230531.1404 was discovered to contain a command injection vulnerability in the devicemac parameter in the formMapDel endpoint.	9.8	More Details
CVE-2025-6758	The Real Spaces - WordPress Properties Directory Theme theme for WordPress is vulnerable to privilege escalation via the 'imic_agent_register' function in all versions up to, and including, 3.6. This is due to a lack of restriction in the registration role. This makes it possible for unauthenticated attackers to arbitrarily choose their role, including the Administrator role, during user registration.	9.8	More Details
CVE-2025-8723	The Cloudflare Image Resizing plugin for WordPress is vulnerable to Remote Code Execution due to missing authentication and insufficient sanitization within its hook_rest_pre_dispatch() method in all versions up to, and including, 1.5.6. This makes it possible for unauthenticated attackers to inject arbitrary PHP into the codebase, achieving remote code execution.	9.8	More Details
CVE-2025-54336	In Plesk Obsidian 18.0.70, _isAdminPasswordValid uses an == comparison. Thus, if the correct password is "0e" followed by any digit string, then an attacker can login with any other string that evaluates to 0.0 (such as the 0e0 string). This occurs in admin/plib/LoginManager.php.	9.8	More Details
CVE-2025-55294	screenshot-desktop allows capturing a screenshot of your local machine. This vulnerability is a command injection issue. When user-controlled input is passed into the format option of the screenshot function, it is interpolated into a shell command without sanitization. This results in arbitrary command execution with the privileges of the calling process. This vulnerability is fixed in 1.15.2.	9.8	More Details
CVE-2024-44373	A Path Traversal vulnerability in AllSky v2023.05.01_04 allows an unauthenticated attacker to create a webshell and remote code execution via the path, content parameter to /includes/save_file.php.	9.8	More Details
CVE-2025-55306	GenX_FX is an advance IA trading platform that will focus on forex trading. A vulnerability was identified in the GenX FX backend where API keys and authentication tokens may be exposed if environment variables are misconfigured. Unauthorized users could gain access to cloud resources (Google Cloud, Firebase, GitHub, etc.).	9.8	More Details
CVE-2025-6715	The LatePoint WordPress plugin before 5.1.94 is vulnerable to Local File Inclusion via the layout parameter. This makes it possible for attackers to include and execute PHP files on the server, allowing the execution of any PHP code in those files.	9.8	More Details
CVE-2025-43984	An issue was discovered on KuWFi GC111 devices (Hardware Version: CPE-LM321_V3.2, Software Version: GC111-GL-LM321_V3.0_20191211). They are vulnerable to unauthenticated /goform/goform_set_cmd_process requests. A crafted POST request, using the SSID parameter, allows remote attackers to execute arbitrary OS commands with root privileges.	9.8	More Details
CVE-2025-8943	The Custom MCPs feature is designed to execute OS commands, for instance, using tools like `npx` to spin up local MCP Servers. However, Flowise's inherent authentication and authorization model is minimal and lacks role-based access controls (RBAC). Furthermore, in Flowise versions before 3.0.1 the default installation operates without authentication unless explicitly configured. This combination allows unauthenticated network attackers to execute unsandboxed OS commands.	9.8	More Details
CVE-2025-43986	An issue was discovered on KuWFi GC111 GC111-GL-LM321_V3.0_20191211 devices. The TELNET service is enabled by default and exposed over the WAN interface without authentication.	9.8	More Details
CVE-2025-8760	A vulnerability was identified in INSTAR 2K+ and 4K 3.11.1 Build 1124. This affects the function base64_decode of the component fcgi_server. The manipulation of the argument Authorization leads to buffer overflow. It is possible to initiate the attack remotely.	9.8	More Details
CVE-2025-8913	Organization Portal System developed by WellChoose has a Local File Inclusion vulnerability, allowing unauthenticated remote attackers to execute arbitrary code on the server.	9.8	More Details
CVE-2025-52385	An issue in Studio 3T v.2025.1.0 and before allows a remote attacker to execute arbitrary code via a crafted payload to the child_process module	9.8	More Details
CVE-2025-51452	In TOTOLINK A7000R firmware 9.1.0u.6115_B20201022, an attacker can bypass login by sending a specific request through formLoginAuth.htm.	9.8	More Details
CVE-2025-50594	An issue was discovered in /Code/Websites/DanpheEMR/Controllers/Settings/SecuritySettingsController.cs in Danphe Health Hospital Management System EMR 3.2 allowing attackers to reset any account password.	9.8	More Details
CVE-2025-48293	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Dylan Kuhn Geo Mashup allows PHP Local File Inclusion. This issue affects Geo Mashup: from n/a through 1.13.16.	9.8	More Details
CVE-2025-43982	Shenzhen Tuoshi NR500-EA RG500UEAABxCOMSLICv3.4.2731.16.43 devices enable the SSH service by default. There is a hidden hard-coded root account that cannot be disabled in the GUI.	9.8	More Details
CVE-2025-8047	The disable-right-click-powered-by-pixterme through v1.2 and pixter-image-digital-license thtough v1.0 WordPress plugins load a JavaScript file which has been compromised from an apparent abandoned S3 bucket. It can be used as a backdoor by those who control it, but it currently displays an alert marketing security services. Users that pay are added to allowedDomains to suppress the popup.	9.8	More Details
CVE-2025-55346	User-controlled input flows to an unsafe implementation of a dynamic Function constructor, allowing network attackers to run arbitrary unsandboxed JS code in the context of the host, by sending a simple POST request.	9.8	More Details
CVE-2025-	In TOTOLINK EX1200T firmware 4.1.2cu.5215, an attacker can bypass login by sending a specific request through	9.8	More Details

51451	formLoginAuth.htm.		
CVE-2011-10018	myBB version 1.6.4 was distributed with an unauthorized backdoor embedded in the source code. The backdoor allowed remote attackers to execute arbitrary PHP code by injecting payloads into a specially crafted collapsed cookie. This vulnerability was introduced during packaging and was not part of the intended application logic. Exploitation requires no authentication and results in full compromise of the web server under the context of the web application.	9.8	More Details
CVE-2025-55733	DeepChat is a smart assistant that connects powerful AI to your personal world. DeepChat before 0.3.1 has a one-click remote code execution vulnerability. An attacker can exploit this vulnerability by embedding a specially crafted deepchat: URL on any website, including a malicious one they control. When a victim visits such a site or clicks on the link, the browser triggers the app's custom URL handler (deepchat:), causing the DeepChat application to launch and process the URL, leading to remote code execution on the victim's machine. This vulnerability is fixed in 0.3.1.	9.6	More Details
CVE-2025-54382	Cherry Studio is a desktop client that supports for multiple LLM providers. In version 1.5.1, a remote code execution (RCE) vulnerability exists in the Cherry Studio platform when connecting to streamableHttp MCP servers. The issue arises from the server's implicit trust in the oauth auth redirection endpoints and failure to properly sanitize the URL. This issue has been patched in version 1.5.2.	9.6	More Details
CVE-2025-55293	Meshtastic is an open source mesh networking solution. Prior to v2.6.3, an attacker can send NodeInfo with a empty publicKey first, then overwrite it with a new key. First sending a empty key bypasses 'if (p.public_key.size > 0) {', clearing the existing publicKey (and resetting the size to 0) for a known node. Then a new key bypasses 'if (info->user.public_key.size > 0) {', and this malicious key is stored in NodeDB. This vulnerability is fixed in 2.6.3.	9.4	More Details
CVE-2025-55299	VaulTLS is a modern solution for managing mTLS (mutual TLS) certificates. Prior to 0.9.1, user accounts created through the User web UI have an empty but not NULL password set, attackers can use this to login with an empty password. This is combined with that fact, that previously disabling the password based login only effected the frontend, but still allowed login via the API. This vulnerability is fixed in 0.9.1.	9.4	More Details
CVE-2025-54678	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in hassantafreshi Easy Form Builder allows Blind SQL Injection. This issue affects Easy Form Builder: from n/a through 3.8.15.	9.3	More Details
CVE-2025-49059	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CleverReach® CleverReach® WP allows SQL Injection. This issue affects CleverReach® WP: from n/a through 1.5.20.	9.3	More Details
CVE-2025-52720	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in highwarden Super Store Finder allows SQL Injection. This issue affects Super Store Finder: from n/a through 7.5.	9.3	More Details
CVE-2025-54669	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RomanCode MapSVG allows SQL Injection. This issue affects MapSVG: from n/a through n/a.	9.3	More Details
CVE-2025-54707	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RealMag777 MDTF allows SQL Injection. This issue affects MDTF: from n/a through 1.3.3.7.	9.3	More Details
CVE-2025-55283	aiven-db-migrate is an Aiven database migration tool. Prior to 1.0.7, there is a privilege escalation vulnerability that allows elevation to superuser inside PostgreSQL databases during a migration from an untrusted source server. The vulnerability stems from psql executing commands embedded in a dump from the source server. This vulnerability is fixed in 1.0.7.	9.1	More Details
CVE-2025-55282	aiven-db-migrate is an Aiven database migration tool. Prior to 1.0.7, there is a privilege escalation vulnerability that allows a user to elevate to superuser inside PostgreSQL databases during a migration from an untrusted source server. By exploiting a lack of search_path restriction, an attacker can override pg_catalog and execute untrusted operators as a superuser. This vulnerability is fixed in 1.0.7.	9.1	More Details
CVE-2025-9060	A vulnerability has been found in the MSoft MFlash application that allows execution of arbitrary code on the server. The issue occurs in the integration configuration functionality that is only available to MFlash administrators. The vulnerability is related to insufficient validation of parameters when setting up security components. This issue affects MFlash v. 8.0 and possibly others. To mitigate apply 8.2-653 hotfix 11.06.2025 and above.	9.1	More Details
CVE-2025-43983	KuWFi CPF908-CP5 WEB5.0_LCD_20210125 devices have multiple unauthenticated access control vulnerabilities within goform/goform_set_cmd_process and goform/goform_get_cmd_process. These allow an unauthenticated attacker to retrieve sensitive information (including the device admin username and password), modify critical device settings, and send arbitrary SMS messages.	9.1	More Details
CVE-2025-50251	Server side request forgery (SSRF) vulnerability in makeplane plane 0.23.1 via the password recovery.	9.1	More Details
CVE-2025-55205	Capsule is a multi-tenancy and policy-based framework for Kubernetes. A namespace label injection vulnerability in Capsule v0.10.3 and earlier allows authenticated tenant users to inject arbitrary labels into system namespaces (kube-system, default, capsule-system), bypassing multi-tenant isolation and potentially accessing cross-tenant resources through TenantResource selectors. This vulnerability enables privilege escalation and violates the fundamental security boundaries that Capsule is designed to enforce. This vulnerability is fixed in 0.10.4.	9.0	More Details
CVE-2025-54693	Unrestricted Upload of File with Dangerous Type vulnerability in epiphyt Form Block allows Upload a Web Shell to a Web Server. This issue affects Form Block: from n/a through 1.5.5.	9.0	More Details
CVE-2025-54117	NamelessMC is a free, easy to use & powerful website software for Minecraft servers. Cross-site scripting (XSS) vulnerability in NamelessMC before 2.2.3 allows remote authenticated attackers to inject arbitrary web script or HTML via the dashboard text editor component. This vulnerability is fixed in 2.2.4.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2025-36120	IBM Storage Virtualize 8.4, 8.5, 8.6, and 8.7 could allow an authenticated user to escalate their privileges in an SSH session due to incorrect authorization checks to resources.
CVE-	The KuWFi 4G AC900 LTE router 1.0.13 is vulnerable to command injection on the HTTP API endpoints /goform/formMultiApnSetting and /goform/atCmd. An authen

2024-53945	attacker can execute arbitrary OS commands with root privileges via shell metacharacters in parameters such as pincode and cmds. Exploitation can lead to full sy compromise, including enabling remote access (e.g., enabling telnet).
CVE-2025-9007	A vulnerability has been found in Tenda CH22 1.0.0.1. Affected by this issue is the function formeditFileName of the file /goform/editFileName. The manipulation le buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-9006	A vulnerability was identified in Tenda CH22 1.0.0.1. Affected by this vulnerability is the function formdelFileName of the file /goform/delFileName. The manipulatio buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-55154	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-27 and 7.1.2-1, the magnified size calculat ReadOneMNGIMage (in coders/png.c) are unsafe and can overflow, leading to memory corruption. This issue has been patched in versions 6.9.13-27 and 7.1.2-1.
CVE-2025-53192	** UNSUPPORTED WHEN ASSIGNED ** Improper Neutralization of Expression/Command Delimiters vulnerability in Apache Commons OGNL. This issue affects Apach Commons OGNL: all versions. When using the API Ognl.getValue, the OGNL engine parses and evaluates the provided expression with powerful capabilities, includi accessing and invoking related methods, etc. Although OgnlRuntime attempts to restrict certain dangerous classes and methods (such as java.lang.Runtime) throu blocklist, these restrictions are not comprehensive. Attackers may be able to bypass the restrictions by leveraging class objects that are not covered by the blockli potentially achieve arbitrary code execution. As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an a or restrict access to the instance to trusted users. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.
CVE-2025-8958	A vulnerability was identified in Tenda TX3 16.03.13.11_multi_TDE01. Affected by this vulnerability is an unknown functionality of the file /goform/fast_setting_wifi_ manipulation of the argument ssid leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and ma
CVE-2025-7654	Multiple FunnelKit plugins are vulnerable to Sensitive Information Exposure via the wf_get_cookie shortcode. This makes it possible for authenticated attackers, wit Contributor-level access and above, to extract sensitive data including authentication cookies of other site users, which may make privilege escalation possible. Ple both FunnelKit – Funnel Builder for WooCommerce Checkout AND FunnelKit Automations – Email Marketing Automation and CRM for WordPress & WooCommerce a affected by this.
CVE-2025-8714	Untrusted data inclusion in pg_dump in PostgreSQL allows a malicious superuser of the origin server to inject arbitrary code for restore-time execution as the client system account running psql to restore the dump, via psql meta-commands. pg_dumpall is also affected. pg_restore is affected when used to generate a plain-form This is similar to MySQL CVE-2024-21096. Versions before PostgreSQL 17.6, 16.10, 15.14, 14.19, and 13.22 are affected.
CVE-2025-8715	Improper neutralization of newlines in pg_dump in PostgreSQL allows a user of the origin server to inject arbitrary code for restore-time execution as the client ope system account running psql to restore the dump, via psql meta-commands inside a purpose-crafted object name. The same attacks can achieve SQL injection as a superuser of the restore target server. pg_dumpall, pg_restore, and pg_upgrade are also affected. Versions before PostgreSQL 17.6, 16.10, 15.14, 14.19, and 13.22 affected. Versions before 11.20 are unaffected. CVE-2012-0868 had fixed this class of problem, but version 11.20 reintroduced it.
CVE-2025-8940	A vulnerability was identified in Tenda AC20 up to 16.03.08.12. Affected by this vulnerability is the function strcpy of the file /goform/saveParentControlInfo. The manipulation of the argument Time leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8939	A vulnerability was determined in Tenda AC20 up to 16.03.08.12. Affected is an unknown function of the file /goform/WifiGuestSet. The manipulation of the argume shareSpeed leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-53946	The KuWFi 4G LTE AC900 router 1.0.13 is vulnerable to Cross-Site Request Forgery (CSRF) on its web management interface. This vulnerability allows an attacker t authenticated admin user into performing unauthorized actions, such as exploiting a command injection vulnerability in /goform/formMultiApnSetting. Successful e can also lead to unauthorized configuration changes.
CVE-2025-52732	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in RealMag777 Google Map Targeting allows File Inclusion. This issue affects Google Map Targeting: from n/a through 1.1.6.
CVE-2025-49895	Cross-Site Request Forgery (CSRF) vulnerability in iThemes ServerBuddy by PluginBuddy.Com allows Object Injection.This issue affects ServerBuddy by PluginBudd from n/a through 1.0.5.
CVE-2025-3671	The WPGYM - Wordpress Gym Management System plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 67.7.0 via the 'pag parameter. This makes it possible for authenticated attackers, with Subscriber-level access and above, to include and execute arbitrary files on the server, allowing 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 images and o “safe” file types can be uploaded and included. The Local File Inclusion exploit can be chained to include various dashboard view files in the plugin. One in particula reported by the researcher can be leveraged to update the password of Super Administrator accounts in Multisite environments making privilege escalation possibl
CVE-2025-6079	The School Management System for Wordpress plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the homework.php versions up to, and including, 93.2.0. This makes it possible for authenticated attackers, with Student-level access and above, to upload arbitrary files on the affect server which may make remote code execution possible.
CVE-2025-6080	The WPGYM - Wordpress Gym Management System plugin for WordPress is vulnerable to unauthorized admin account creation in all versions up to, and including, This is due to the plugin not properly validating a user's capabilities prior to adding users. This makes it possible for authenticated attackers, with Subscriber-level and above, to create new users, including admins.
CVE-2025-53587	Cross-Site Request Forgery (CSRF) vulnerability in ApusTheme Findgo allows Cross Site Request Forgery. This issue affects Findgo: from n/a through 1.3.57.
CVE-2025-8876	Improper Input Validation vulnerability in N-able N-central allows OS Command Injection.This issue affects N-central: before 2025.3.1.
CVE-2025-9089	A vulnerability was determined in Tenda AC20 16.03.08.12. This issue affects the function sub_48E628 of the file /goform/SetIpMacBind. The manipulation of the ar list leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-	A vulnerability was found in Tenda AC20 16.03.08.12. This vulnerability affects the function save_virtualser_data of the file /goform/formSetVirtualSer. The manipul

9088	the argument list leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-9087	A vulnerability has been found in Tenda AC20 16.03.08.12. This affects the function set_qosMib_list of the file /goform/SetNetControlList of the component SetNetC Endpoint. The manipulation of the argument list leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to public and may be used.
CVE-2025-8142	The Soledad theme for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 8.6.7 via the 'header_layout' parameter. This makes it pos authenticated attackers, with Contributor-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code 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.
CVE-2025-32451	A memory corruption vulnerability exists in Foxit Reader 2025.1.0.27937 due to the use of an uninitialized pointer. A specially crafted Javascript code inside a malic document can trigger this vulnerability, which can lead to memory corruption and result in arbitrary code execution. An attacker needs to trick the user into openir malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled.
CVE-2025-8218	The Real Spaces - WordPress Properties Directory Theme theme for WordPress is vulnerable to privilege escalation via the 'change_role_member' parameter in all v up to, and including, 3.5. This is due to a lack of restriction in the profile update role. This makes it possible for unauthenticated attackers to arbitrarily choose thei including the Administrator role, during a profile update.
CVE-2025-8879	Heap buffer overflow in libaom in Google Chrome prior to 139.0.7258.127 allowed a remote attacker to potentially exploit heap corruption via a curated set of gest (Chromium security severity: High)
CVE-2025-8882	Use after free in Aura in Google Chrome prior to 139.0.7258.127 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially ex heap corruption via a crafted HTML page. (Chromium security severity: Medium)
CVE-2025-8901	Out of bounds write in ANGLE in Google Chrome prior to 139.0.7258.127 allowed a remote attacker to perform out of bounds memory access via a crafted HTML pa (Chromium security severity: High)
CVE-2025-9023	A vulnerability has been found in Tenda AC7 and AC18 15.03.05.19/15.03.06.44. Affected is the function formSetSchedLed of the file /goform/SetLEDCfg. The mani of the argument Time leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-6184	The Tutor LMS Pro – eLearning and online course solution plugin for WordPress is vulnerable to time-based SQL Injection via the 'order' parameter used in the get_submitted_assignments() function in all versions up to, and including, 3.7.0 due to insufficient escaping on the user supplied parameter and lack of sufficient p on the existing SQL query. This makes it possible for authenticated attackers, with Tutor-level access and above, to append additional SQL queries into already exis queries that can be used to extract sensitive information from the database. Only the Pro version is affected.
CVE-2025-9046	A vulnerability was identified in Tenda AC20 16.03.08.12. This issue affects the function sub_46A2AC of the file /goform/setMacFilterCfg. The manipulation of the ar deviceList leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-55345	Using Codex CLI in workspace-write mode inside a malicious context (repo, directory, etc) could lead to arbitrary file overwrite and potentially remote code executi symlinks being followed outside the allowed current working directory.
CVE-2025-49869	Deserialization of Untrusted Data vulnerability in Arraytics Eventin allows Object Injection. This issue affects Eventin: from n/a through 4.0.31.
CVE-2025-8880	Race in V8 in Google Chrome prior to 139.0.7258.127 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium s severity: High)
CVE-2025-7739	An issue has been discovered in GitLab CE/EE affecting all versions from 18.2 before 18.2.2 that, under certain conditions, could have allowed authenticated users stored cross-site scripting by injecting malicious HTML content in scoped label descriptions.
CVE-2025-7734	An issue has been discovered in GitLab CE/EE affecting all versions from 14.2 before 18.0.6, 18.1 before 18.1.4 and 18.2 before 18.2.2 that, under certain condition have allowed a successful attacker to execute actions on behalf of users by injecting malicious content.
CVE-2025-6186	An issue has been discovered in GitLab CE/EE affecting all versions from 18.1 before 18.1.4, and 18.2 before 18.2.2 that could have allowed authenticated users to account takeover by injecting malicious HTML into work item names.
CVE-2025-40758	A vulnerability has been identified in Mendix SAML (Mendix 10.12 compatible) (All versions < V4.0.3), Mendix SAML (Mendix 10.21 compatible) (All versions < V4.1 Mendix SAML (Mendix 9.24 compatible) (All versions < V3.6.21). Affected versions of the module insufficiently enforce signature validation and binding checks. This allow unauthenticated remote attackers to hijack an account in specific SSO configurations.
CVE-2025-52478	n8n is a workflow automation platform. From 1.77.0 to before 1.98.2, a stored Cross-Site Scripting (XSS) vulnerability was identified in n8n, specifically in the Form node's HTML form element. An authenticated attacker can inject malicious HTML via an <iframe> with a srcdoc payload that includes arbitrary JavaScript executio attacker can also inject malicious Javascript by using <video> coupled <source> using an onerror event. While using iframe or a combination of video and source vulnerability allows for Account Takeover (ATO) by exfiltrating n8n-browserId and session cookies from authenticated users who visit a maliciously crafted form. Us tokens and cookies, an attacker can impersonate the victim and change account details such as email addresses, enabling full control over the account—especially not enabled. Users should upgrade to version >= 1.98.2.
CVE-2025-20253	A vulnerability in the IKEv2 feature of Cisco IOS Software, IOS XE Software, Secure Firewall ASA Software, and Secure FTD Software could allow an unauthenticated attacker to cause the device to reload, resulting in a DoS condition. This vulnerability is due to the improper processing of IKEv2 packets. An attacker could exploit vulnerability by sending crafted IKEv2 packets to an affected device. A successful exploit could allow the attacker to cause an infinite loop that exhausts resources cause the device to reload.
CVE-2025-20133	A vulnerability in the management and VPN web servers of the Remote Access SSL VPN feature of Cisco Secure Firewall ASA Software and Secure FTD Software co an unauthenticated, remote attacker to cause the device to unexpectedly stop responding, resulting in a DoS condition. This vulnerability is due to ineffective valid user-supplied input during the Remote Access SSL VPN authentication process. An attacker could exploit this vulnerability by sending a crafted request to the VPN an affected device. A successful exploit could allow the attacker to cause a DoS condition where the device stops responding to Remote Access SSL VPN authentica

	requests.
CVE-2025-20263	A vulnerability in the web services interface of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) So could allow an unauthenticated, remote attacker to cause a buffer overflow on an affected system. This vulnerability is due to insufficient boundary checks f specific data that is provided to the web services interface of an affected system. An attacker could exploit this vulnerability by sending a crafted HTTP request to t affected system. A successful exploit could allow the attacker to cause a buffer overflow condition on the affected system, which could cause the system to reload, in a denial of service (DoS) condition.
CVE-2025-20239	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) feature of Cisco IOS Software, IOS XE Software, Secure Firewall Adaptive Security Appliance (ASA) So and Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a memory leak, resulting in a denial of service (DoS) condition. This vulnerability is due to a lack of proper processing of IKEv2 packets. An attacker could exploit this vulnerability by sending crafted IKEv2 packets to a device. In the case of Cisco IOS and IOS XE Software, a successful exploit could allow the attacker to cause the device to reload unexpectedly. In the case of Cisco FTD Software, a successful exploit could allow the attacker to partially exhaust system memory, causing system instability such as being unable to establish new IK sessions. A manual reboot of the device is required to recover from this condition.
CVE-2025-20134	A vulnerability in the certificate processing of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Sof could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is du improper parsing of SSL/TLS certificates. An attacker could exploit this vulnerability by sending crafted DNS packets that match a static Network Address Translatio rule with DNS inspection enabled through an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS conditio
CVE-2025-20217	A vulnerability in the packet inspection functionality of the Snort 3 Detection Engine of Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthe remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to incorrect processing of traffic that is inspected by an device. An attacker could exploit this vulnerability by sending crafted traffic through the affected device. A successful exploit could allow the attacker to cause the device to enter an infinite loop while inspecting traffic, resulting in a DoS condition. The system watchdog will restart the Snort process automatically.
CVE-2025-20136	A vulnerability in the function that performs IPv4 and IPv6 Network Address Translation (NAT) DNS inspection for Cisco Secure Firewall Adaptive Security Appliance Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, re a denial of service (DoS) condition. This vulnerability is due to an infinite loop condition that occurs when a Cisco Secure ASA or Cisco Secure FTD device pro DNS packets with DNS inspection enabled and the device is configured for NAT44, NAT64, or NAT46. An attacker could exploit this vulnerability by sending crafted packets that match a static NAT rule with DNS inspection enabled through an affected device. A successful exploit could allow the attacker to create an infinite loo cause the device to reload, resulting in a DoS condition.
CVE-2025-20243	A vulnerability in the management and VPN web servers of Cisco Secure Firewall ASA Software and Secure FTD Software could allow an unauthenticated, remote a cause the device to reload unexpectedly, resulting in a DoS condition. This vulnerability is due to improper validation of user-supplied input on an interface with VP services. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted web server on an affected device. A successful exploit could al attacker to cause a DoS condition when the device reloads.
CVE-2025-20222	A vulnerability in the RADIUS proxy feature for the IPsec VPN feature of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper processi packets. An attacker could exploit this vulnerability by sending IPv6 packets over an IPsec VPN connection to an affected device. A successful exploit could a attacker to trigger a reload of the device, resulting in a DoS condition.
CVE-2025-20148	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, remote attacke arbitrary HTML content into a device-generated document. This vulnerability is due to improper validation of user-supplied data. An attacker could exploit this vuln by submitting malicious content to an affected device and using the device to generate a document that contains sensitive information. A successful exploit could attacker to alter the standard layout of the device-generated documents, read arbitrary files from the underlying operating system, and conduct server-side reques (SSRF) attacks. To exploit this vulnerability, the attacker must have valid credentials for a user account with at least the role of Security Analyst (Read Only).
CVE-2025-20251	A vulnerability in the Remote Access SSL VPN service for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defens Software could allow an authenticated, remote attacker to create or delete arbitrary files on the underlying operating system. If critical system files are manipulate Remote Access SSL VPN sessions could be denied and existing sessions could be dropped, causing a denial of service (DoS) condition. An exploited device requires reboot to recover. This vulnerability is due to insufficient input validation when processing HTTP requests. An attacker could exploit this vulnerability by sending cra HTTP requests to an affected device. A successful exploit could allow the attacker to create or delete files on the underlying operating system, which could cause t Remote Access SSL VPN service to become unresponsive. To exploit this vulnerability, the attacker must be authenticated as a VPN user of the affected device.
CVE-2025-52820	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in infosoftplugin WooCommerce Point Of Sale (POS) allows SQL This issue affects WooCommerce Point Of Sale (POS): from n/a through 1.4.
CVE-2025-49033	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Metagauss ProfileGrid allows Blind SQL Injection. This issue a ProfileGrid : from n/a through 5.9.5.3.
CVE-2025-30998	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Rico Macchi WP Links Page allows SQL Injection. This issue a Links Page: from n/a through 4.9.6.
CVE-2025-39510	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ValvePress Pinterest Automatic Pin allows SQL Injection. This affects Pinterest Automatic Pin: from n/a through n/a.
CVE-2025-49267	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Shabti Kaplan Frontend Admin by DynamiApps allows Blind S Injection. This issue affects Frontend Admin by DynamiApps: from n/a through 3.28.3.
CVE-2025-4046	A missing authorization vulnerability in Lexmark Cloud Services badge management allows attacker to reassign badges within their organization
CVE-2025-52823	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ovatheme Cube Portfolio allows SQL Injection. This issue affe Portfolio: from n/a through 1.16.8.
CVE-2025-32992	Thermo Fisher Scientific ePort through 3.0.0 has Incorrect Access Control.
CVE-	

2025-49897	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in gopiplus Vertical scroll slideshow gallery v2 allows Blind SQL This issue affects Vertical scroll slideshow gallery v2: from n/a through 9.1.
CVE-2025-55708	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ExpressTech Systems Quiz And Survey Master allows SQL In This issue affects Quiz And Survey Master: from n/a through 10.2.4.
CVE-2025-31713	In engineer mode service, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with no additional privileges needed.
CVE-2025-8450	Improper Access Control issue in the Workflow component of Fortra's FileCatalyst allows unauthenticated users to upload arbitrary files via the order forms page.
CVE-2025-4044	Improper Restriction of XML External Entity Reference in various Lexmark printer drivers for Windows allows attacker to disclose sensitive information to an arbitra
CVE-2025-52797	Cross-Site Request Forgery (CSRF) vulnerability in josepsitjar StoryMap allows SQL Injection. This issue affects StoryMap: from n/a through 2.1.
CVE-2025-8342	The WooCommerce OTP Login With Phone Number, OTP Verification plugin for WordPress is vulnerable to authentication bypass due to insufficient empty value ch the lwp_ajax_register function in all versions up to, and including, 1.8.47. This makes it possible for unauthenticated attackers to bypass OTP verification and gain administrative access to any user account with a configured phone number by exploiting improper Firebase API error handling when the Firebase API key is not cor
CVE-2025-54689	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in thembay Urna allows PHP Local File Inclus issue affects Urna: from n/a through 2.5.7.
CVE-2025-30635	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeAtelier IDonatePro allows PHP Loca Inclusion. This issue affects IDonatePro: from n/a through 2.1.9.
CVE-2025-49036	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in octagonwebstudio Premium Addons for KingComposer allows PHP Local File Inclusion. This issue affects Premium Addons for KingComposer: from n/a through 1.1.1.
CVE-2025-54690	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in themeStek Xinterio allows PHP Local File I This issue affects Xinterio: from n/a through 4.2.
CVE-2025-28979	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThimPress WP Pipes allows PHP Local File This issue affects WP Pipes: from n/a through 1.4.3.
CVE-2025-54700	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove Makeaholic allows PHP Local Inclusion. This issue affects Makeaholic: from n/a through 1.8.4.
CVE-2025-54701	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove Unicamp allows PHP Local Fil Inclusion. This issue affects Unicamp: from n/a through 2.6.3.
CVE-2025-25172	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in beeteam368 VidMov allows PHP Local File This issue affects VidMov: from n/a through 1.9.4.
CVE-2025-48860	A vulnerability in the web application of the ctrlX OS setup mechanism facilitated an authenticated (low privileged) attacker to gain remote access to backup archiv created by a user with elevated permissions. Depending on the content of the backup archive, the attacker may have been able to access sensitive data.
CVE-2025-8875	Deserialization of Untrusted Data vulnerability in N-able N-central allows Local Execution of Code.This issue affects N-central: before 2025.3.1.
CVE-2025-52584	In Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share versions prior to 12.6.1204.204, the affected applications lack proper validation of user-supplied parsing XE files. This could lead to a heap-based buffer overflow. An attacker could leverage this vulnerability to execute arbitrary code in the context of the currer
CVE-2025-46269	In Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share versions prior to 12.6.1204.204, the affected applications lack proper validation of user-supplied parsing VC6 files. This could lead to a heap-based buffer overflow. An attacker could leverage this vulnerability to execute arbitrary code in the context of the curre process.
CVE-2025-53705	In Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share versions prior to 12.6.1204.204, the affected applications lack proper validation of user-supplied parsing CO files. This could lead to an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current proc
CVE-2025-23298	NVIDIA Merlin Transformers4Rec for all platforms contains a vulnerability in a python dependency, where an attacker could cause a code injection issue. A successf of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.
CVE-2025-23304	NVIDIA NeMo library for all platforms contains a vulnerability in the model loading component, where an attacker could cause code injection by loading .nemo files maliciously crafted metadata. A successful exploit of this vulnerability may lead to remote code execution and data tampering.
CVE-	NVIDIA Apex for all platforms contains a vulnerability in a Python component where an attacker could cause a code injection issue by providing a malicious file. A s

2025-23295	exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.
CVE-2025-8098	An improper permission vulnerability was reported in Lenovo PC Manager that could allow a local attacker to escalate privileges.
CVE-2025-41392	In Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share versions prior to 12.6.1204.204, the affected applications lack proper validation of user-supplied parsing AR files. This could lead to an out-of-bounds read. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current proce
CVE-2025-5047	A maliciously crafted DGN file, when parsed through Autodesk AutoCAD, can force an Uninitialized Variable vulnerability. A malicious actor can leverage this vulner cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
CVE-2025-23306	NVIDIA Megatron-LM for all platforms contains a vulnerability in the megatron/training/ arguments.py component where an attacker could cause a code injection is providing a malicious input. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, information disclosure, and data tamperir
CVE-2025-5048	A maliciously crafted DGN file, when linked or imported into Autodesk AutoCAD, can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.
CVE-2025-23305	NVIDIA Megatron-LM for all platforms contains a vulnerability in the tools component, where an attacker may exploit a code injection issue. A successful exploit of t vulnerability may lead to code execution, escalation of privileges, information disclosure, and data tampering.
CVE-2025-23303	NVIDIA NeMo Framework for all platforms contains a vulnerability where a user could cause a deserialization of untrusted data by remote code execution. A succes exploit of this vulnerability might lead to code execution and data tampering.
CVE-2025-23296	NVIDIA Isaac-GR00T for all platforms contains a vulnerability in a Python component where an attacker could cause a code injection issue. A successful exploit of th vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.
CVE-2025-8941	A flaw was found in linux-pam. The pam_namespace module may improperly handle user-controlled paths, allowing local users to exploit symlink attacks and race to elevate their privileges to root. This CVE provides a "complete" fix for CVE-2025-6020.
CVE-2025-23294	NVIDIA WebDataset for all platforms contains a vulnerability where an attacker could execute arbitrary code with elevated permissions. A successful exploit of this vulnerability might lead to escalation of privileges, data tampering, information disclosure, and denial of service.
CVE-2025-5046	A maliciously crafted DGN file, when linked or imported into Autodesk AutoCAD, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
CVE-2025-20244	A vulnerability in the Remote Access SSL VPN service for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defens Software could allow a remote attacker that is authenticated as a VPN user to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condit vulnerability is due to incomplete error checking when parsing an HTTP header field value. An attacker could exploit this vulnerability by sending a crafted HTTP re targeted Remote Access SSL VPN service on an affected device. A successful exploit could allow the attacker to cause a DoS condition, which would cause the affe device to reload.
CVE-2025-20127	A vulnerability in the TLS 1.3 implementation for a specific cipher for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Th Defense (FTD) Software for Cisco Firepower 3100 and 4200 Series devices could allow an authenticated, remote attacker to consume resources that are associatec incoming TLS 1.3 connections, which eventually could cause the device to stop accepting any new SSL/TLS or VPN requests. This vulnerability is due to the implem of the TLS 1.3 Cipher TLS_CHACHA20_POLY1305_SHA256. An attacker could exploit this vulnerability by sending a large number of TLS 1.3 connections with the sp 1.3 Cipher TLS_CHACHA20_POLY1305_SHA256. A successful exploit could allow the attacker to cause a denial of service (DoS) condition where no new incoming er connections are accepted. The device must be reloaded to clear this condition. Note: These incoming TLS 1.3 connections include both data traffic and user-manag traffic. After the device is in the vulnerable state, no new encrypted connections can be accepted.
CVE-2025-8092	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal COOKiES Consent Management allows Cross-Site Script (XSS).This issue affects COOKiES Consent Management: from 0.0.0 before 1.2.16.
CVE-2025-8361	Missing Authorization vulnerability in Drupal Config Pages allows Forceful Browsing.This issue affects Config Pages: from 0.0.0 before 2.18.0.
CVE-2025-55004	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to version 7.1.2-1, ImageMagick is vulnerable to heap-buffer read around the handling of images with separate alpha channels when performing image magnification in ReadOneMNGIMage. This can likely be used to leak sub memory contents into the output image. This issue has been patched in version 7.1.2-1.
CVE-2025-55197	pypdf is a free and open-source pure-python PDF library. Prior to version 6.0.0, an attacker can craft a PDF which leads to the RAM being exhausted. This requires j reading the file if a series of FlateDecode filters is used on a malicious cross-reference stream. Other content streams are affected on explicit access. This issue has fixed in 6.0.0. If an update is not possible, a workaround involves including the fixed code from pypdf.filters.decompress into the existing filters file.
CVE-2023-43692	An issue was discovered in Malwarebytes before 4.6.14.326 and before 5.1.5.116 (and Nebula 2020-10-21 and later). Out-of-bound reads in strings detection utiliti system crashes.
CVE-2025-30639	Missing Authorization vulnerability in ThemeAtelier IDonatePro allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects IDonatePr n/a through 2.1.9.
CVE-2025-49271	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in GravityWP GravityWP - Merge Tags allows File Inclusion. This issue affects GravityWP - Merge Tags: from n/a through 1.4.4.

CVE-2025-7342	A security issue was discovered in the Kubernetes Image Builder where default credentials are enabled during the Windows image build process when using the Nu VMware OVA providers. These credentials, which allow root access, are disabled at the conclusion of the build. Kubernetes clusters are only affected if their nodes images created via the Image Builder project and the vulnerability was exploited during the build process, which requires an attacker to access the build VM and m image while the build is in progress.
CVE-2025-52806	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in eyecix JobSearch allows PHP Local File Inc This issue affects JobSearch: from n/a through 2.9.0.
CVE-2025-52731	Missing Authorization vulnerability in themefunction WordPress Event Manager, Event Calendar and Booking Plugin allows Exploiting Incorrectly Configured Access Security Levels. This issue affects WordPress Event Manager, Event Calendar and Booking Plugin: from n/a through 4.0.24.
CVE-2025-31425	Missing Authorization vulnerability in kamleshyadav WP Lead Capturing Pages allows Exploiting Incorrectly Configured Access Control Security Levels. This issue af Lead Capturing Pages: from n/a through 2.3.
CVE-2025-32288	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in stmcan RT-Theme 18 | Extensions allows I File Inclusion. This issue affects RT-Theme 18 | Extensions: from n/a through 2.4.
CVE-2025-55586	TOTOLINK A3002R v4.0.0-B20230531.1404 was discovered to contain a buffer overflow in the url parameter at /boafrm/formFilter. This vulnerability allows attacke cause a Denial of Service (DoS) via a crafted input.
CVE-2025-24766	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in WP Royal Themes News Magazine X allow Local File Inclusion. This issue affects News Magazine X: from n/a through 1.2.37.
CVE-2025-52728	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in WebCodingPlace Responsive Posts Carous WordPress Plugin allows PHP Local File Inclusion. This issue affects Responsive Posts Carousel WordPress Plugin: from n/a through 15.0.
CVE-2025-54679	Missing Authorization vulnerability in vertim Neon Channel Product Customizer Free allows Exploiting Incorrectly Configured Access Control Security Levels. This iss Neon Channel Product Customizer Free: from n/a through 2.0.
CVE-2025-54692	Missing Authorization vulnerability in WP Swings Membership For WooCommerce allows Accessing Functionality Not Properly Constrained by ACLs. This issue affect Membership For WooCommerce: from n/a through 2.9.0.
CVE-2025-54472	Unlimited memory allocation in redis protocol parser in Apache bRPC (all versions < 1.14.1) on all platforms allows attackers to crash the service via network. Root the bRPC Redis protocol parser code, memory for arrays or strings of corresponding sizes is allocated based on the integers read from the network. If the integer re the network is too large, it may cause a bad alloc error and lead to the program crashing. Attackers can exploit this feature by sending special data packets to the service to carry out a denial-of-service attack on it. The bRPC 1.14.0 version tried to fix this issue by limited the memory allocation size, however, the limitation che code is not well implemented that may cause integer overflow and evade such limitation. So the 1.14.0 version is also vulnerable, although the integer range that version 1.14.0 is different from that affect version < 1.14.0. Affected scenarios: Using bRPC as a Redis server to provide network services to untrusted clients, or us as a Redis client to call untrusted Redis services. How to Fix: we provide two methods, you can choose one of them: 1. Upgrade bRPC to version 1.14.1. 2. Apply th https://github.com/apache/brpc/pull/3050) manually. No matter you choose which method, you should note that the patch limits the maximum length of memory a for each time in the bRPC Redis parser. The default limit is 64M. If some of you redis request or response have a size larger than 64M, you might encounter error af upgrade. For such case, you can modify the gflag redis_max_allocation_size to set a larger limit.
CVE-2025-3703	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in wipeoutmedia CSS & JavaScript Toolbox a Local File Inclusion. This issue affects CSS & JavaScript Toolbox: from n/a through n/a.
CVE-2025-52716	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Acato WP REST Cache allows PHP Local Fil Inclusion. This issue affects WP REST Cache: from n/a through 2025.1.0.
CVE-2025-55587	TOTOLINK A3002R v4.0.0-B20230531.1404 was discovered to contain a buffer overflow in the hostname parameter at /boafrm/formMapDelDevice. This vulnerabilit attackers to cause a Denial of Service (DoS) via a crafted input.
CVE-2025-33090	IBM Concert Software 1.0.0 through 1.1.0 could allow a remote attacker to cause a denial of service using a specially crafted regular expression that would cause e resource consumption.
CVE-2025-48332	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in PublishPress Gutenberg Blocks allows PHP Inclusion. This issue affects Gutenberg Blocks: from n/a through 3.3.1.
CVE-2025-6625	CWE-20: Improper Input Validation vulnerability exists that could cause a Denial Of Service when specific crafted FTP command is sent to the device.
CVE-2025-53948	The Sante PACS Server allows a remote attacker to crash the main thread by sending a crafted HL7 message, causing a denial-of-service condition. The application require a manual restart and no authentication is required.
CVE-2025-4276	UsbCoreDxe has a vulnerability which can be used to write arbitrary memory inside SMRAM and execute arbitrary code at SMM level.
CVE-2025-49264	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Cloud Infrastructure Services Cloud SAML Single Sign On Login allows PHP Local File Inclusion. This issue affects Cloud SAML SSO - Single Sign On Login: from n/a through 1.0.18.

CVE-2025-7670	The JS Archive List plugin for WordPress is vulnerable to time-based SQL Injection via the build_sql_where() function in all versions up to, and including, 6.1.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2024-12612	The School Management System for Wordpress plugin for WordPress is vulnerable to SQL Injection via several parameters across multiple AJAX action in all versions and including, 93.2.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2025-50614	A buffer overflow vulnerability has been discovered in the Netis WF2880 v2.1.40207 in the FUN_0047151c function of the cgitest.cgi file. Attackers can trigger this vulnerability by controlling the value of wds_set in the payload, which can cause the program to crash and potentially lead to a Denial of Service (DoS) attack.
CVE-2025-8959	HashiCorp's go-getter library subdirectory download feature is vulnerable to symlink attacks leading to unauthorized read access beyond the designated directory boundaries. This vulnerability, identified as CVE-2025-8959, is fixed in go-getter 1.7.9.
CVE-2025-50613	A buffer overflow vulnerability has been discovered in Netis WF2880 v2.1.40207 in the FUN_00475e1c function of the cgitest.cgi file. Attackers can trigger this vuln by controlling the value of wds_key_wep in the payload, which can cause the program to crash and potentially lead to a Denial of Service (DoS) attack.
CVE-2025-8671	A mismatch caused by client-triggered server-sent stream resets between HTTP/2 specifications and the internal architectures of some HTTP/2 implementations ma in excessive server resource consumption leading to denial-of-service (DoS). By opening streams and then rapidly triggering the server to reset them—using malfo frames or flow control errors—an attacker can exploit incorrect stream accounting. Streams reset by the server are considered closed at the protocol level, even th backend processing continues. This allows a client to cause the server to handle an unbounded number of concurrent streams on a single connection. This CVE will updated as affected product details are released.
CVE-2025-48989	Improper Resource Shutdown or Release vulnerability in Apache Tomcat made Tomcat vulnerable to the made you reset attack. This issue affects Apache Tomcat: 11.0.0-M1 through 11.0.9, from 10.1.0-M1 through 10.1.43 and from 9.0.0.M1 through 9.0.107. Older, EOL versions may also be affected. Users are recommended upgrade to one of versions 11.0.10, 10.1.44 or 9.0.108 which fix the issue.
CVE-2025-50612	A buffer overflow vulnerability has been discovered in the Netis WF2880 v2.1.40207 in the FUN_004743f8 function of the cgitest.cgi file. Attackers can trigger this vulnerability by controlling the value of wl_sec_set in the payload, which may cause the program to crash and potentially lead to a Denial of Service (DoS) attack.
CVE-2025-50611	A buffer overflow vulnerability has been discovered in Netis WF2880 v2.1.40207 in the FUN_00473154 function of the cgitest.cgi file. Attackers can trigger this vuln by controlling the value of wl_sec_set_5g and wl_sec_rp_set_5g in the payload, which can cause the program to crash and potentially lead to a Denial of Service (D
CVE-2025-50610	A buffer overflow vulnerability has been discovered in Netis WF2880 v2.1.40207 in the FUN_00476598 function of the cgitest.cgi file. Attackers can trigger this vuln by controlling the value of wl_base_set_5g in the payload, which can cause the program to crash and potentially lead to a Denial of Service (DoS) attack.
CVE-2025-50609	A buffer overflow vulnerability has been discovered in Netis WF2880 v2.1.40207 in the Function_00465620 of the cgitest.cgi file. Attackers can trigger this vulnerab controlling the value of specify_parame in the payload, which can cause the program to crash and potentially lead to a Denial of Service (DoS) attack.
CVE-2025-50608	A buffer overflow vulnerability has been discovered in Netis WF2880 v2.1.40207 in the FUN_00471994 function of the cgitest.cgi file. Attackers can trigger this vuln by controlling the value of wl_base_set in the payload, which can cause the program to crash and potentially lead to a Denial of Service (DoS) attack.
CVE-2025-8912	Organization Portal System developed by WellChoose has an Arbitrary File Reading vulnerability, allowing unauthenticated remote attackers to exploit Absolute Pa Traversal to download arbitrary system files.
CVE-2025-50615	A buffer overflow vulnerability has been discovered in Netis WF2880 v2.1.40207 in the FUN_00470c50 function of the cgitest.cgi file. Attackers can trigger this vuln by controlling the value of wl_mac_filter_set in the payload, which can cause the program to crash and lead to a Denial of Service (DoS) attack.
CVE-2025-50616	A buffer overflow vulnerability has been discovered in Netis WF2880 v2.1.40207 in the FUN_0046f984 function of the cgitest.cgi file. Attackers can trigger this vuln by controlling the value of wl_advanced_set in the payload, which can cause the program to crash and lead to a Denial of Service (DoS) attack.
CVE-2025-50617	A buffer overflow vulnerability has been discovered in Netis WF2880 v2.1.40207 in the FUN_0046ed68 function of the cgitest.cgi file. Attackers can trigger this vuln by controlling the value of wps_set in the payload, which can cause the program to crash and potentially lead to a Denial of Service (DoS) attack.
CVE-2025-8754	Missing Authentication for Critical Function vulnerability in ABB ABB AbilityTM zenon.This issue affects ABB AbilityTM zenon: from 7.50 through 14.
CVE-2025-7641	The Assistant for NextGEN Gallery plugin for WordPress is vulnerable to arbitrary directory deletion due to insufficient file path validation in the /wp-json/nextgenassistant/v1.0.0/control REST endpoint in all versions up to, and including, 1.0.9. This makes it possible for unauthenticated attackers to delete arbitra directories on the server, which can cause a complete loss of availability.
CVE-2025-4410	A buffer overflow vulnerability exists in the module SetupUtility. An attacker with local privileged access can exploit this vulnerability by executeing arbitrary code.
CVE-2025-46405	When Network Access is configured on a BIG-IP APM virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Sof versions which have reached End of Technical Support (EoTS) are not evaluated.
CVE-2025-50635	A null pointer dereference vulnerability was discovered in Netis WF2780 v2.2.35445. The vulnerability exists in the FUN_0048a728 function of the cgitest.cgi file. A can trigger this vulnerability by controlling the CONTENT_LENGTH variable, causing the program to crash and potentially leading to a denial-of-service (DoS) attack
CVE-2025-6025	The Order Tip for WooCommerce plugin for WordPress is vulnerable to Unauthenticated Improper Input Validation in all versions up to, and including, 1.5.4. This is lack of server-side validation on the `data-tip` attribute, which makes it possible for unauthenticated attackers to apply an excessive or even negative tip amount, in unauthorized discount up to free orders depending on the value submitted.

CVE-2025-8761	A vulnerability has been found in INSTAR 2K+ and 4K 3.11.1 Build 1124. This vulnerability affects unknown code of the component Backend IPC Server. The manipu leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-43988	KuWFi 5G01-X55 FL2020_V0.0.12 devices expose an unauthenticated API endpoint (ajax_get.cgi), allowing remote attackers to retrieve sensitive configuration data including admin credentials.
CVE-2025-7650	The BizCalendar Web plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.1.0.50 via the 'bizcalv' shortcode. This makes it for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be upload included.
CVE-2025-51986	An issue was discovered in the demo/LINUXTCP implementation of cwalter-at freemodbus v.2018-09-12 allowing attackers to reach an infinite loop via a crafted ler for a packet.
CVE-2025-52585	When a BIG-IP LTM Client SSL profile is configured on a virtual server with SSL Forward Proxy enabled and Anonymous Diffie-Hellman (ADH) ciphers enabled, undis requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not
CVE-2025-55588	TOTOLINK A3002R v4.0.0-B20230531.1404 was discovered to contain a buffer overflow in the fw_ip parameter at /boafrm/formPortFw. This vulnerability allows atta cause a Denial of Service (DoS) via a crafted input.
CVE-2025-7664	The AL Pack plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the check_activate_permission() permission callback fo json/presslearn/v1/activate REST API endpoint in all versions up to, and including, 1.0.2. The callback reads the client-supplied Origin header and, after parsing, allo request if it matches one of the trusted domains, without ever verifying user authentication, capabilities, or nonce tokens. This makes it possible for unauthenticate attackers to activate premium features by simply spoofing the Origin header.
CVE-2025-4277	Tcg2Smm has a vulnerability which can be used to write arbitrary memory inside SMRAM and execute arbitrary code at SMM level.
CVE-2025-54809	F5 Access for Android before version 3.1.2 which uses HTTPS does not verify the remote endpoint identity. Note: Software versions which have reached End of Tech Support (EoTS) are not evaluated.
CVE-2025-54156	The Sante PACS Server Web Portal sends credential information without encryption.
CVE-2025-9010	A vulnerability was found in itsourcecode Online Tour and Travel Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/booking_report.php. The manipulation of the argument from_date leads to sql injection. The attack can be launched remotely. The exploit has been disclose public and may be used.
CVE-2025-9009	A vulnerability has been found in itsourcecode Online Tour and Travel Management System 1.0. Affected is an unknown function of the file /admin/email_setup.php manipulation of the argument Name leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be use
CVE-2025-9051	A vulnerability was determined in projectworlds Travel Management System 1.0. Affected by this issue is some unknown functionality of the file /updatecategory.pl manipulation of the argument t1 leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-52801	Missing Authorization vulnerability in VonStroheim TheBooking allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects TheBooking: fro through 1.4.4.
CVE-2025-52800	Missing Authorization vulnerability in Unity Business Technology Pty Ltd The E-Commerce ERP allows Accessing Functionality Not Properly Constrained by ACLs. Thi affects The E-Commerce ERP: from n/a through 2.1.1.3.
CVE-2025-9011	A vulnerability was determined in PHPGurukul Online Shopping Portal Project 2.0. Affected by this issue is some unknown functionality of the file /shopping/signup.p manipulation of the argument emailid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-9012	A vulnerability was identified in PHPGurukul Online Shopping Portal Project 2.0. This affects an unknown part of the file shopping/bill-ship-addresses.php. The manip the argument billingpincode leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-9013	A vulnerability has been found in PHPGurukul Online Shopping Portal Project 2.0. This vulnerability affects unknown code of the file /shopping/password-recovery.p manipulation of the argument emailid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-9008	A vulnerability was identified in itsourcecode Online Tour and Travel Management System 1.0. This issue affects some unknown processing of the file /admin/sms_setting.php. The manipulation of the argument uname leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to th and may be used.
CVE-2025-9050	A vulnerability was found in projectworlds Travel Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /addcategory.php. T manipulation of the argument t1 leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-9047	A vulnerability has been found in projectworlds Visitor Management System 1.0. Affected is an unknown function of the file /visitor_out.php. The manipulation of th argument rid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-	A vulnerability was determined in SourceCodester Online Bank Management System up to 1.0. This vulnerability affects unknown code of the file /bank/transfer.ph

2025-9021	manipulation of the argument email leads to sql injection. The attack can be initiated remotely.
CVE-2025-9022	A vulnerability was identified in SourceCodester Online Bank Management System up to 1.0. This issue affects some unknown processing of the file /bank/statemer The manipulation of the argument email leads to sql injection. The attack may be initiated remotely.
CVE-2025-9028	A vulnerability was found in code-projects Online Medicine Guide 1.0. This issue affects some unknown processing of the file /adphar.php. The manipulation of the phuname leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-9024	A vulnerability was found in PHPGurukul Beauty Parlour Management System 1.1. Affected by this vulnerability is an unknown functionality of the file /book-appointment.php. The manipulation of the argument Message leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the pu may be used.
CVE-2025-9026	A vulnerability was identified in D-Link DIR-860L 2.04.B04. This affects the function ssdpcgi_main of the file htdocs/cgibin of the component Simple Service Discove Protocol. The manipulation leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be use vulnerability only affects products that are no longer supported by the maintainer.
CVE-2025-9052	A vulnerability was identified in projectworlds Travel Management System 1.0. This affects an unknown part of the file /updatepackage.php. The manipulation of th argument s1 leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8957	A vulnerability was determined in Campcodes Online Flight Booking Management System 1.0. Affected is an unknown function of the file /flights.php. The manipula the argument departure_airport_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-9053	A vulnerability has been found in projectworlds Travel Management System 1.0. This vulnerability affects unknown code of the file /updatesubcategory.php. The manipulation of the argument t1/s1 leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8983	A vulnerability was identified in itsourcecode Online Tour and Travel Management System 1.0. This issue affects some unknown processing of the file /admin/operations/expense.php. The manipulation of the argument expense_for leads to sql injection. The attack may be initiated remotely. The exploit has been d to the public and may be used.
CVE-2025-55195	@std/toml is the Deno Standard Library. Prior to version 1.0.9, an attacker can pollute the prototype chain in Node.js runtime and Browser when parsing untrusted data, thus achieving Prototype Pollution (PP) vulnerability. This is because the library is merging an untrusted object with an empty object, which by default the em has the prototype chain. This issue has been patched in version 1.0.9.
CVE-2025-8968	A vulnerability was identified in itsourcecode Online Tour and Travel Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/disapprove_user.php. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to th and may be used.
CVE-2025-8969	A vulnerability has been found in itsourcecode Online Tour and Travel Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/approve_user.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the and may be used.
CVE-2025-8967	A vulnerability was determined in itsourcecode Online Tour and Travel Management System 1.0. Affected is an unknown function of the file /admin/operations/pack The manipulation of the argument pname leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may b
CVE-2025-8966	A vulnerability was found in itsourcecode Online Tour and Travel Management System 1.0. This issue affects some unknown processing of the file /admin/operation The manipulation of the argument tname leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used
CVE-2025-8970	A vulnerability was found in itsourcecode Online Tour and Travel Management System 1.0. This affects an unknown part of the file /admin/operations/booking.php. manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8971	A vulnerability was determined in itsourcecode Online Tour and Travel Management System 1.0. This vulnerability affects unknown code of the file /admin/operations/travellers.php. The manipulation of the argument val-username leads to sql injection. The attack can be initiated remotely. The exploit has been to the public and may be used.
CVE-2025-8972	A vulnerability was identified in itsourcecode Online Tour and Travel Management System 1.0. This issue affects some unknown processing of the file /admin/page- The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8981	A vulnerability was found in itsourcecode Online Tour and Travel Management System 1.0. This affects an unknown part of the file /admin/operations/payment.php manipulation of the argument payment_type leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and ma used.
CVE-2025-8982	A vulnerability was determined in itsourcecode Online Tour and Travel Management System 1.0. This vulnerability affects unknown code of the file /admin/operations/currency.php. The manipulation of the argument curr_code leads to sql injection. The attack can be initiated remotely. The exploit has been disc the public and may be used.
CVE-2025-5296	CWE-59: Improper Link Resolution Before File Access ('Link Following') vulnerability exists that could cause arbitrary data to be written to protected locations, pote leading to escalation of privilege, arbitrary file corruption, exposure of application and system information or persistent denial of service when a low-privileged atta tampers with the installation folder.
CVE-2025-9002	A vulnerability was identified in Surbowl dormitory-management-php 1.0. This affects an unknown part of the file login.php. The manipulation of the argument Acc to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products t longer supported by the maintainer.
CVE-2025-8984	A vulnerability has been found in itsourcecode Online Tour and Travel Management System 1.0. Affected is an unknown function of the file /admin/operations/expense_category.php. The manipulation of the argument expense_name leads to sql injection. It is possible to launch the attack remotely. The has been disclosed to the public and may be used.
CVE-2025-	A vulnerability was found in SourceCodester COVID 19 Testing Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /profile manipulation of the argument mobilenumber leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be

8985	Other parameters might be affected as well.
CVE-2025-8986	A vulnerability was determined in SourceCodester COVID 19 Testing Management System 1.0. Affected by this issue is some unknown functionality of the file /sear result.php. The manipulation of the argument serachdata leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public be used.
CVE-2025-8987	A vulnerability was identified in SourceCodester COVID 19 Testing Management System 1.0. This affects an unknown part of the file /test-details.php. The manipula the argument remark leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8988	A vulnerability has been found in SourceCodester COVID 19 Testing Management System 1.0. This vulnerability affects unknown code of the file /bwdates-report-re The manipulation of the argument fromdate leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be us
CVE-2025-8989	A vulnerability was found in SourceCodester COVID 19 Testing Management System 1.0. This issue affects some unknown processing of the file /edit-phlebotomist. manipulation of the argument mobilenumber leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be Other parameters might be affected as well.
CVE-2025-8990	A vulnerability was determined in code-projects Online Medicine Guide 1.0. Affected is an unknown function of the file /browsemdcn.php. The manipulation of the a Search leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8993	A vulnerability was found in itsourcecode Online Tour and Travel Management System 1.0. This affects an unknown part of the file /admin/expense_report.php. The manipulation of the argument from_date leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be
CVE-2025-8960	A vulnerability has been found in Campcodes Online Flight Booking Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/save_airlines.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the may be used.
CVE-2025-8105	The The Soledad theme for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 8.6.7. This is due to the software allowing execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary sh
CVE-2025-8973	A vulnerability has been found in SourceCodester Cashier Queuing System 1.0. Affected is an unknown function of the file /Actions.php. The manipulation of the arg Username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-9027	A vulnerability has been found in code-projects Online Medicine Guide 1.0. This vulnerability affects unknown code of the file /addelivery.php. The manipulation of argument deName leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-48500	A missing file integrity check vulnerability exists on MacOS F5 VPN browser client installer that may allow a local, authenticated attacker with access to the local fil to replace it with a malicious package installer. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.
CVE-2025-8924	A vulnerability was identified in Campcodes Online Water Billing System 1.0. This issue affects some unknown processing of the file /viewbill.php. The manipulation argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8926	A vulnerability was found in SourceCodester COVID 19 Testing Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /login. manipulation of the argument Username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used
CVE-2025-9150	A vulnerability was identified in Surbowl dormitory-management-php up to 9f1d9d1f528cabffc66fda3652c56ff327fda317. Affected is an unknown function of the fil /admin/violation_add.php?id=2. Such manipulation of the argument ID leads to sql injection. The attack may be performed from a remote location. The exploit is pu available and might be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated release disclosed. This vulnerability only affects products that are no longer supported by the maintainer.
CVE-2025-8921	A vulnerability has been found in code-projects Job Diary 1.0. Affected by this issue is some unknown functionality of the file /user-apply.php. The manipulation of t argument job_title leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8955	A vulnerability has been found in PHPGurukul Hospital Management System 4.0. This vulnerability affects unknown code of the file /admin/edit-doctor.php. The ma of the argument docfees leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8954	A vulnerability was identified in PHPGurukul Hospital Management System 4.0. This affects an unknown part of the file /admin/doctor-specilization.php. The manipu the argument doctorspecilization leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8953	A vulnerability was determined in SourceCodester COVID 19 Testing Management System 1.0. Affected by this issue is some unknown functionality of the file /check_availability.php. The manipulation of the argument employeeid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed public and may be used.
CVE-2025-8952	A vulnerability was found in Campcodes Online Flight Booking Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin action=login of the component Login. The manipulation of the argument Username leads to sql injection. The attack can be launched remotely. The exploit has bee disclosed to the public and may be used.
CVE-2025-9154	A flaw has been found in itsourcecode Online Tour and Travel Management System 1.0. This issue affects some unknown processing of the file /user/page-login.php manipulation of the argument email causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.
CVE-2025-8951	A vulnerability has been found in PHPGurukul Teachers Record Management System 2.1. Affected is an unknown function of the file /admin/search.php. The manipu the argument searchdata leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-	A vulnerability was identified in Campcodes Online Recruitment Management System 1.0. This issue affects some unknown processing of the file /Recruitment/inde

2025-8950	page=view_vacancy. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public be used.
CVE-2025-8948	A vulnerability was determined in projectworlds Visitor Management System 1.0. Affected is an unknown function of the file /front.php. The manipulation of the arg leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8947	A vulnerability was found in projectworlds Visitor Management System 1.0. This issue affects some unknown processing of the file /query_data.php. The manipulati argument dateF/dateP leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8946	A vulnerability has been found in projectworlds Online Notes Sharing Platform 1.0. This vulnerability affects unknown code of the file /login.php. The manipulation c argument User leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-9156	A vulnerability was found in itsourcecode Sports Management System 1.0. The affected element is an unknown function of the file /Admin/sports.php. Performing manipulation of the argument code results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.
CVE-2025-9155	A vulnerability has been found in itsourcecode Online Tour and Travel Management System 1.0. Impacted is an unknown function of the file /user/forget_password. manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8932	A vulnerability was determined in 1000 Projects Sales Management System 1.0. This vulnerability affects unknown code of the file /superstore/admin/sales.php. Th manipulation of the argument ssalescat leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8935	A vulnerability was found in 1000 Projects Sales Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /superstore/custcmp. manipulation of the argument Username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used
CVE-2025-8925	A vulnerability has been found in itsourcecode Sports Management System 1.0. Affected is an unknown function of the file /Admin/match.php. The manipulation of argument code leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8936	A vulnerability was determined in 1000 Projects Sales Management System 1.0. Affected by this issue is some unknown functionality of the file /superstore/dist/dordupdate.php. The manipulation of the argument select2 leads to sql injection. The attack may be launched remotely. The exploit has been discl the public and may be used.
CVE-2025-8922	A vulnerability was found in code-projects Job Diary 1.0. This affects an unknown part of the file /admin-inbox.php. The manipulation of the argument ID leads to sq injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8923	A vulnerability was determined in code-projects Job Diary 1.0. This vulnerability affects unknown code of the file /edit-details.php. The manipulation of the argumer to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-54697	Incorrect Privilege Assignment vulnerability in Ben Ritner - Kadence WP Kadence WooCommerce Email Designer allows Privilege Escalation. This issue affects Kade WooCommerce Email Designer: from n/a through 1.5.16.
CVE-2025-47536	Deserialization of Untrusted Data vulnerability in keywordrush Content Egg allows Object Injection. This issue affects Content Egg: from n/a through 7.0.0.
CVE-2025-8949	A vulnerability was identified in D-Link DIR-825 2.10. Affected by this vulnerability is the function get_ping_app_stat of the file ping_response.cgi of the component manipulation of the argument ping_ipaddr leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public be used. This vulnerability only affects products that are no longer supported by the maintainer.
CVE-2025-1929	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Risk Yazılım Teknolojileri Ltd. Şti. Reel Sektör Hazine ve Risk Yazılımı allows SQL Injection, CAPEC - 7 - Blind SQL Injection.This issue affects Reel Sektör Hazine ve Risk Yönetimi Yazılımı: through 1.0.0.4.
CVE-2025-54421	NamelessMC is a free, easy to use & powerful website software for Minecraft servers. Cross-site scripting (XSS) vulnerability in NamelessMC before 2.2.4 allows ren authenticated attackers to inject arbitrary web script or HTML via the default_keywords crafted parameter. This vulnerability is fixed in 2.2.4.
CVE-2025-24975	Firebird is a relational database. Prior to snapshot versions 4.0.6.3183, 5.0.2.1610, and 6.0.0.609, Firebird is vulnerable if ExtConnPoolSize is not set equal to 0. If connections stored in ExtConnPool are not verified for presence and suitability of the CryptCallback interface is used when created versus what is available could re segfault in the server process. Encrypted databases, accessed by execute statement on external, may be accessed later by an attachment missing a key to that da a case when execute statement are chained, segfault may happen. Additionally, the segfault may affect unencrypted databases. This issue has been patched in sn versions 4.0.6.3183, 5.0.2.1610, and 6.0.0.609 and point releases 4.0.6 and 5.0.2. A workaround for this issue involves setting ExtConnPoolSize equal to 0 in firebir
CVE-2025-49038	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Soflyy WP Dynamic Links allows Reflected XSS. This issue affec Dynamic Links: from n/a through 1.0.1.
CVE-2025-49044	Cross-Site Request Forgery (CSRF) vulnerability in tosend.it Simple Poll allows Stored XSS. This issue affects Simple Poll: from n/a through 1.1.1.
CVE-2025-49065	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BestiaDurmiente Visit Counter allows Stored XSS. This issue af Counter: from n/a through 1.0.
CVE-2025-55291	Shaarli is a minimalist bookmark manager and link sharing service. Prior to 0.15.0, the input string in the cloud tag page is not properly sanitized. This allows the < to be prematurely closed, leading to a reflected Cross-Site Scripting (XSS) vulnerability. This vulnerability is fixed in 0.15.0.

CVE-2025-49064	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Webilop User Language Switch allows Reflected XSS. This issue User Language Switch: from n/a through 1.6.10.
CVE-2025-49056	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in shen2 多说社会化评论框 allows Reflected XSS. This issue affects 评论框: from n/a through 1.2.
CVE-2025-49037	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Federico Rota Authentication and xmlrpc log writer allows Refl This issue affects Authentication and xmlrpc log writer: from n/a through 1.2.2.
CVE-2025-52765	Cross-Site Request Forgery (CSRF) vulnerability in lisensee NetInsight Analytics Implementation Plugin allows Stored XSS. This issue affects NetInsight Analytics Implementation Plugin: from n/a through 1.0.3.
CVE-2025-48862	Ambiguous wording in the web interface of the ctrlX OS setup mechanism could lead the user to believe that the backup file is encrypted when a password is set. H only the private key - if available in the backup - is encrypted, while the backup file itself remains unencrypted.
CVE-2025-49057	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ko Min WP Voting allows Reflected XSS. This issue affects WP V from n/a through 1.8.
CVE-2025-49063	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in i3geek BaiduXZH Submit(百度熊掌号) allows Reflected XSS. This affects BaiduXZH Submit(百度熊掌号): from n/a through 1.4.6.
CVE-2025-49062	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cornfeed WP-jScrollPane allows Reflected XSS. This issue affect jScrollPane: from n/a through 2.0.3.
CVE-2025-53575	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in primersoftware Primer MyData for Woocommerce allows Reflec This issue affects Primer MyData for Woocommerce: from n/a through 4.2.5.
CVE-2025-49054	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mrdenny Time Sheets allows Reflected XSS. This issue affects Sheets: from n/a through 2.1.3.
CVE-2025-29014	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ZoomIt FoodMenu allows Reflected XSS. This issue affects Food from n/a through 1.20.
CVE-2025-28975	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in redqteam Alike - WordPress Custom Post Comparison allows Re XSS. This issue affects Alike - WordPress Custom Post Comparison: from n/a through 3.0.1.
CVE-2025-47689	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in johnh10 Video Blogster Lite allows Reflected XSS. This issue af Video Blogster Lite: from n/a through 1.2.
CVE-2025-31007	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alvind Billplz Addon for Contact Form 7 allows Reflected XSS. T affects Billplz Addon for Contact Form 7: from n/a through 1.2.0.
CVE-2025-52775	Missing Authorization vulnerability in Ronik@UnlimitedWP Project Cost Calculator allows Exploiting Incorrectly Configured Access Control Security Levels. This issue Project Cost Calculator: from n/a through 1.0.0.
CVE-2025-52785	Missing Authorization vulnerability in softnwords SMM API allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects SMM API: from through 6.0.30.
CVE-2025-52788	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Russell Jamieson CaptionPix allows Reflected XSS. This issue af CaptionPix: from n/a through 1.8.
CVE-2025-30626	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Multimedia Playlist Slider Addon for WPBakery P Builder allows Reflected XSS. This issue affects Multimedia Playlist Slider Addon for WPBakery Page Builder: from n/a through 2.1.
CVE-2025-28999	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ZoomIt WooCommerce Shop Page Builder allows Reflected XSS issue affects WooCommerce Shop Page Builder: from n/a through 2.27.7.
CVE-2025-49058	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sound Strategies SoundSt SEO Search allows Reflected XSS. Th affects SoundSt SEO Search: from n/a through 1.2.3.
CVE-2025-54867	Youki is a container runtime written in Rust. Prior to version 0.5.5, if /proc and /sys in the rootfs are symbolic links, they can potentially be exploited to gain access host root filesystem. This issue has been patched in version 0.5.5.
CVE-2025-9000	A vulnerability was found in Mechrevo Control Center GX V2 5.56.51.48. Affected by this vulnerability is an unknown functionality of the component reg File Handle manipulation leads to uncontrolled search path. It is possible to launch the attack on the local host. The complexity of an attack is rather high. The exploitation app difficult. The exploit has been disclosed to the public and may be used.

CVE-2025-9016	A vulnerability was identified in Mechrevo Control Center GX V2 5.56.51.48. This affects an unknown part of the file C:\Program Files\OEM\机械革命控制中心\AiStoneService\MyControlCenter\Command of the component Powershell Script Handler. The manipulation leads to uncontrolled search path. Local access is requi approach this attack. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be us
CVE-2025-8907	A vulnerability was found in H3C M2 NAS V100R006. Affected by this vulnerability is an unknown functionality of the component Webserver Configuration. The mar leads to execution with unnecessary privileges. An attack has to be approached locally. The complexity of an attack is rather high. The exploitation appears to be d The exploit has been disclosed to the public and may be used. The vendor explains: "[T]he device only has configuration files and does not actually have boa funct is impossible to access or upload files anonymously to the device through boa services". This vulnerability only affects products that are no longer supported by th maintainer.
CVE-2025-4371	A potential vulnerability was reported in the Lenovo 510 FHD and Performance FHD web cameras that could allow an attacker with physical access to write arbitrar firmware updates to the device over a USB connection.
CVE-2025-31714	In Developer Tools, there is a possible missing verification incorrect input. This could lead to local escalation of privilege with no additional execution privileges nee
CVE-2025-8762	A vulnerability was found in INSTAR 2K+ and 4K 3.11.1 Build 1124. This issue affects some unknown processing of the component UART Interface. The manipulatio improper physical access control. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used.
CVE-2025-21110	Dell Data Lakehouse, versions prior to 1.5.0.0, contains an Execution with Unnecessary Privileges vulnerability. A high privileged attacker with local access could p exploit this vulnerability, leading to Denial of service.
CVE-2025-38738	SupportAssist for Home PCs Installer exe version(s) 4.8.2.29006 and prior, contain(s) an Incorrect Privilege Assignment vulnerability in the Installer. A low privilege with local access could potentially exploit this vulnerability, leading to elevation of privileges.
CVE-2024-12303	An issue has been discovered in GitLab CE/EE affecting all versions from 17.7 before 18.0.6, 18.1 before 18.1.4, and 18.2 before 18.2.2 that under certain condition have allowed authenticated users with specific roles and permissions to delete issues including confidential ones by inviting users with a specific role.
CVE-2025-36612	SupportAssist for Business PCs, version(s) 4.5.3 and prior, contain(s) an Incorrect Privilege Assignment vulnerability. A low privileged attacker with local access cou potentially exploit this vulnerability, leading to elevation of privileges.
CVE-2025-8980	A vulnerability has been found in Tenda G1 16.01.7.8(3660). Affected by this issue is the function check_upload_file of the component Firmware Update Handler. Th manipulation leads to insufficient verification of data authenticity. The attack may be launched remotely. The complexity of an attack is rather high. The exploitatio known to be difficult. The exploit has been disclosed to the public and may be used.
CVE-2025-9146	A flaw has been found in Linksys E5600 1.1.0.26. The affected element is the function verify_gemtek_header of the file checkFw.sh of the component Firmware Har Executing manipulation can lead to risky cryptographic algorithm. The attack may be launched remotely. The attack requires a high level of complexity. The exploi described as difficult. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-8979	A vulnerability was identified in Tenda AC15 15.13.07.13. Affected by this vulnerability is the function check_fw_type/split_fireware/check_fw of the component Firm Update Handler. The manipulation leads to insufficient verification of data authenticity. The attack can be launched remotely. The complexity of an attack is rather exploitation appears to be difficult. The exploit has been disclosed to the public and may be used.
CVE-2025-8978	A vulnerability was determined in D-Link DIR-619L 6.02CN02. Affected is the function FirmwareUpgrade of the component boa. The manipulation leads to insufficie verification of data authenticity. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.
CVE-2024-8393	The Woocommerce Blocks – Woolook plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.7.0 via the via the 'tab' parame makes it possible for authenticated attackers, with Administrator-level access and above, to include and execute arbitrary files on the server, allowing the executio PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file ty be uploaded and included. Please note that this can also be exploited via CSRF techniques.
CVE-2025-55199	Helm is a package manager for Charts for Kubernetes. Prior to version 3.18.5, it is possible to craft a JSON Schema file in a manner which could cause Helm to use available memory and have an out of memory (OOM) termination. This issue has been resolved in Helm 3.18.5. A workaround involves ensuring all Helm charts tha being loaded into Helm do not have any reference of $ref pointing to /dev/zero.
CVE-2025-54746	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cartpauj Shortcode Redirect allows Stored XSS. This issue affec Shortcode Redirect: from n/a through 1.0.02.
CVE-2025-8878	The The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress plugin for WordPress is vulnerable arbitrary shortcode execution in all versions up to, and including, 4.16.4. This is due to the software allowing users to execute an action that does not properly vali value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.
CVE-2025-55198	Helm is a package manager for Charts for Kubernetes. Prior to version 3.18.5, when parsing Chart.yaml and index.yaml files, an improper validation of type error c a panic. This issue has been resolved in Helm 3.18.5. A workaround involves ensuring YAML files are formatted as Helm expects prior to processing them with Helm
CVE-2025-8770	An issue has been discovered in GitLab EE affecting all versions from 18.0 prior to 18.0.6, 18.1 prior to 18.1.4, and 18.2 prior to 18.2.2 that could have allowed aut users with specific access to bypass merge request approval policies by manipulating approval rule identifiers.
CVE-2025-54740	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michael Nelson Print My Blog allows Stored XSS. This issue affe My Blog: from n/a through 3.27.9.
CVE-2025-43989	The /goform/formJsonAjaxReq POST endpoint of Shenzhen Tuoshi NR500-EA RG500UEAABxCOMSLICv3.4.2731.16.43 devices mishandles the set_timesetting action ntpserver0 parameter, which is used in a system command. By setting a username=admin cookie (bypassing normal session checks), an unauthenticated attacker that parameter to execute arbitrary OS commands.
CVE-	

2023-43687	An issue was discovered in Malwarebytes before 4.6.14.326 and before 5.1.5.116 (and Nebula 2020-10-21 and later). There is a Race condition that leads to code e because of a lack of locks between file verification and execution.
CVE-2025-2614	An issue has been discovered in GitLab CE/EE affecting all versions from 11.6 before 18.0.6, 18.1 before 18.1.4, and 18.2 before 18.2.2 that could have allowed an authenticated user to cause a denial of service condition by creating specially crafted content that consumes excessive server resources when processed.
CVE-2025-52337	An authenticated arbitrary file upload vulnerability in the Content Explorer feature of LogicData eCommerce Framework v5.0.9.7000 allows attackers to execute ar code via uploading a crafted file.
CVE-2024-37945	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBits WPBITS Addons For Elementor Page Builder allows Stor XSS.This issue affects WPBITS Addons For Elementor Page Builder: from n/a through 1.5.
CVE-2025-53330	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WpEstate WP Rentals allows Stored XSS. This issue affects WP from n/a through 3.13.1.
CVE-2025-55295	qBit Manage is a tool that helps manage tedious tasks in qBittorrent and automate them. A path traversal vulnerability exists in qbit_manage's web API that allows authenticated users to read arbitrary files from the server filesystem through the restore_config_from_backup endpoint. The vulnerability allows attackers to bypas directory restrictions and read arbitrary files from the server filesystem by manipulating the backup_id parameter with path traversal sequences (e.g., ../). This vuln is fixed in 4.5.4.
CVE-2025-50515	An issue was discovered in phome Empirebak 2010 in ebak2008/upload/class/config.php allowing attackers to execute arbitrary code when the config file was load
CVE-2025-53342	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GoodLayers Modernize allows Stored XSS. This issue affects Mo from n/a through 3.4.0.
CVE-2025-20301	A vulnerability in the web-based management interface of Cisco Secure FMC Software could allow an authenticated, low-privileged, remote attacker to access troul files for a different domain. This vulnerability is due to missing authorization checks. An attacker could exploit this vulnerability by directly accessing a troubleshoo different domain that is managed on the same Cisco Secure FMC instance. A successful exploit could allow the attacker to retrieve a troubleshoot file for a differen which could allow the attacker to access sensitive information contained in the troubleshoot file.
CVE-2025-50891	Adform Site Tracking 1.1 allows attackers to inject HTML or execute arbitrary code via cookie hijacking.
CVE-2025-49051	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in biscia7 Hide Text Shortcode allows Stored XSS. This issue affec Text Shortcode: from n/a through 1.1.
CVE-2025-50461	A deserialization vulnerability exists in Volcengine's verl 3.0.0, specifically in the scripts/model_merger.py script when using the "fsdp" backend. The script calls tor with weights_only=False on user-supplied .pt files, allowing attackers to execute arbitrary code if a maliciously crafted model file is loaded. An attacker can exploit convincing a victim to download and place a malicious model file in a local directory with a specific filename pattern. This vulnerability may lead to arbitrary code e with the privileges of the user running the script.
CVE-2025-53582	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WordLift WordLift allows Stored XSS. This issue affects WordLif n/a through 3.54.5.
CVE-2025-51506	In the smartLibrary component of the HRForecast Suite 0.4.3, a SQL injection vulnerability was discovered in the valueKey parameter. This flaw enables any auther user to execute arbitrary SQL queries, via crafted payloads to valueKey to the api/smartlibrary/v2/en/dictionaries/options/lookup endpoint.
CVE-2025-54054	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AA Web Servant 12 Step Meeting List allows Stored XSS. This is affects 12 Step Meeting List: from n/a through 3.18.3.
CVE-2025-55668	Session Fixation vulnerability in Apache Tomcat via rewrite valve. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0-M1 through 10.1.4 9.0.0.M1 through 9.0.105. Older, EOL versions may also be affected. Users are recommended to upgrade to version 11.0.8, 10.1.42 or 9.0.106, which fix the issue.
CVE-2025-54708	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins B Blocks allows DOM-Based XSS. This issue affects B B from n/a through 2.0.5.
CVE-2025-53249	Cross-Site Request Forgery (CSRF) vulnerability in hakeemnala Build App Online allows Cross Site Request Forgery. This issue affects Build App Online: from n/a thr 1.0.23.
CVE-2025-41685	A low-privileged remote attacker can obtain the username of another registered Sunny Portal user by entering that user's email address.
CVE-2024-10219	An issue has been discovered in GitLab CE/EE affecting all versions from 15.6 before 18.0.6, 18.1 before 18.1.4, and 18.2 before 18.2.2 that under certain condition have allowed authenticated users to bypass access controls and download private artifacts by accessing specific API endpoints.
CVE-2023-43683	An issue was discovered in Malwarebytes 4.6.14.326 and before 5.1.5.116 (and Nebula 2020-10-21 and later). A Stack buffer out-of-bounds access exists because integer underflow when handling newline characters.
CVE-	

2025-50926	Easy Hosting Control Panel EHCP v20.04.1.b was discovered to contain a SQL injection vulnerability via the id parameter in the List All Email Addresses function.
CVE-2025-1477	An issue has been discovered in GitLab CE/EE affecting all versions from 8.14 before 18.0.6, 18.1 before 18.1.4, and 18.2 before 18.2.2 that could have allowed an unauthenticated user to create a denial of service condition by sending specially crafted payloads to specific integration API endpoints.
CVE-2025-8914	Organization Portal System developed by WellChoose has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commanc database contents.
CVE-2025-52771	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bcupham Video Expander allows Stored XSS. This issue affects Expander: from n/a through 1.0.
CVE-2025-54747	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpbakery Templatera allows DOM-Based XSS. This issue affect Templatera: from n/a through 2.3.0.
CVE-2025-28962	Missing Authorization vulnerability in stefanoai Advanced Google Universal Analytics allows Exploiting Incorrectly Configured Access Control Security Levels. This is affects Advanced Google Universal Analytics: from n/a through 1.0.3.
CVE-2025-54688	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetEngine allows Stored XSS. This issue affects JetE from n/a through 3.7.1.2.
CVE-2025-55740	nginx-defender is a high-performance, enterprise-grade Web Application Firewall (WAF) and threat detection system engineered for modern web infrastructure. Thi configuration vulnerability affecting nginx-defender deployments. Example configuration files config.yaml and docker-compose.yml contain default credentials (default_password: "change_me_please", GF_SECURITY_ADMIN_PASSWORD=admin123). If users deploy nginx-defender without changing these defaults, attackers network access could gain administrative control, bypassing security protections. The issue is addressed in v1.5.0 and later.
CVE-2025-54685	Insertion of Sensitive Information Into Sent Data vulnerability in Brainstorm Force SureDash allows Retrieve Embedded Sensitive Data. This issue affects SureDash: through 1.1.0.
CVE-2025-45317	A zip slip vulnerability in the /modules/ImportModule.php component of hortusfox-web v4.4 allows attackers to execute arbitrary code via a crafted archive.
CVE-2025-55589	TOTOLINK A3002R v4.0.0-B20230531.1404 was discovered to contain multiple OS command injection vulnerabilities via the macstr, bandstr, and clientoff paramet /boafrm/formMapDelDevice.
CVE-2025-54680	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sparkle Themes Blogger Buzz allows Stored XSS. This issue aff Blogger Buzz: from n/a through 1.2.6.
CVE-2025-54676	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in vcita Online Booking & Scheduling Calendar for WordPress by v allows Stored XSS. This issue affects Online Booking & Scheduling Calendar for WordPress by vcita: from n/a through 4.5.3.
CVE-2025-50861	The Lotus Cars Android app (com.lotus.carsdomestic.intl) 1.2.8 contains an exported component, PushDeepLinkActivity, which is accessible without authentication or malicious apps. This poses a risk of unintended access to application internals and can cause denial of service or logic abuse.
CVE-2025-0818	Several WordPress plugins using elFinder versions 2.1.64 and prior are vulnerable to Directory Traversal in various versions. This makes it possible for unauthentica attackers to delete arbitrary files. Successful exploitation of this vulnerability requires a site owner to explicitly make an instance of the file manager available to us
CVE-2025-55585	TOTOLINK A3002R v4.0.0-B20230531.1404 was discovered to contain an eval injection vulnerability via the eval() function.
CVE-2025-54668	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Saad Iqbal myCred allows Stored XSS. This issue affects myCre n/a through 2.9.4.3.
CVE-2025-30993	Missing Authorization vulnerability in VillaTheme Thank You Page Customizer for WooCommerce – Increase Your Sales allows Exploiting Incorrectly Configured Acce Security Levels. This issue affects Thank You Page Customizer for WooCommerce – Increase Your Sales: from n/a through 1.1.7.
CVE-2025-8909	Organization Portal System developed by WellChoose has an Arbitrary File Reading vulnerability, allowing remote attackers with regular privileges to exploit Absolu Traversal to download arbitrary system files.
CVE-2025-52730	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themefunction WordPress Event Manager, Event Calendar and Plugin allows Stored XSS. This issue affects WordPress Event Manager, Event Calendar and Booking Plugin: from n/a through 4.0.24.
CVE-2025-39483	Improper Control of Generation of Code ('Code Injection') vulnerability in imithemes Eventer allows Code Injection. This issue affects Eventer: from n/a through 3.9.
CVE-2025-52721	Missing Authorization vulnerability in LCweb Global Gallery allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Global Gallery through 9.2.3.
CVE-	

2025-47610	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wetail WooCommerce Fortnox Integration allows Stored XSS. T affects WooCommerce Fortnox Integration: from n/a through 4.5.6.
CVE-2025-50040	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in moshensky CF7 Spreadsheets allows Stored XSS. This issue aff Spreadsheets: from n/a through 2.3.2.
CVE-2025-50031	Missing Authorization vulnerability in syedamirhussain91 DB Backup allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects DB B from n/a through 6.0.
CVE-2025-50029	Missing Authorization vulnerability in Ashish AI Tools allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects AI Tools: from n/a th 4.0.7.
CVE-2025-49437	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in worstguy WP LOL Rotation allows Stored XSS. This issue affects Rotation: from n/a through 1.0.
CVE-2025-49433	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThanhD Supermalink allows DOM-Based XSS. This issue affects Supermalink: from n/a through 1.1.
CVE-2025-49061	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in perteus Porn Videos Embed allows Stored XSS. This issue affec Videos Embed: from n/a through 0.9.1.
CVE-2025-8881	Inappropriate implementation in File Picker in Google Chrome prior to 139.0.7258.127 allowed a remote attacker who convinced a user to engage in specific UI ges leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)
CVE-2025-7662	The Gestion de tarifs plugin for WordPress is vulnerable to SQL Injection via the 'tarif' and 'intitule' shortcodes in all versions up to, and including, 1.4 due to insuffi escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Cont level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2025-54687	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetTabs allows DOM-Based XSS. This issue affects Je from n/a through 2.2.9.1.
CVE-2025-50946	OS Command Injection in Olivetin 2025.4.22 Custom Themes via the ParseRequestURI function in service/internal/executor/arguments.go.
CVE-2025-55711	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Table Builder WP Table Builder allows Stored XSS. This issu WP Table Builder: from n/a through 2.0.12.
CVE-2025-54749	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetProductGallery allows Stored XSS. This issue affe JetProductGallery: from n/a through 2.2.0.2.
CVE-2025-54704	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hashthemes Easy Elementor Addons allows DOM-Based XSS. T affects Easy Elementor Addons: from n/a through 2.2.6.
CVE-2025-54696	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFunnels WPFunnels allows Stored XSS. This issue affects WP from n/a through 3.5.26.
CVE-2025-55714	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetElements For Elementor allows Stored XSS. This affects JetElements For Elementor: from n/a through 2.7.9.
CVE-2025-55590	TOTOLINK A3002R v4.0.0-B20230531.1404 was discovered to contain an command injection vulnerability via the component bupload.html.
CVE-2025-55675	Apache Superset contains an improper access control vulnerability in its /explore endpoint. A missing authorization check allows an authenticated user to discover about datasources they do not have permission to access. By iterating through the datasource_id in the URL, an attacker can enumerate and confirm the existence names of protected datasources, leading to sensitive information disclosure. This issue affects Apache Superset: before 5.0.0. Users are recommended to upgrade 5.0.0, which fixes the issue.
CVE-2025-55674	A bypass of the DISALLOWED_SQL_FUNCTIONS security feature in Apache Superset allows for the execution of blocked SQL functions. An attacker can use a specia block to circumvent the denylist. This allows a user with SQL Lab access to execute functions that were intended to be disabled, leading to the disclosure of sensiti database information like the software version. This issue affects Apache Superset: before 5.0.0. Users are recommended to upgrade to version 5.0.0, which fixes t
CVE-2025-55709	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Visual Composer Visual Composer Website Builder allows Store This issue affects Visual Composer Website Builder: from n/a through n/a.
CVE-2025-54706	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noor Alam Magical Posts Display allows DOM-Based XSS. This i affects Magical Posts Display: from n/a through 1.2.52.
CVE-2025-54699	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in masteriyo Masteriyo - LMS allows Stored XSS. This issue affects Masteriyo - LMS: from n/a through 1.18.3.

CVE-2025-5998	The PPWP – Password Protect Pages WordPress plugin before version 1.9.11 allows to put the site content behind a password authorization, however users with sub greater roles can view content via the REST API.
CVE-2025-2937	An issue has been discovered in GitLab CE/EE affecting all versions from 13.2 before 18.0.6, 18.1 before 18.1.4, and 18.2 before 18.2.2 that could have allowed authenticated users to create a denial of service condition by sending specially crafted markdown payloads to the Wiki feature.
CVE-2025-55712	Missing Authorization vulnerability in POSIMYTH The Plus Addons for Elementor Page Builder Lite allows Exploiting Incorrectly Configured Access Control Security Le issue affects The Plus Addons for Elementor Page Builder Lite: from n/a through 6.3.13.
CVE-2025-7440	The Anber Elementor Addon plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the $item['button_link']['url'] parameter in all versions up to, and i 1.0.1 to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arl web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-8143	The Soledad theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pcsml_smartlists_h' parameter in all versions up to, and including, 8.6.7 due t insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary w in pages that will execute whenever a user accesses an injected page.
CVE-2025-8293	The Intl DateTime Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'date' parameter in all versions up to, and including, 1.0.1 due insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary w in pages that will execute whenever a user accesses an injected page.
CVE-2025-8604	The WP Table Builder – WordPress Table Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wptb shortcode in all versions up to including, 2.0.12 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with cont level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-8451	The Essential Addons for Elementor – Popular Elementor Templates & Widgets plugin for WordPress is vulnerable to DOM-Based Stored Cross-Site Scripting via the gallery-items' parameter in all versions up to, and including, 6.2.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticate attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-28987	Server-Side Request Forgery (SSRF) vulnerability in PressForward PressForward allows Server Side Request Forgery. This issue affects PressForward: from n/a throu
CVE-2025-8896	The User Profile Builder – Beautiful User Registration Forms, User Profiles & User Role Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via th 'gdpr_communication_preferences[]' parameter in all versions up to, and including, 3.14.3 due to insufficient input sanitization and output escaping. This makes it for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected This is only exploitable when the GDPR Communication Preferences module is enabled and at least one GDPR Communication Preferences field has been added to profile form.
CVE-2025-5844	The Radius Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'subHeadingTagName' parameter in all versions up to, and including, 2.2 insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary w in pages that will execute whenever a user accesses an injected page.
CVE-2025-7439	Anber Elementor Addon plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the $anber_item['button_link']['url']' parameter in all versions up to, ar including, 1.0.1 to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, t arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-7507	The elink – Embed Content plugin for WordPress is vulnerable to Malicious Redirect in all versions up to, and including, 1.1.0. This is due to the plugin not restrictin that can be supplied through the elink shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to supply an HTML fil be leverged to redirect users to a malicious domain.
CVE-2025-7496	The WPC Smart Compare for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via DOM elements in all versions up to, and including due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbi scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-6221	The Embed Bokun plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'align' parameter in all versions up to, and including, 0.23 due to insuffic sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in page execute whenever a user accesses an injected page.
CVE-2025-7651	The Earnware Connect plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ew_hasrole' shortcode in all versions up to, and including, 1 to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access a to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-7649	The Surbma | Recent Comments Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'recent-comments' shortcode in all vers to, and including, 2.0 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.
CVE-2025-8720	The Plugin README Parser plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'target' parameter in all versions up to, and including, 1.3.15 du insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary w in pages that will execute whenever a user accesses an injected page.
CVE-2024-45062	A stack based buffer overflow vulnerability is present in OpenPrinting ippusbxd 1.34. A specially configured printer that supports IPP-over-USB can cause a buffer o which can lead to a arbitrary code execution in a privileged service. To trigger the vulnerability, a malicious device would need to be connected to the vulnerable s over USB.
CVE-2025-8622	The Flexible Map plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Flexible Maps shortcode in all versions up to, and including, 1.18. insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-8867	The Graphina - Elementor Charts and Graphs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple chart widget parameters in version 3.1.3 below. This is due to insufficient input sanitization and output escaping on user supplied attributes such as chart categories, titles, and tooltip settings. This makes 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
CVE-2025-8567	The Nexter Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 4.5.4 due to insufficient sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject a web scripts in pages that will execute whenever a user accesses an injected page.

CVE-2025-8719	The Translate This gTranslate Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'base_lang' parameter in all versions up to, and in 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2025-9148	A vulnerability was found in CodePhiliaX Chat2DB up to 0.3.7. This affects an unknown function of the file ai/chat2db/server/web/api/controller/data/source/DataSourceController.java of the component JDBC Connection Handler. The manipulation results in sql injection. T can be executed remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any v
CVE-2025-9140	A vulnerability was identified in Shanghai Lingdang Information Technology Lingdang CRM up to 8.6.4.7. Affected by this issue is some unknown functionality of the /crm/crmapi/erp/tabdetail_moduleSave.php. The manipulation of the argument getvaluestring leads to sql injection. It is possible to initiate the attack remotely. Th is publicly available and might be used. Upgrading to version 8.6.5.4 can resolve this issue. The affected component should be upgraded. The vendor explains: "All injection vectors were patched via parameterized queries and input sanitization in v8.6.5+."
CVE-2025-8930	A vulnerability was found in code-projects Medical Store Management System 1.0. This issue affects some unknown processing of the file UpdateCompany.java of t component Update Company Page. The manipulation of the argument companyNameTxt leads to sql injection. The attack may be initiated remotely. The exploit ha disclosed to the public and may be used.
CVE-2025-8929	A vulnerability has been found in code-projects Medical Store Management System 1.0. This vulnerability affects unknown code of the file MainPanel.java. The man of the argument searchTxt leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-9153	A vulnerability was detected in itsourcecode Online Tour and Travel Management System 1.0. This vulnerability affects unknown code of the file /admin/operations/travellers.php. The manipulation of the argument photo results in unrestricted upload. The attack can be launched remotely. The exploit is now may be used.
CVE-2025-8965	A vulnerability has been found in linlinjava litemall up to 1.8.0. This vulnerability affects the function create of the file litemall-admin-api/src/main/java/org/linlinjava/litemall/admin/web/AdminStorageController.java of the component Endpoint. The manipulation of the argument File leads to unrestr upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8908	A vulnerability was determined in Shanghai Lingdang Information Technology Lingdang CRM up to 8.6.5.4. Affected by this issue is some unknown functionality of t crm/WeiXinApp/yunzhijia/event.php. The manipulation of the argument openid leads to sql injection. The attack may be launched remotely. The exploit has been d the public and may be used. Upgrading to version 8.6.5 is able to address this issue. It is recommended to upgrade the affected component. The vendor explains: injection vectors were patched via parameterized queries and input sanitization in v8.6.5+."
CVE-2025-8928	A vulnerability was identified in code-projects Medical Store Management System 1.0. This affects an unknown part of the file UpdateMedicines.java of the compon Update Medicines Page. The manipulation of the argument productNameTxt leads to sql injection. It is possible to initiate the attack remotely. The exploit has beer to the public and may be used.
CVE-2025-8937	A vulnerability has been found in TOTOLINK N350R 1.2.3-B20130826. This vulnerability affects unknown code of the file /boafrm/formSysCmd. The manipulation lea command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-9099	A vulnerability was identified in Acrel Environmental Monitoring Cloud Platform up to 20250804. This affects an unknown part of the file /NewsManage/UploadNews manipulation of the argument File leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may b The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-8938	A vulnerability was found in TOTOLINK N350R 1.2.3-B20130826. This issue affects the function formSysTel of the file /boafrm/formSysTel of the component Telnet S The manipulation of the argument TelEnabled leads to backdoor. The attack may be initiated remotely. The exploit has been disclosed to the public and may be us
CVE-2025-54466	Improper Control of Generation of Code ('Code Injection') vulnerability leading to a possible RCE in Apache OFBiz scrum plugin. This issue affects Apache OFBiz: be 24.09.02 only when the scrum plugin is used. Even unauthenticated attackers can exploit this vulnerability. Users are recommended to upgrade to version 24.09.0 fixes the issue.
CVE-2025-9090	A vulnerability was identified in Tenda AC20 16.03.08.12. Affected is the function websFormDefine of the file /goform/telnet of the component Telnet Service. The manipulation leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8963	A vulnerability was determined in jeecgboot JimuReport up to 2.1.1. Affected by this issue is some unknown functionality of the file /drag/onlDragDataSource/testC of the component Data Large Screen Template. The manipulation leads to deserialization. The attack may be launched remotely. The vendor response to the GitHu report is: "Modified, next version updated".
CVE-2025-8931	A vulnerability was determined in code-projects Medical Store Management System 1.0. Affected is an unknown function of the file ChangePassword.java. The man of the argument newPassTxt leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8905	The Inpersttion For Theme plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.0 via the theme_section_shortcode() This is due to the plugin not restricting what functions can be called. This makes it possible for authenticated attackers, with Contributor-level access and above, to code on the server which is limited to arbitrary functions without any user supplied parameters.
CVE-2025-9151	A security flaw has been discovered in LiuYuYang01 ThriveX-Blog up to 3.1.7. Affected by this vulnerability is the function updateJsonValueByName of the file /web_config/json/name/web. Performing manipulation results in improper authorization. It is possible to initiate the attack remotely. The exploit has been released public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-9025	A vulnerability was determined in code-projects Simple Cafe Ordering System 1.0. Affected by this issue is some unknown functionality of the file /portal.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8956	A vulnerability was found in D-Link DIR-818L up to 1.05B01. This issue affects the function getenv of the file /htdocs/cgibin of the component ssdpcgi. The manipula to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-9149	A vulnerability was determined in Wavlink WL-NU516U1 M16U1_V240425. This impacts the function sub_4032E4 of the file /cgi-bin/wireless.cgi. This manipulation argument Guest_ssid causes command injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.
CVE-	AIDE is an advanced intrusion detection environment. Prior to version 0.19.2, there is an improper output neutralization vulnerability in AIDE. An attacker can craft malicious filename by including terminal escape sequences to hide the addition or removal of the file from the report and/or tamper with the log output. A local use

2025-54389	exploit this to bypass the AIDE detection of malicious files. Additionally the output of extended attribute key names and symbolic links targets are also not properly neutralized. This issue has been patched in version 0.19.2. A workaround involves configuring AIDE to write the report output to a regular file, redirecting stdout to file, or redirecting the log output written to stderr to a regular file.
CVE-2025-54409	AIDE is an advanced intrusion detection environment. From versions 0.13 to 0.19.1, there is a null pointer dereference vulnerability in AIDE. An attacker can crash program during report printing or database listing after setting extended file attributes with an empty attribute value or with a key containing a comma. A local use exploit this to cause a local denial of service. This issue has been patched in version 0.19.2. A workaround involves removing xattrs group from rules matching files affected file systems.
CVE-2025-43201	This issue was addressed with improved checks. This issue is fixed in Apple Music Classical 2.3 for Android. An app may be able to unexpectedly leak a user's crede
CVE-2025-33100	IBM Concert Software 1.0.0 through 1.1.0 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authenticati outbound communication to external components, or encryption of internal data.
CVE-2025-8910	Organization Portal System developed by WellChoose has a Reflected Cross-site Scripting vulnerability, allowing unauthenticated remote attackers to execute arbit JavaScript codes in user's browser through phishing attacks.
CVE-2025-45316	A cross-site scripting (XSS) vulnerability in the TextBlockModule.php component of hortusfox-web v4.4 allows attackers to execute arbitrary web scripts or HTML vi a crafted payload into the name parameter.
CVE-2025-45314	A cross-site scripting (XSS) vulnerability in the /Calendar endpoint of hortusfox-web v4.4 allows attackers to execute arbitrary JavaScript in the context of a user's b via a crafted payload injected into the add function.
CVE-2025-54759	Sante PACS Server is vulnerable to stored cross-site scripting. An attacker could inject malicious HTML codes redirecting a user to a malicious webpage and stealin user's cookie.
CVE-2025-8911	Organization Portal System developed by WellChoose has a Reflected Cross-site Scripting vulnerability, allowing unauthenticated remote attackers to execute arbit JavaScript codes in user's browser through phishing attacks.
CVE-2025-7808	The WP Shopify WordPress plugin before 1.5.4 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Sc which could be used against high privilege users such as admin
CVE-2025-8046	The Injection Guard WordPress plugin before 1.2.8 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could Reflected Cross-Site Scripting in old web browsers
CVE-2025-7688	The Add User Meta plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing or incorrect no validation on the 'add-user-meta' page. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged reques they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-7684	The Last.fm Recent Album Artwork plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.2. This is due to missing incorrect nonce validation on the 'lastfm_albums_artwork.php' page. This makes it possible for unauthenticated attackers to update settings and inject malicious w via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-7683	The LatestCheckins plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1. This is due to missing or incorrect nonce validation on the 'LatestCheckins' page. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged reque they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-5417	An insufficient access control vulnerability was found in the Red Hat Developer Hub rhdh/rhdh-hub-rhel9 container image. The Red Hat Developer Hub cluster admi who has standard user access to the cluster, and the Red Hat Developer Hub namespace, can access the rhdh/rhdh-hub-rhel9 container image and modify the ima content. This issue affects the confidentiality and integrity of the data, and any changes made are not permanent, as they reset after the pod restarts.
CVE-2025-7686	The weichuncai(WP伪春菜) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5. This is due to missing or incorre validation on the sm-options.php page. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged reques they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-45313	A cross-site scripting (XSS) vulnerability in the /tasks endpoint of hortusfox-web v4.4 allows attackers to execute arbitrary JavaScript in the context of a user's brow crafted payload injected into the title parameter.
CVE-2025-52335	EyouCMS 1.7.3 is vulnerale to Cross Site Scripting (XSS) in index.php, which can be exploited to obtain sensitive information.
CVE-2025-7668	The Linux Promotional Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4. This is due to missing or inco nonce validation on the 'inux-promotional-plugin.php' page. This makes it possible for unauthenticated attackers to update settings and inject malicious web script forged request granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-8113	The Ebook Store WordPress plugin before 5.8015 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could l Reflected Cross-Site Scripting in old web browsers.
CVE-2025-51691	Cross-Site Scripting (XSS) vulnerability found in MarkTwo commit e3a1d3f90cce4ea9c26efcbbf3a1cbfb9dcdb298 (May 2025) allows a remote attacker to execute a code via a crafted script input to the editor interface. The application does not properly sanitize user-supplied Markdown before rendering it. Successful exploitatio lead to session hijacking, credential theft, or arbitrary client-side code execution in the context of the victim's browser.
CVE-2025-	A Cross-Site Scripting (XSS) vulnerability exists in SpatialReference.org (OSGeo/spatialreference.org) versions prior to 2025-05-17 (commit 2120adfa17ddd535bd0f539e6c4988fa3a2cb491). The vulnerability is caused by improper handling of user input in the search query parameter. An attacker can cr specially formed URL with malicious JavaScript code, which is then reflected back and executed in the victim's browser. This flaw allows an attacker to execute arb

50690	JavaScript in the context of the victim's session, potentially leading to session hijacking, phishing attacks, data theft, or redirection to malicious sites. The issue is e on publicly accessible pages, making it exploitable by an unauthenticated attacker.
CVE-2025-50938	Cross site scripting (XSS) vulnerability in Hustoj 2025-01-31 via the TID parameter to thread.php.
CVE-2025-20235	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attac conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by inserting crafted input into various data fields in an affected interface. A successful exploit co the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.
CVE-2025-55160	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-27 and 7.1.2-1, there is undefined behavio (function-type-mismatch) in splay tree cloning callback. This results in a deterministic abort under UBSan (DoS in sanitizer builds), with no crash in a non-sanitized issue has been patched in versions 6.9.13-27 and 7.1.2-1.
CVE-2025-51965	OURPHP thru 8.6.1 is vulnerable to Cross-Site Scripting (XSS) via the "Name" field of the "Complete Profile" functionality under the "My User Center" page, which ca accessed after registering through the front-end interface.
CVE-2025-20238	A vulnerability in Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authen local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. To exploit this vulnerability, the attacker must have va administrative credentials. This vulnerability is due to insufficient input validation of commands that are supplied by the user. An attacker could exploit this vulnera authenticating to a device and submitting crafted input for specific commands. A successful exploit could allow the attacker to execute commands on the underlyir operating system as root.
CVE-2025-20237	A vulnerability in Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authen local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. To exploit this vulnerability, the attacker must have va administrative credentials. This vulnerability is due to insufficient input validation of commands that are supplied by the user. An attacker could exploit this vulnera authenticating to a device and submitting crafted input for specific commands. A successful exploit could allow the attacker to execute commands on the underlyir operating system as root.
CVE-2025-20220	A vulnerability in the CLI of Cisco Secure Firewall Management Center (FMC) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an auth local attacker to execute arbitrary commands on the underlying operating system as root. This vulnerability is due to improper input validation for specific CLI com An attacker could exploit this vulnerability by injecting operating system commands into a legitimate command. A successful exploit could allow the attacker to es restricted command prompt and execute arbitrary commands on the underlying operating system. To successfully exploit this vulnerability, an attacker would nee Administrator credentials. For more information about vulnerable scenarios, see the Details ["#details"] section of this advisory.
CVE-2025-49898	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Xolluteon Dropshix allows DOM-Based XSS.This issue affects D from n/a through 4.0.14.
CVE-2025-49048	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in inspectlet Inspectlet – User Session Recording and Hea allows Stored XSS. This issue affects Inspectlet – User Session Recording and Heatmaps: from n/a through 2.0.
CVE-2025-50862	The Lotus Cars Android app (com.lotus.carsdomestic.intl) 1.2.8 has allowBackup=true set in its manifest, allowing data exfiltration via ADB backup on rooted or del enabled devices. This presents a risk of user data exposure.
CVE-2025-49047	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in keeross DigitalOcean Spaces Sync allows Stored XSS. This issu DigitalOcean Spaces Sync: from n/a through 2.2.1.
CVE-2025-49053	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kadesthemes WP Airdrop Manager allows Stored XSS. This issu WP Airdrop Manager: from n/a through 1.0.5.
CVE-2025-55713	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CreativeThemes Blocksy allows Stored XSS. This issue affects B from n/a through 2.1.6.
CVE-2025-54683	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Astoundify WP Modal Popup with Cookie Integration allows Refl XSS. This issue affects WP Modal Popup with Cookie Integration: from n/a through 2.4.
CVE-2025-54729	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Webba Appointment Booking Webba Booking allows Stored XS issue affects Webba Booking: from n/a through 6.0.5.
CVE-2025-54727	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CreativeMindsSolutions CM On Demand Search And Replace al Stored XSS. This issue affects CM On Demand Search And Replace: from n/a through 1.5.2.
CVE-2025-54684	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CRM Perks Integration for Contact Form 7 and Constant Contac Stored XSS. This issue affects Integration for Contact Form 7 and Constant Contact: from n/a through 1.1.7.
CVE-2025-53581	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in artiosmedia RSS Feed Pro allows Stored XSS. This issue affects Pro: from n/a through 1.1.8.
CVE-2025-41242	Spring Framework MVC applications can be vulnerable to a “Path Traversal Vulnerability” when deployed on a non-compliant Servlet container. An application can vulnerable when all the following are true: * the application is deployed as a WAR or with an embedded Servlet container * the Servlet container does not reject su sequences https://jakarta.ee/specifications/servlet/6.1/jakarta-servlet-spec-6.1.html#uri-path-canonicalization * the application serves static resources https://docs.spring.io/spring-framework/reference/web/webmvc/mvc-config/static-resources.html#page-title with Spring resource handling We have verified that applications deployed on Apache Tomcat or Eclipse Jetty are not vulnerable, as long as default security features are not disabled in the configuration. Because we c check exploits against all Servlet containers and configuration variants, we strongly recommend upgrading your application.

CVE-2025-1759	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 m
CVE-2025-20224	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) module of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Secure Firewall Thre Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a memory leak, resulting in a denial of service (DoS) condition. This vulnerabilit improper parsing of IKEv2 packets. An attacker could exploit this vulnerability by sending a continuous stream of crafted IKEv2 packets to an affected device. A suc exploit could allow the attacker to partially exhaust system memory, causing system instability like being unable to establish new IKEv2 VPN sessions. A manual re the device is required to recover from this condition.
CVE-2025-20252	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) module of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Secure Firewall Thre Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a memory leak, resulting in a denial of service (DoS) condition. This vulnerabilit improper parsing of IKEv2 packets. An attacker could exploit this vulnerability by sending a continuous stream of crafted IKEv2 packets to an affected device. A suc exploit could allow the attacker to partially exhaust system memory, causing system instability like being unable to establish new IKEv2 VPN sessions. A manual re the device is required to recover from this condition.
CVE-2025-20254	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) module of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Secure Firewall Thre Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a memory leak, resulting in a denial of service (DoS) condition. This vulnerabilit improper parsing of IKEv2 packets. An attacker could exploit this vulnerability by sending a continuous stream of crafted IKEv2 packets to an affected device. A suc exploit could allow the attacker to partially exhaust system memory, causing system instability like being unable to establish new IKEv2 VPN sessions. A manual re the device is required to recover from this condition.
CVE-2025-20268	A vulnerability in the Geolocation-Based Remote Access (RA) VPN feature of Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, r attacker to bypass configured policies to allow or deny HTTP connections based on a country or region. This vulnerability exists because the URL string is not fully p attacker could exploit this vulnerability by sending a crafted HTTP connection through the targeted device. A successful exploit could allow the attacker to bypass c policies and gain access to a network where the connection should have been denied.
CVE-2025-20225	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) feature of Cisco IOS Software, IOS XE Software, Secure Firewall Adaptive Security Appliance (ASA) Sc and Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a memory leak, resulting in a denial of service (DoS) condition. This vulnerability is due to a lack of proper processing of IKEv2 packets. An attacker could exploit this vulnerability by sending crafted IKEv2 packets to a device. In the case of Cisco IOS and IOS XE Software, a successful exploit could allow the attacker to cause the device to reload unexpectedly. In the case of Cisco A FTD Software, a successful exploit could allow the attacker to partially exhaust system memory, causing system instability such as being unable to establish new IK sessions. A manual reboot of the device is required to recover from this condition.
CVE-2025-26709	There is an unauthorized access vulnerability in ZTE F50. Due to improper permission control of the Web module interface, an unauthorized attacker can obtain sen information through the interface
CVE-2025-55194	Part-DB is an open source inventory management system for electronic components. Prior to version 1.17.3, any authenticated user can upload a profile picture wi misleading file extension (e.g., .jpg.txt), resulting in a persistent 500 Internal Server Error when attempting to view or edit that user's profile. This makes the profile permanently inaccessible via the UI for both users and administrators, constituting a Denial of Service (DoS) within the user management interface. This issue has patched in version 1.17.3.
CVE-2025-55296	librenms is a community-based GPL-licensed network monitoring system. A stored Cross-Site Scripting (XSS) vulnerability exists in LibreNMS (<= 25.6.0) in the Ale Template creation feature. This allows a user with the admin role to inject malicious JavaScript, which will be executed when the template is rendered, potentially compromising other admin accounts. This vulnerability is fixed in 25.8.0.
CVE-2025-53241	Server-Side Request Forgery (SSRF) vulnerability in kodeshpa Simplified allows Server Side Request Forgery. This issue affects Simplified: from n/a through 1.0.9.
CVE-2025-26484	Dell CloudLink, versions 8.0 through 8.1.1, contains an Improper Restriction of XML External Entity Reference vulnerability. A high privileged attacker with remote a could potentially exploit this vulnerability, leading to Denial of service.
CVE-2025-55005	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to version 7.1.2-1, when preparing to transform from Log to s colorspaces, the logmap construction fails to handle cases where the reference-black or reference-white value is larger than 1024. This leads to corrupting memory the end of the allocated logmap buffer. This issue has been patched in version 7.1.2-1.
CVE-2025-55288	Genealogy is a family tree PHP application. Prior to 4.4.0, Authenticated Reflected Cross-Site Scripting (XSS) vulnerability was identified in the Genealogy applicatio Authenticated attackers could run arbitrary JavaScript in another user's session, leading to session hijacking, data theft, and UI manipulation. This vulnerability is fi 4.4.0.
CVE-2025-54698	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in RadiusTheme Classified Listing allows Code Injection. This issue affe Classified Listing: from n/a through 5.0.0.
CVE-2025-27909	IBM Concert Software 1.0.0 through 1.1.0 uses cross-origin resource sharing (CORS) which could allow an attacker to carry out privileged actions as the domain na being limited to only trusted domains.
CVE-2025-55672	A stored Cross-Site Scripting (XSS) vulnerability exists in Apache Superset's chart visualization. An authenticated user with permissions to edit charts can inject a m payload into a column's label. The payload is not properly sanitized and gets executed in the victim's browser when they hover over the chart, potentially leading t hijacking or the execution of arbitrary commands on behalf of the user. This issue affects Apache Superset: before 5.0.0. Users are recommended to upgrade to ve 5.0.0, which fixes the issue.
CVE-2025-54695	Missing Authorization vulnerability in HasTech HT Mega allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects HT Mega: from n/ 2.9.0.
CVE-2025-3414	The Structured Content (JSON-LD) #wpsc WordPress plugin before 1.7.0 does not validate and escape some of its block options before outputting them back in a pa where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
CVE-2025-54862	Sante PACS Server web portal is vulnerable to stored cross-site scripting. An attacker could inject malicious HTML codes redirecting a user to a malicious webpage stealing the user's cookie.

CVE-2025-54682	Cross-Site Request Forgery (CSRF) vulnerability in CRM Perks Connector for Gravity Forms and Google Sheets allows Cross Site Request Forgery. This issue affects for Gravity Forms and Google Sheets: from n/a through 1.2.4.
CVE-2025-52386	CycloneDX Sunshine v0.9 is vulnerable to CSV Formula Injection via a crafted JSON file
CVE-2025-52392	Soosyze CMS 2.0 allows brute-force login attacks via the /user/login endpoint due to missing rate-limiting and lockout mechanisms. An attacker can repeatedly sub attempts without restrictions, potentially gaining unauthorized administrative access. This vulnerability corresponds to CWE-307: Improper Restriction of Excessive Authentication Attempts.
CVE-2025-54674	Cross-Site Request Forgery (CSRF) vulnerability in mklacroix Product Configurator for WooCommerce allows Cross Site Request Forgery. This issue affects Product Configurator for WooCommerce: from n/a through 1.4.4.
CVE-2025-50817	A vulnerability in the Python-Future 1.0.0 module allows for arbitrary code execution via the unintended import of a file named test.py. When the module is loaded automatically imports test.py, if present in the same directory or in the sys.path. This behavior can be exploited by an attacker who has the ability to write files to t server, allowing the execution of arbitrary code.
CVE-2025-54717	Missing Authorization vulnerability in e-plugins WP Membership allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Memb from n/a through 1.6.3.
CVE-2025-45315	A cross-site scripting (XSS) vulnerability in the /controller/admin.php endpoint of hortusfox-web v4.4 allows attackers to execute arbitrary JavaScript in the context user's browser via a crafted payload injected into the email parameter.
CVE-2025-33008	IBM Sterling B2B Integrator 6.2.1.0 and IBM Sterling File Gateway 6.2.1.0 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to emb arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.
CVE-2025-55203	Plane is open-source project management software. Prior to version 0.28.0, a stored cross-site scripting (XSS) vulnerability exists in the description_html field of Pla flaw allows an attacker to inject malicious JavaScript code that is stored and later executed in other users' browsers. The description_html field is not properly sanit escaped. An attacker can submit crafted JavaScript payloads that are saved in the application's database. When another user views the affected content, the inject executes in their browser, running in the application's context and bypassing standard security protections. Successful exploitation can lead to session hijacking, th sensitive information, or forced redirection to malicious sites. The vulnerability can also be chained with CSRF attacks to perform unauthorized actions, or leverage distribute malware and exploit additional browser vulnerabilities. This issue has been patched in version 0.28.0.
CVE-2025-36088	IBM TS4500 1.11.0.0-D00, 1.11.0.1-C00, 1.11.0.2-C00, and 1.10.00-F00 web GUI is vulnerable to cross-site scripting. This vulnerability allows an authenticated user embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.
CVE-2025-8089	The Advanced iFrame plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'additional' parameter in version less than, or equal to, 2025.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary w in pages that will execute whenever a user accesses an injected page.
CVE-2025-53219	Cross-Site Request Forgery (CSRF) vulnerability in pl4g4 WP-Database-Optimizer-Tools allows Cross Site Request Forgery. This issue affects WP-Database-Optimize from n/a through 0.2.
CVE-2025-54118	NamelessMC is a free, easy to use & powerful website software for Minecraft servers. Sensitive information disclosure in NamelessMC before 2.2.4 allows unauthen remote attacker to gain sensitive information such as absolute path of the source code via list parameter. This vulnerability is fixed in 2.2.4.
CVE-2025-51529	Incorrect Access Control in the AJAX endpoint functionality in jonkastonka Cookies and Content Security Policy plugin through version 2.29 allows remote attackers a denial of service (database server resource exhaustion) via unlimited database write operations to the wp_ajax_nopriv_cacsp_insert_consent_data endpoint.
CVE-2025-50434	A security issue has been identified in Appian Enterprise Business Process Management version 25.3. The vulnerability is related to incorrect access control, which certain conditions could allow unauthorized access to information.
CVE-2025-9134	A security vulnerability has been detected in AfterShip Package Tracker App up to 5.24.1 on Android. The affected element is an unknown function of the file AndroidManifest.xml of the component com.aftership.AfterShip. The manipulation leads to improper export of android application components. The attack must be out locally. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure and replied: "After reviewing your repor have confirmed that this vulnerability does indeed exist and we are actively working to fix it."
CVE-2025-52619	HCL BigFix SaaS Authentication Service is affected by a sensitive information disclosure. Under certain conditions, error messages disclose sensitive version inform about the underlying platform.
CVE-2025-51539	EzGED3 3.5.0 contains an unauthenticated arbitrary file read vulnerability due to improper access control and insufficient input validation in a script exposed via th interface. A remote attacker can supply a crafted path parameter to a PHP script to read arbitrary files from the filesystem. The script lacks both authentication che secure path handling, allowing directory traversal attacks (e.g., ../../../) to access sensitive files such as configuration files, database dumps, source code, and pass tokens. If phpMyAdmin is exposed, extracted credentials can be used for direct administrative access. In environments without such tools, attacker-controlled file r allow full database extraction by targeting raw MySQL data files. The vendor states that the issue is fixed in 3.5.72.27183.
CVE-2025-51540	EzGED3 3.5.0 stores user passwords using an insecure hashing scheme: md5(md5(password)). This hashing method is cryptographically weak and allows attackers perform efficient offline brute-force attacks if password hashes are disclosed. The lack of salting and use of a fast, outdated algorithm makes it feasible to recover credentials using precomputed tables or GPU-based cracking tools. The vendor states that the issue is fixed in 3.5.72.27183.
CVE-2025-9174	A vulnerability was determined in neurobin shc up to 4.0.3. This vulnerability affects the function make of the file src/shc.c of the component Filename Handler. Exe manipulation can lead to os command injection. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized.
CVE-	

2025-55584	TOTOLINK A3002R v4.0.0-B20230531.1404 was discovered to contain insecure credentials for the telnet service and root account.
CVE-2024-12575	The Poll Maker – Versus Polls, Anonymous Polls, Image Polls plugin for WordPress is vulnerable to Basic Information Exposure in all versions up to, and including, 5. the 'ays_finish_poll' AJAX action. This makes it possible for unauthenticated attackers to retrieve admin email information which is exposed in the poll response.
CVE-2025-9157	A vulnerability was determined in appneta tcpreplay up to 4.5.2-beta2. The impacted element is the function untrunc_packet of the file src/tcpedit/edit_packet.c of component tcprewrite. Executing manipulation can lead to use after free. It is possible to launch the attack on the local host. The exploit has been publicly disclose may be utilized. This patch is called 73008f261f1cdf7a1087dc8759115242696d35da. Applying a patch is advised to resolve this issue.
CVE-2025-7499	The BetterDocs – Advanced AI-Driven Documentation, FAQ & Knowledge Base Tool for Elementor & Gutenberg with Encyclopedia, AI Support, Instant Answers plug WordPress is vulnerable to unauthorized access of data due to a missing capability check on the get_response function in all versions up to and including 4.1.1. Thi possible for unauthenticated attackers to retrieve passwords for password-protected documents as well as the metadata of private and draft documents.
CVE-2025-52621	HCL BigFix SaaS Authentication Service is vulnerable to cache poisoning. The BigFix SaaS's HTTP responses were observed to include the Origin header. Its presen alongside an unvalidated reflection of the Origin header value introduces a potential for cache poisoning.
CVE-2025-49432	Missing Authorization vulnerability in FWDesign Ultimate Video Player allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Ulti Video Player: from n/a through 10.1.
CVE-2025-9102	A security vulnerability has been detected in 1&1 Mail & Media mail.com App 8.8.0 on Android. Affected is an unknown function of the file AndroidManifest.xml of t component com.mail.mobile.android.mail. The manipulation leads to improper export of android application components. It is possible to launch the attack on the 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.
CVE-2025-9100	A security flaw has been discovered in zhenfeng13 My-Blog 1.0.0. This vulnerability affects unknown code of the file /blog/comment of the component Frontend Blo Comment Handler. The manipulation leads to authentication bypass by capture-replay. The attack can be initiated remotely. The exploit has been disclosed to the may be used.
CVE-2025-52338	An issue in the default configuration of the password reset function in LogicData eCommerce Framework v5.0.9.7000 allows attackers to bypass authentication and compromise user accounts via a bruteforce attack.
CVE-2025-9098	A vulnerability was determined in Elseplus File Recovery App 4.4.21 on Android. Affected by this issue is some unknown functionality of the file AndroidManifest.xm manipulation leads to improper export of android application components. The attack needs to be approached locally. The exploit has been disclosed to the public be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-9097	A vulnerability was found in Euro Information CIC banque et compte en ligne App 12.56.0 on Android. Affected by this vulnerability is an unknown functionality of t AndroidManifest.xml of the component com.cic_prod.bad. The manipulation leads to improper export of android application components. It is possible to launch the on the local host. 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 w
CVE-2025-51543	An issue was discovered in Cicool builder 3.4.4 allowing attackers to reset the administrator's password via the /administrator/auth/reset_password endpoint.
CVE-2025-9093	A security vulnerability has been detected in BuzzFeed App 2024.9 on Android. This affects an unknown part of the file AndroidManifest.xml of the component com.buzzfeed.android. The manipulation leads to improper export of android application components. The attack needs to be approached locally. The exploit has b disclosed to the public and may be used.
CVE-2025-50579	A CORS misconfiguration in Nginx Proxy Manager v2.12.3 allows unauthorized domains to access sensitive data, particularly JWT tokens, due to improper validatio Origin header. This misconfiguration enables attackers to intercept tokens using a simple browser script and exfiltrate them to a remote attacker-controlled server, potentially leading to unauthorized actions within the application.
CVE-2025-9136	A flaw has been found in libretro RetroArch 1.18.0/1.19.0/1.20.0. This affects the function filestream_vscanf of the file libretro-common/streams/file_stream.c. This manipulation causes out-of-bounds read. The attack needs to be launched locally. Upgrading to version 1.21.0 mitigates this issue. It is recommended to upgrade t affected component.
CVE-2025-9135	A vulnerability was detected in Verkehrsauskunft Österreich SmartRide, cleVVVer and BusBahnBim up to 12.1.1(258). The impacted element is an unknown functio file AndroidManifest.xml. The manipulation results in improper export of android application components. The attack must be initiated from a local position. The ex now public and may be used. Upgrading to version 12.1.2(259) is sufficient to resolve this issue. Upgrading the affected component is recommended.
CVE-2025-41689	An unauthenticated remote attacker can grant access without password protection to the affected device. This enables the unprotected read-only access to the sto measurement data.
CVE-2025-54989	Firebird is a relational database. Prior to versions 3.0.13, 4.0.6, and 5.0.3, there is an XDR message parsing NULL pointer dereference denial-of-service vulnerabilit Firebird. This specific flaw exists within the parsing of xdr message from client. It leads to NULL pointer dereference and DoS. This issue has been patched in versio 4.0.6, and 5.0.3.
CVE-2025-8464	The Drag and Drop Multiple File Upload for Contact Form 7 plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.3.9.0 via wpcf7_guest_user_id cookie. This makes it possible for unauthenticated attackers to upload and delete files outside of the originally intended directory. The impact vulnerability is limited, as file types are validated and only safe ones can be uploaded, while deletion is limited to the plugin's uploads folder.
CVE-2025-9175	A vulnerability was identified in neurobin shc up to 4.0.3. This issue affects the function make of the file src/shc.c. The manipulation leads to stack-based buffer ove The attack can only be performed from a local environment. The exploit is publicly available and might be used.
CVE-2025-54667	Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Saad Iqbal myCred allows Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditio issue affects myCred: from n/a through 2.9.4.3.
CVE-2025-48861	A vulnerability in the Task API endpoint of the ctrlX OS setup mechanism allowed a remote, unauthenticated attacker to access and extract internal application data, including potential debug logs and the version of installed apps.
CVE-	A vulnerability was found in code-projects Hostel Management System 1.0. Affected by this vulnerability is an unknown functionality of the file hostel_manage.exe

2025-8962	component Login Form. The manipulation of the argument uname leads to stack-based buffer overflow. Local access is required to approach this attack. The exploi been disclosed to the public and may be used.
CVE-2025-8964	A vulnerability was identified in code-projects Hostel Management System 1.0. This affects an unknown part of the file hostel_manage.exe of the component Login. manipulation leads to improper authentication. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used.
CVE-2025-9001	A vulnerability was determined in LemonOS up to nightly-2024-07-12 on LemonOS. Affected by this issue is the function HTTPGet of the file /Applications/Steal/mai the component HTTP Client. The manipulation of the argument chunkSize leads to stack-based buffer overflow. The attack may be launched remotely. The exploit h disclosed to the public and may be used.
CVE-2025-54739	Missing Authorization vulnerability in POSIMYTH Nexter Blocks allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Nexter Blo n/a through 4.5.4.
CVE-2025-54736	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in NordicMade Savoy allows Retrieve Embedded Sensitive Data. This issu Savoy: from n/a through 3.0.8.
CVE-2025-54730	Missing Authorization vulnerability in PARETO Digital Embedder for Google Reviews allows Accessing Functionality Not Properly Constrained by ACLs. This issue affe Embedder for Google Reviews: from n/a through 1.7.3.
CVE-2025-33142	IBM WebSphere Application Server 8.5 and 9.0 could provide weaker than expected security for TLS connections.
CVE-2025-54500	An HTTP/2 implementation flaw allows a denial-of-service (DoS) that uses malformed HTTP/2 control frames in order to break the max concurrent streams limit (HT MadeYouReset Attack). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.
CVE-2025-54791	OMERO.web provides a web based client and plugin infrastructure. Prior to version 5.29.2, if an error occurred when resetting a user's password using the Forgot P option in OMERO.web, the error message displayed on the Web page can disclose information about the user. This issue has been patched in version 5.29.2. A wor involves disabling the Forgot password option in OMERO.web using the omero.web.show_forgot_password configuration property.
CVE-2025-36047	IBM WebSphere Application Server Liberty 18.0.0.2 through 25.0.0.8 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote at could exploit this vulnerability to cause the server to consume memory resources.
CVE-2025-20219	A vulnerability in the implementation of access control rules for loopback interfaces in Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to send traffic that should have been blocked to a loopback interface. This vulnerability is due to improper enforcement of access control rules for loopback interfaces. An attacker could exploit this vulnerability by sending traffic to a loopb interface on an affected device. A successful exploit could allow the attacker to bypass configured access control rules and send traffic that should have bee to a loopback interface on the device.
CVE-2025-54691	Authorization Bypass Through User-Controlled Key vulnerability in Stylemix Motors allows Exploiting Incorrectly Configured Access Control Security Levels. This issu Motors: from n/a through 1.4.80.
CVE-2023-43694	An issue was discovered in Malwarebytes 4.6.14.326 and before and 5.1.5.116 and before (and Nebula 2020-10-21 and later). An Out of bounds read in several disassembling utilities causes stability issues and denial of service.
CVE-2025-5819	An issue has been discovered in GitLab CE/EE affecting all versions from 15.7 before 17.11.6, 18.0 before 18.0.4, and 18.1 before 18.1.2 that could have allowed authenticated users with developer access to obtain ID tokens for protected branches under certain circumstances.
CVE-2025-54715	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Dmitry V. (CEO of "UKR Solution") Barcode Scanner with Inventory & Manager allows Path Traversal. This issue affects Barcode Scanner with Inventory & Order Manager: from n/a through 1.9.0.
CVE-2025-20218	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, remote attacke retrieve sensitive information from an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sendin crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to retrieve sensitive information from t affected device. To exploit this vulnerability, the attacker must have valid administrative credentials.
CVE-2025-20306	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, remote attacke Administrator-level privileges to execute arbitrary commands on the underlying operating system. This vulnerability is due to insufficient input validation of certain request parameters that are sent to the web-based management interface. An attacker could exploit this vulnerability by authenticating to the interface and sendi crafted HTTP request to an affected device. A successful exploit could allow the attacker to execute commands as the root user on the affected device. To ex vulnerability, an attacker would need Administrator-level credentials.
CVE-2025-31988	HCL Digital Experience is susceptible to cross site scripting (XSS) in an administrative UI with restricted access.
CVE-2025-51488	A stored cross-site scripting (XSS) vulnerability in the Create Admin function of MoonShine v3.12.3 allows attackers to execute arbitrary web scripts or HTML via inj crafted payload into the Name parameter.
CVE-2025-51510	MoonShine v3.12.5 was discovered to contain a SQL injection vulnerability via the Data parameter under the Blog module.
CVE-2025-38745	Dell OpenManage Enterprise, versions 3.10, 4.0, 4.1, and 4.2, contains an Insertion of Sensitive Information into Log File vulnerability in the Backup and Restore. A privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.

CVE-2025-31987	HCL Connections Docs may mishandle validation of certain uploaded documents leading to denial of service due to resource exhaustion.
CVE-2025-8675	Server-Side Request Forgery (SSRF) vulnerability in Drupal AI SEO Link Advisor allows Server Side Request Forgery.This issue affects AI SEO Link Advisor: from 0.0. 1.0.6.
CVE-2025-54681	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CRM Perks Connector for Gravity Forms and Google Sheets allows Phishing. This issue affects Co for Gravity Forms and Google Sheets: from n/a through 1.2.4.
CVE-2025-51489	An arbitrary file upload vulnerability in MoonShine v3.12.4 allows attackers to execute arbitrary code via uploading a crafted SVG file.
CVE-2025-9020	A vulnerability was found in PX4 PX4-Autopilot up to 1.15.4. This issue affects the function MavlinkReceiver::handle_message_serial_control of the file src/modules/mavlink/mavlink_receiver.cpp of the component Mavlink Shell Closing Handler. The manipulation of the argument _mavlink_shell leads to use after fre attack has to be approached locally. The complexity of an attack is rather high. The exploitation is known to be difficult. The identifier of the patch is 4395d4f00c49b888f030f5b43e2a779f1fa78708. It is recommended to apply a patch to fix this issue.
CVE-2025-51487	A stored cross-site scripting (XSS) vulnerability in the Create Article function of MoonShine v3.12.3 allows attackers to execute arbitrary web scripts or HTML via inj crafted payload into the Link parameter.
CVE-2025-8080	The Alobaidi Captcha plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin settings in all versions up to, and including, 1.0.3 due to insuff input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web s pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disab
CVE-2025-8783	The Contact Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' parameter in all versions up to, and including, 8.6.5 due to insu input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages t execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.
CVE-2025-8891	The OceanWP theme for WordPress is vulnerable to Cross-Site Request Forgery in versions 4.0.9 to 4.1.1. This is due to missing or incorrect nonce validation on the oceanwp_notice_button_click() function. This makes it possible for unauthenticated attackers to install the Ocean Extra plugin via a forged request granted they ca site administrator into performing an action such as clicking on a link.
CVE-2025-20135	A vulnerability in the DHCP client functionality of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) could allow an unauthenticated, adjacent attacker to exhaust available memory. This vulnerability is due to improper validation of incoming DHCP packets. An atta exploit this vulnerability by repeatedly sending crafted DHCPv4 packets to an affected device. A successful exploit could allow the attacker to exhaust available me which would affect availability of services and prevent new processes from starting, resulting in a Denial of Service (DoS) condition that would require a manual reb Note: On Cisco Secure FTD Software, this vulnerability does not affect management interfaces.
CVE-2025-8491	The Easy restaurant menu manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.2. This is due to missi incorrect nonce validation on the nsc_eprm_save_menu() function. This makes it possible for unauthenticated attackers to upload a menu file via a forged request they can trick a site administrator into performing an action such as clicking on a link.
CVE-2025-27847	In ESPEC North America Web Controller 3 before 3.3.8, /api/v4/auth/ users session privileges are not revoked on logout.
CVE-2025-50897	A vulnerability exists in riscv-boom SonicBOOM 1.2 (BOOMv1.2) processor implementation, where valid virtual-to-physical address translations configured with writ permissions (PTE_W) in SV39 mode may incorrectly trigger a Store/AMO access fault during store instructions (sd). This occurs despite the presence of proper page entries and valid memory access modes. The fault is reproducible when transitioning into virtual memory and attempting store operations in mapped kernel memo indicating a potential flaw in the MMU, PMP, or memory access enforcement logic. This may cause unexpected kernel panics or denial of service in systems using B
CVE-2025-4690	A regular expression used by AngularJS' linky https://docs.angularjs.org/api/ngSanitize/filter/linky filter to detect URLs in input text is vulnerable to super-linear run to backtracking. With a large carefully-crafted input, this can cause a Regular expression Denial of Service (ReDoS) https://owasp.org/www-community/attacks/Regular_expression_Denial_of_Service_-_ReDoS attack on the application. This issue affects all versions of AngularJS. Note: The AngularJS proje of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .
CVE-2025-20302	A vulnerability in the web-based management interface of Cisco Secure FMC Software could allow an authenticated, low-privileged, remote attacker to retrieve a g report from a different domain. This vulnerability is due to missing authorization checks. An attacker could exploit this vulnerability by directly accessing a generat file for a different domain that is managed on the same Cisco Secure FMC instance. A successful exploit could allow the attacker to access a previously run report f different domain, which could allow an attacker to read activity recorded in that domain.
CVE-2025-9139	A vulnerability was determined in Scada-LTS 2.7.8.1. Affected by this vulnerability is an unknown functionality of the file /Scada-LTS/dwr/call/plaincall/WatchListDw Executing manipulation can lead to information disclosure. The attack may be performed from a remote location. The exploit has been publicly disclosed and may utilized. The vendor explains: "[T]he risks of indicated vulnerabilities seem to be minimal as all scenarios likely require admin permissions. Moreover, regardless ou fixes those vulnerabilities - the overall risk change to the user due to malicious admin actions will not be lower."
CVE-2025-9094	A vulnerability was detected in ThingsBoard 4.1. This vulnerability affects unknown code of the component Add Gateway Handler. The manipulation leads to impro neutralization of special elements used in a template engine. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. T replies, that "[t]he fix will come within upcoming release (v4.2) and will be inherited by maintenance releases of LTS versions (starting 4.0)."
CVE-2025-8933	A vulnerability was identified in 1000 Projects Sales Management System 1.0. This issue affects some unknown processing of the file /superstore/admin/sales.php. manipulation of the argument ssalescat leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be
CVE-2025-9108	Affected is an unknown function of the component Login Page. The manipulation leads to improper restriction of rendered ui layers. It is possible to launch the atta remotely.
CVE-2025-27846	In ESPEC North America Web Controller 3 before 3.3.8, an attacker with physical access can gain elevated privileges because GRUB and the BIOS are unprotected.
CVE-	A vulnerability was determined in Portabilis i-Diario up to 1.5.0. This impacts an unknown function of the file /alunos/search_autocomplete. Executing manipulation

2025-9107	argument q can lead to cross site scripting. The attack may be performed from a remote location. The exploit has been publicly disclosed and may be utilized. The was contacted early about this disclosure but did not respond in any way.
CVE-2025-8934	A vulnerability has been found in 1000 Projects Sales Management System 1.0. Affected is an unknown function of the file /sales.php. The manipulation of the argu select2112 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.
CVE-2025-55673	When a guest user accesses a chart in Apache Superset, the API response from the /chart/data endpoint includes a query field in its payload. This field contains the underlying query, which improperly discloses database schema information, such as table names, to the low-privileged guest user. This issue affects Apache Super before 4.1.3. Users are recommended to upgrade to version 4.1.3, which fixes the issue.
CVE-2025-54705	Missing Authorization vulnerability in magepeopleteam WpEvently allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WpEve n/a through 4.4.6.
CVE-2025-54703	Cross-Site Request Forgery (CSRF) vulnerability in Prince Integrate Google Drive allows Cross Site Request Forgery. This issue affects Integrate Google Drive: from through 1.5.2.
CVE-2025-54702	Cross-Site Request Forgery (CSRF) vulnerability in motov.net Ebook Store allows Cross Site Request Forgery. This issue affects Ebook Store: from n/a through 5.801
CVE-2025-54694	Cross-Site Request Forgery (CSRF) vulnerability in bPlugins Button Block allows Cross Site Request Forgery. This issue affects Button Block: from n/a through 1.2.0.
CVE-2025-9039	We identified an issue in the Amazon ECS agent where, under certain conditions, an introspection server could be accessed off-host by another instance if the insta in the same security group or if their security groups allow incoming connections that include the port where the server is hosted. This issue does not affect instanc the option to allow off-host access to the introspection server is set to 'false'. This issue has been addressed in ECS agent version 1.97.1. We recommend upgradin latest version and ensuring any forked or derivative code is patched to incorporate the new fixes. If customers cannot update to the latest AMI, they can modify the EC2 security groups to restrict incoming access to the introspection server port (51678).
CVE-2025-54673	Cross-Site Request Forgery (CSRF) vulnerability in Ays Pro Chartify allows Cross Site Request Forgery. This issue affects Chartify: from n/a through 3.5.3.
CVE-2025-54672	Cross-Site Request Forgery (CSRF) vulnerability in Jordy Meow Photo Engine allows Cross Site Request Forgery. This issue affects Photo Engine: from n/a through 6.
CVE-2025-54671	Cross-Site Request Forgery (CSRF) vulnerability in bobbingwide oik allows Cross Site Request Forgery. This issue affects oik: from n/a through 4.15.2.
CVE-2025-49052	Missing Authorization vulnerability in Dariolee Netease Music allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Netease Mu n/a through 3.2.1.
CVE-2025-8357	The Media Library Assistant plugin for WordPress is vulnerable to arbitrary file deletion in the /wp-content/uploads directory due to insufficient file path validation a capability checking in the _process_mla_download_file function in all versions up to, and including, 3.27. This makes it possible for authenticated attackers, with Au access and above, to delete arbitrary files on the server from the /wp-content/uploads/ directory.
CVE-2025-6790	The Quiz and Survey Master (QSM) WordPress plugin before 10.2.3 does not have CSRF check in place when updating its settings, which could allow attackers to m logged in admin change them via a CSRF attack.
CVE-2025-54675	Cross-Site Request Forgery (CSRF) vulnerability in YITHEMES YITH WooCommerce Popup allows Cross Site Request Forgery. This issue affects YITH WooCommerce from n/a through 1.48.0.
CVE-2025-8091	The EventON Lite plugin for WordPress is vulnerable to Information Exposure in all versions less than, or equal to, 2.4.6 via the add_single_eventon and add_eventc shortcodes due to insufficient restrictions on which posts can be included. This makes it possible for unauthenticated attackers to extract data from password prote private, or draft posts that they should not have access to.
CVE-2025-8991	A vulnerability was identified in linlinjava litemall up to 1.8.0. Affected by this vulnerability is an unknown functionality of the file /admin/config/express of the comp Business Logic Handler. The manipulation of the argument litemall_express_freight_min leads to business logic errors. The attack can be launched remotely. The ex been disclosed to the public and may be used.
CVE-2025-8362	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal GoogleTag Manager allows Cross-Site Scripting (XSS).Th affects GoogleTag Manager: from 0.0.0 before 1.10.0.
CVE-2025-53347	Cross-Site Request Forgery (CSRF) vulnerability in Laborator Kalium allows Cross Site Request Forgery. This issue affects Kalium: from n/a through 3.18.3.
CVE-2025-54712	Missing Authorization vulnerability in hashthemes Easy Elementor Addons allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Elementor Addons: from n/a through 2.2.7.
CVE-2025-54728	Cross-Site Request Forgery (CSRF) vulnerability in CreativeMindsSolutions CM On Demand Search And Replace allows Cross Site Request Forgery. This issue affects Demand Search And Replace: from n/a through 1.5.2.
CVE-2025-54732	Cross-Site Request Forgery (CSRF) vulnerability in Shahjada WPDM – Premium Packages allows Cross Site Request Forgery. This issue affects WPDM – Premium Pac from n/a through 6.0.2.

CVE-2025-55710	Insertion of Sensitive Information Into Sent Data vulnerability in Steve Burge TaxoPress allows Retrieve Embedded Sensitive Data. This issue affects TaxoPress: fro through 3.37.2.
CVE-2025-55716	Missing Authorization vulnerability in VeronaLabs WP Statistics allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Statist n/a through 14.15.
CVE-2025-52620	HCL BigFix SaaS Authentication Service is affected by a Cross-Site Scripting (XSS) vulnerability. The image upload functionality inadequately validated the submitte format.
CVE-2025-52618	HCL BigFix SaaS Authentication Service is affected by a SQL injection vulnerability. The vulnerability allows potential attackers to manipulate SQL queries.
CVE-2025-8992	A vulnerability has been found in mtons mblog up to 3.5.0. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forge attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-8996	Missing Authorization vulnerability in Drupal Layout Builder Advanced Permissions allows Forceful Browsing.This issue affects Layout Builder Advanced Permissions 0.0.0 before 2.2.0.
CVE-2025-9017	A vulnerability has been found in PHPGurukul Zoo Management System 2.1. This vulnerability affects unknown code of the file /admin/add-foreigner-ticket.php. The manipulation of the argument visitorname leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may
CVE-2025-53341	Missing Authorization vulnerability in Themovation Stratus allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Stratus: from r through 4.2.5.
CVE-2025-53221	Missing Authorization vulnerability in codeablepress CodeablePress allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Codea from n/a through 1.0.0.
CVE-2025-8676	The B Slider- Gutenberg Slider Block for WP plugin for WordPress is vulnerable to Sensitive Information Exposure in versions less than, or equal to, 2.0.0 via the get_active_plugins function. This makes it possible for authenticated attackers, with subscriber-level access and above to extract sensitive data including installed information.
CVE-2025-52767	Cross-Site Request Forgery (CSRF) vulnerability in lisensee NetInsight Analytics Implementation Plugin allows Cross Site Request Forgery. This issue affects NetInsi Analytics Implementation Plugin: from n/a through 1.0.3.
CVE-2025-52769	Cross-Site Request Forgery (CSRF) vulnerability in flexostudio flexo-social-gallery allows Cross Site Request Forgery. This issue affects flexo-social-gallery: from n/a 1.0006.
CVE-2025-53343	Missing Authorization vulnerability in GoodLayers Modernize allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Modernize: f through 3.4.0.
CVE-2025-8680	The B Slider- Gutenberg Slider Block for WP plugin for WordPress is vulnerable to Server-Side Request Forgery in version less than, or equal to, 2.0.0 via the fs_api_ function. This makes it possible for authenticated attackers, with subscriber-level access and above to make web requests to arbitrary locations originating from th application which can be used to query and modify information from internal services.
CVE-2025-52712	Path Traversal vulnerability in BoldGrid Post and Page Builder by BoldGrid – Visual Drag and Drop Editor allows Path Traversal. This issue affects Post and Page Buil BoldGrid – Visual Drag and Drop Editor: from n/a through 1.27.8.
CVE-2023-5342	The Fedora Secure Boot CA certificate shipped with shim in Fedora was expired which could lead to old or invalid signed boot components being loaded.
CVE-2025-36581	Dell PowerEdge Platform version(s) 14G AMD BIOS v1.25.0 and prior, contain(s) an Access of Memory Location After End of Buffer vulnerability. A low privileged att local access could potentially exploit this vulnerability, leading to Information exposure.
CVE-2025-8013	The Quttera Web Malware Scanner plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 3.5.1.41 via the 'RunExte function. This makes it possible for authenticated attackers, with Administrator-level access and above, to make web requests to arbitrary locations originating fro application and can be used to query and modify information from internal services.
CVE-2025-9109	A security flaw has been discovered in Portabilis i-Diario up to 1.5.0. Affected by this vulnerability is an unknown functionality of the file /password/email of the com Password Recovery Endpoint. The manipulation results in observable response discrepancy. It is possible to launch the attack remotely. This attack is characterized complexity. The exploitation appears to be difficult. The exploit has been released to the public and may be exploited.
CVE-2025-9004	A vulnerability was found in mtons mblog up to 3.5.0. This issue affects some unknown processing of the file /settings/password. The manipulation leads to impro restriction of excessive authentication attempts. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be c The exploit has been disclosed to the public and may be used.
CVE-2025-8974	A vulnerability was determined in linlinjava litemall up to 1.8.0. Affected by this issue is some unknown functionality of the file litemall-wx-api/src/main/java/org/linlinjava/litemall/wx/util/JwtHelper.java of the component JSON Web Token Handler. The manipulation of the argument SECRET with the input Litemall-Token leads to hard-coded credentials. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be c The exploit has been disclosed to the public and may be used.
CVE-2024-49827	IBM Concert Software 1.0.0 through 1.1.0 is vulnerable to excessive data exposure, allowing attackers to access sensitive information without proper filtering.

CVE-2025-53859	NGINX Open Source and NGINX Plus have a vulnerability in the ngx_mail_smtp_module that might allow an unauthenticated attacker to over-read NGINX SMTP authentication process memory; as a result, the server side may leak arbitrary bytes sent in a request to the authentication server. This issue happens during the N SMTP authentication process and requires the attacker to make preparations against the target system to extract the leaked data. The issue affects NGINX only if (built with the ngx_mail_smtp_module, (2) the smtp_auth directive is configured with method "none," and (3) the authentication server returns the "Auth-Wait" resp header. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.
CVE-2025-31961	HCL Connections contains a broken access control vulnerability that may allow unauthorized user to update data in certain scenarios.
CVE-2025-9005	A vulnerability was determined in mtons mblog up to 3.5.0. Affected is an unknown function of the file /register. The manipulation leads to information exposure th error message. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been to the public and may be used.
CVE-2025-8927	A vulnerability was determined in mtons mblog up to 3.5.0. Affected by this issue is some unknown functionality of the file /email/send_code of the component Veri Code Handler. The manipulation of the argument email leads to improper restriction of excessive authentication attempts. The attack may be launched remotely. T complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used.
CVE-2025-9095	A flaw has been found in ExpressGateway express-gateway up to 1.16.10. This issue affects some unknown processing in the library lib/rest/routes/users.js of the c REST Endpoint. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-9147	A vulnerability has been found in jasonclark getsemantic up to 040c96eb8cf9947488bd01b8de99b607b0519f7d. The impacted element is an unknown function of t /index.php. The manipulation of the argument view leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed to the and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The was contacted early about this disclosure but did not respond in any way.
CVE-2025-8975	A vulnerability was identified in givanz Vvveb up to 1.0.5. This affects an unknown part of the file admin/template/content/edit.tpl. The manipulation of the argume leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.0.6 address this issue. The patch is named 84c11d69df8452dc378feecd17e2a62ac10dac66. It is recommended to upgrade the affected component.
CVE-2025-9138	A vulnerability was found in Scada-LTS 2.7.8.1. Affected is an unknown function of the file pointHierarchy/new/. Performing manipulation of the argument Title resu cross site scripting. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The vendor explains: "[T]he risks of indi vulnerabilities seem to be minimal as all scenarios likely require admin permissions. Moreover, regardless our team fixes those vulnerabilities - the overall risk cha user due to malicious admin actions will not be lower. An admin user - by definition - has full control over HTML and JS code that is delivered to users in regular syn panels. In other words - due to the design of the system it is not possible to limit the admin user to attack the users."
CVE-2025-9096	A vulnerability has been found in ExpressGateway express-gateway up to 1.16.10. Affected is an unknown function in the library lib/rest/routes/apps.js of the comp REST Endpoint. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-9101	A weakness has been identified in zhenfeng13 My-Blog up to 1.0.0. This issue affects some unknown processing of the file /admin/tags/save of the component Tag The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2025-9104	A flaw has been found in Portabilis i-Diario up to 1.5.0. The affected element is an unknown function of the file /planos-de-aulas-por-disciplina/ of the component Int Adicionais Page. This manipulation of the argument Parecer/Objeto de Conhecimento/Habilidades causes cross site scripting. Remote exploitation of the attack is p The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-9106	A vulnerability was found in Portabilis i-Diario up to 1.5.0. This affects an unknown function of the file /planos-de-ensino-por-disciplina/ of the component Informaçõ Adicionais Page. Performing manipulation of the argument Parecer/Conteúdos/Objetivos results in cross site scripting. The attack is possible to be carried out remo exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-9137	A vulnerability has been found in Scada-LTS 2.7.8.1. This impacts an unknown function of the file scheduled_events.shtm. Such manipulation of the argument alias cross site scripting. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The vendor explains: "[T]he risks of indica vulnerabilities seem to be minimal as all scenarios likely require admin permissions. Moreover, regardless our team fixes those vulnerabilities - the overall risk cha user due to malicious admin actions will not be lower. An admin user - by definition - has full control over HTML and JS code that is delivered to users in regular syn panels. In other words - due to the design of the system it is not possible to limit the admin user to attack the users."
CVE-2025-9143	A security flaw has been discovered in Scada-LTS 2.7.8.1. This affects an unknown part of the file mailing_lists.shtm. The manipulation of the argument name/userList/address results in cross site scripting. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.
CVE-2025-9144	A weakness has been identified in Scada-LTS 2.7.8.1. This vulnerability affects unknown code of the file publisher_edit.shtm. This manipulation of the argument Na causes cross site scripting. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.
CVE-2025-9145	A security vulnerability has been detected in Scada-LTS 2.7.8.1. This issue affects some unknown processing of the file view_edit.shtm of the component SVG File H Such manipulation of the argument backgroundImageMP leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed publicly be used.
CVE-2025-8976	A vulnerability has been found in givanz Vvveb up to 1.0.5. This vulnerability affects unknown code of the file /vadmin123/index.php?module=content/post&type=p component Endpoint. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be Upgrading to version 1.0.6 is able to address this issue. It is recommended to upgrade the affected component.
CVE-2025-9105	A vulnerability has been found in Portabilis i-Diario up to 1.5.0. The impacted element is an unknown function of the file /planos-de-ensino-por-areas-de-conhecime component Informações Adicionais Page. Such manipulation of the argument Parecer/Conteúdos/Objetivos leads to cross site scripting. The attack can be executed 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.
CVE-2025-9167	A vulnerability has been found in SolidInvoice up to 2.4.0. This vulnerability affects unknown code of the file /invoice/recurring of the component Recurring Invoice The manipulation of the argument client name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-9168	A vulnerability was found in SolidInvoice up to 2.4.0. This issue affects some unknown processing of the file /invoice of the component Invoice Creation Module. The manipulation of the argument Client Name results in cross site scripting. The attack may be launched remotely. The exploit has been made public and could be use vendor was contacted early about this disclosure but did not respond in any way.
CVE-	A security flaw has been discovered in SolidInvoice up to 2.4.0. The impacted element is an unknown function of the file /clients of the component Clients Module.

2025-9171	Performing manipulation of the argument Name results in cross site scripting. The attack is possible to be carried out remotely. The exploit has been released to th and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-9170	A vulnerability was identified in SolidInvoice up to 2.4.0. The affected element is an unknown function of the file /tax/rates of the component Tax Rates Module. Suc manipulation of the argument Name leads to cross site scripting. The attack can be executed remotely. The exploit is publicly available and might be used. The ver contacted early about this disclosure but did not respond in any way.
CVE-2025-9169	A vulnerability was determined in SolidInvoice up to 2.4.0. Impacted is an unknown function of the file /quotes of the component Quote Module. This manipulation c argument Name causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. The vendor v contacted early about this disclosure but did not respond in any way.
CVE-2025-9003	A vulnerability has been found in D-Link DIR-818LW 1.04. This vulnerability affects unknown code of the file /bsc_lan.php of the component DHCP Reserved Address The manipulation of the argument Name leads to cross site scripting. The attack can be initiated remotely. This vulnerability only affects products that are no longe supported by the maintainer.
CVE-2025-8961	A vulnerability was identified in LibTIFF 4.7.0. This issue affects the function May of the file tiffcrop.c of the component tiffcrop. The manipulation leads to memory corruption. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used.
CVE-2025-9165	A flaw has been found in LibTIFF 4.7.0. This affects the function _TIFFmallocExt/_TIFFCheckRealloc/TIFFHashSetNew/InitCCITTFax3 of the file tools/tiffcmp.c of the c tiffcmp. Executing manipulation can lead to memory leak. The attack is restricted to local execution. The exploit has been published and may be used. This patch i ed141286a37f6e5ddafb5069347ff5d587e7a4e0. It is best practice to apply a patch to resolve this issue.
CVE-2017-20199	A vulnerability was found in Buttercup buttercup-browser-extension up to 0.14.2. Affected by this vulnerability is an unknown functionality. The manipulation result improper access controls. The attack may be performed from a remote location. A high complexity level is associated with this attack. The exploitation appears to difficult. The exploit has been made public and could be used. Upgrading to version 1.0.1 addresses this issue. The patch is identified as 89. Upgrading the affected component is recommended. This vulnerability only affects products that are no longer supported by the maintainer.
CVE-2025-9019	A vulnerability has been found in tcpreplay 4.5.1. This vulnerability affects the function mask_cidr6 of the file cidr.c of the component tcpprep. The manipulation le heap-based buffer overflow. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit ha disclosed to the public and may be used. The researcher is able to reproduce this with the latest official release 4.5.1 and the current master branch. The code mai cannot reproduce this for 4.5.2-beta1. In his reply the maintainer explains that "[i]n that case, this is a duplicate that was fixed in 4.5.2."
CVE-2025-2498	An improper access control in Gitlab EE affecting all versions from 12.0 prior to 18.0.6, 18.1 prior to 18.1.4, and 18.2 prior to 18.2.2 that under certain conditions c allowed users to view assigned issues from restricted groups by bypassing IP restrictions.
CVE-2025-8713	PostgreSQL optimizer statistics allow a user to read sampled data within a view that the user cannot access. Separately, statistics allow a user to read sampled dat row security policy intended to hide. PostgreSQL maintains statistics for tables by sampling data available in columns; this data is consulted during the query planr process. Prior to this release, a user could craft a leaky operator that bypassed view access control lists (ACLs) and bypassed row security policies in partitioning or inheritance hierarchies. Reachable statistics data notably included histograms and most-common-values lists. CVE-2017-7484 and CVE-2019-10130 intended to clo class of vulnerability, but this gap remained. Versions before PostgreSQL 17.6, 16.10, 15.14, 14.19, and 13.22 are affected.
CVE-2025-36613	SupportAssist for Home PCs versions 4.6.3 and prior and SupportAssist for Business PCs versions 4.5.3 and prior, contain(s) an Incorrect Privilege Assignment vulne low privileged attacker with local access could potentially exploit this vulnerability, leading to unauthorized access.
CVE-2025-2988	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.0.0.0 through 6.1.2.7, 6.2.0.0 through 6.2.0.4, and 6.2.1.0 could disclose sensitive server information t unauthorized user that could aid in further attacks against the system.
CVE-2025-55285	@backstage/plugin-scaffolder-backend is the backend for the default Backstage software templates. Prior to version 2.1.1, duplicate logging of the input values in t fetch:template action in the Scaffolder meant that some of the secrets were not properly redacted. If ${{ secrets.x }} is not passed through to fetch:template ther impact. This issue has been resolved in 2.1.1 of the scaffolder-backend plugin. A workaround for this issue involves Template Authors removing the use of ${{ secr being used as an argument to fetch:template.
CVE-2025-9091	A security flaw has been discovered in Tenda AC20 16.03.08.12. Affected by this vulnerability is an unknown functionality of the file /etc_ro/shadow. The manipulat to hard-coded credentials. It is possible to launch the attack on the local host. The complexity of an attack is rather high. The exploitation appears to be difficult. Th has been disclosed to the public and may be used.
CVE-2025-8919	A vulnerability was determined in Portabilis i-Diario up to 1.6. Affected is an unknown function of the file /objetivos-de-aprendizagem-e-habilidades of the compone Page. The manipulation of the argument código/objetivo habilidade leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been d to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-8920	A vulnerability was identified in Portabilis i-Diario 1.6. Affected by this vulnerability is an unknown functionality of the file /dicionario-de-termos-bncc of the compon Dicionário de Termos BNCC Page. The manipulation of the argument Planos de ensino leads to cross site scripting. The attack can be launched remotely. The explo been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-9119	A vulnerability was determined in Netis WF2419 1.2.29433. This vulnerability affects unknown code of the file /index.htm of the component Wireless Settings Page. manipulation of the argument SSID with the input <img/src/onerror=prompt(8)> causes cross site scripting. Remote exploitation of the attack is possible. The expl been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-9103	A vulnerability was detected in ZenCart 2.1.0. Affected by this vulnerability is an unknown functionality of the component CKEditor. The manipulation leads to cross scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubte moment. The vendor declares this as "intended behavior, allowed for authorized administrators".
CVE-2025-8918	A vulnerability was found in Portabilis i-Educar up to 2.10. This issue affects some unknown processing of the file /intranet/educar_instituicao_cad.php of the compo Editar Page. The manipulation of the argument neighborhood name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclos public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2025-54234	ColdFusion versions 2025.1, 2023.13, 2021.19 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to limited file system r high-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs. Exploitation of this issue does not require interaction.
	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid panic in f2fs_evict_inode As syzbot [1] reported as below: R10: 00000000000001 0000000000000206 R12: 00007ffe17473450 R13: 00007f28b1c10854 R14: 000000000000dae5 R15: 00007ffe17474520 </TASK> ---[end trace 00000000000000 ========== BUG: KASAN: use-after-free in __list_del_entry_valid+0xa6/0x130 lib/list_debug.c:62 Read of size 8 at addr ffff88812d962278 by task syz-executor/564 CPU: 1 PID: 564 Comm: syz-executor Taint

CVE-2025-38577	6.1.129-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 02/12/2025 Call Trace: <TASK> __dump_stack+0x21/ lib/dump_stack.c:88 dump_stack_lvl+0xee/0x158 lib/dump_stack.c:106 print_address_description+0x71/0x210 mm/kasan/report.c:316 print_report+0x4a/0x60 mm/kasan/report.c:427 kasan_report+0x122/0x150 mm/kasan/report.c:531 __asan_report_load8_noabort+0x14/0x20 mm/kasan/report_generic.c:351 __list_del_entry_valid+0xa6/0x130 lib/list_debug.c:62 __list_del_entry include/linux/list.h:134 [inline] list_del_init include/linux/list.h:206 [inline] f2fs_inode_synced+0xf7/0x2e0 fs/f2fs/super.c:1531 f2fs_update_inode+0x74/0x1c40 fs/f2fs/inode.c:585 f2fs_update_inode_page+0x137/0x170 fs/f2fs/inode.c:703 f2fs_write_inode+0x4ec/0x770 fs/f2fs/inode.c:731 write_inode fs/fs-writeback.c:1460 [inline] __writeback_single_inode+0x4a0/0xab0 fs/fs-writeback.c:1677 writeback_single_inode+0x221/0x8b0 fs/fs-writeback.c:1733 sync_inode_metadata+0xb6/0x110 fs/fs-writeback.c:2789 f2fs_sync_inode_meta+0x16d/0x2a0 fs/f2fs/checkpoint.c:1159 block_operations fs/f2fs/checkpoint.c:1269 [inline] f2fs_write_checkpoint+0xca3/0x2100 fs/f2fs/checkpoint.c:1658 kill_f2fs_super+0x231/ fs/f2fs/super.c:4668 deactivate_locked_super+0x98/0x100 fs/super.c:332 deactivate_super+0xaf/0xe0 fs/super.c:363 cleanup_mnt+0x45f/0x4e0 fs/namespace.c:1 __cleanup_mnt+0x19/0x20 fs/namespace.c:1193 task_work_run+0x1c6/0x230 kernel/task_work.c:203 exit_task_work include/linux/task_work.h:39 [inline] do_exit+0x9fb/0x2410 kernel/exit.c:871 do_group_exit+0x210/0x2d0 kernel/exit.c:1021 __do_sys_exit_group kernel/exit.c:1032 [inline] __se_sys_exit_group kernel/exit.c:1030 [inline] __x64_sys_exit_group+0x3f/0x40 kernel/exit.c:1030 x64_sys_call+0x7b4/0x9a0 arch/x86/include/generated/asm/syscalls_64.h:232 do_sy arch/x86/entry/common.c:51 [inline] do_syscall_64+0x4c/0xa0 arch/x86/entry/common.c:81 entry_SYSCALL_64_after_hwframe+0x68/0xd2 RIP: 0033:0x7f28b1b8e Code: Unable to access opcode bytes at 0x7f28b1b8e13f. RSP: 002b:00007ffe174710a8 EFLAGS: 00000246 ORIG_RAX: 00000000000000e7 RAX: ffffffffffffffda RBX 00007f28b1c10879 RCX: 00007f28b1b8e169 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000001 RBP: 0000000000000002 R08: 00007ffe1746ee47 R09: 00007ffe17472360 R10: 0000000000000009 R11: 0000000000000246 R12: 00007ffe17472360 R13: 00007f28b1c10854 R14: 000000000 R15: 00007ffe17474520 </TASK> Allocated by task 569: kasan_save_stack mm/kasan/common.c:45 [inline] kasan_set_track+0x4b/0x70 mm/kasan/common.c:52 kasan_save_alloc_info+0x25/0x30 mm/kasan/generic.c:505 __kasan_slab_alloc+0x72/0x80 mm/kasan/common.c:328 kasan_slab_alloc include/linux/kasan.h:201 [i slab_post_alloc_hook+0x4f/0x2c0 mm/slab.h:737 slab_alloc_node mm/slub.c:3398 [inline] slab_alloc mm/slub.c:3406 [inline] __kmem_cache_alloc_lru mm/slub.c:34 [inline] kmem_cache_alloc_lru+0x104/0x220 mm/slub.c:3429 alloc_inode_sb include/linux/fs.h:3245 [inline] f2fs_alloc_inode+0x2d/0x340 fs/f2fs/super.c:1419 alloc fs/inode.c:261 [inline] iget_locked+0x186/0x880 fs/inode.c:1373 f2fs_iget+0x55/0x4c60 fs/f2fs/inode.c:483 f2fs_lookup+0x366/0xab0 fs/f2fs/namei.c:487 __lookup_slow+0x2a3/0x3d0 fs/namei.c:1690 lookup_slow+0x57/0x70 fs/namei.c:1707 walk_component+0x2e6/0x410 fs/namei ---truncated---
CVE-2025-38578	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid UAF in f2fs_sync_inode_meta() syzbot reported an UAF issue as below: [1] [2] [1] https://syzkaller.appspot.com/text?tag=CrashReport&x=16594c60580000 == BUG: KASAN: use-after-free in __list_del_entry_valid+0xa6/0x130 lib/list_debug.c:62 Read of size 8 at addr ffff888100567dc8 by task kworker/u4:0/8 CPU: 1 PID: 8 Comm: kworker/u4:0 Tainted: G 6.1.129-syzkaller-00017-g642656a36791 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 02/12/2025 Workqueue: write wb_workfn (flush-7:0) Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x151/0x1b7 lib/dump_stack.c:106 print_address_description mm/kasan/report.c:316 [inline] print_report+0x158/0x4e0 mm/kasan/report.c:427 kasan_report+0x13c/0x170 mm/kasan/report.c:531 __asan_report_load8_noabort+0x14/0x20 mm/kasan/report_generic.c:351 __list_del_entry_valid+0xa6/0x130 lib/list_debug.c:62 __list_del_entry include/linux/list.h: [inline] list_del_init include/linux/list.h:206 [inline] f2fs_inode_synced+0x100/0x2e0 fs/f2fs/super.c:1553 f2fs_update_inode+0x72/0x1c40 fs/f2fs/inode.c:588 f2fs_update_inode_page+0x135/0x170 fs/f2fs/inode.c:706 f2fs_write_inode+0x416/0x790 fs/f2fs/inode.c:734 write_inode fs/fs-writeback.c:1460 [inline] __writeback_single_inode+0x4cf/0xb80 fs/fs-writeback.c:1677 writeback_sb_inodes+0xb32/0x1910 fs/fs-writeback.c:1903 __writeback_inodes_wb+0x118/0x3f0 fs/f writeback.c:1974 wb_writeback+0x3da/0xa00 fs/fs-writeback.c:2081 wb_check_background_flush fs/fs-writeback.c:2151 [inline] wb_do_writeback fs/fs-writeback.c: [inline] wb_workfn+0xbba/0x1030 fs/fs-writeback.c:2266 process_one_work+0x73d/0xcb0 kernel/workqueue.c:2299 worker_thread+0xa60/0x1260 kernel/workque kthread+0x26d/0x300 kernel/kthread.c:386 ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:295 </TASK> Allocated by task 298: kasan_save_stack mm/kasan/common.c:45 [inline] kasan_set_track+0x4b/0x70 mm/kasan/common.c:52 kasan_save_alloc_info+0x1f/0x30 mm/kasan/generic.c:505 __kasan_slab_alloc+0x6c/0x80 mm/kasan/common.c:333 kasan_slab_alloc include/linux/kasan.h:202 [inline] slab_post_alloc_hook+0x53/0x2c0 mm/slab.h:768 slab_alloc_node mm/slub.c:3421 [inline] slab_alloc mm/slub.c:3431 [inline] __kmem_cache_alloc_lru mm/slub.c:3438 [inline] kmem_cache_alloc_lru+0x102/0x270 mm/slub.c:3454 alloc_inode_sb include/linux/fs.h:3255 [inline] f2fs_alloc_inode+0x2d/0x350 fs/f2fs/super.c:1437 alloc_inode fs/inode.c:261 [inline] iget_locked+0x fs/inode.c:1373 f2fs_iget+0x55/0x4ca0 fs/f2fs/inode.c:486 f2fs_lookup+0x3c1/0xb50 fs/f2fs/namei.c:484 __lookup_slow+0x2b9/0x3e0 fs/namei.c:1689 lookup_slow+0x5a/0x80 fs/namei.c:1706 walk_component+0x2e7/0x410 fs/namei.c:1997 lookup_last fs/namei.c:2454 [inline] path_lookupat+0x16d/0x450 fs/nam filename_lookup+0x251/0x600 fs/namei.c:2507 vfs_statx+0x107/0x4b0 fs/stat.c:229 vfs_fstatat fs/stat.c:267 [inline] vfs_lstat include/linux/fs.h:3434 [inline] __do_sys_newlstat fs/stat.c:423 [inline] __se_sys_newlstat+0xda/0x7c0 fs/stat.c:417 __x64_sys_newlstat+0x5b/0x70 fs/stat.c:417 x64_sys_call+0x52/0x9a0 arch/x86/include/generated/asm/syscalls_64.h:7 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x3b/0x80 arch/x86/entry/common.c:81 entry_SYSCALL_64_after_hwframe+0x68/0xd2 Freed by task 0: kasan_save_stack mm/kasan/common.c:45 [inline] kasan_set_track+0x4b/0x70 mm/kasan/commor kasan_save_free_info+0x2b/0x40 mm/kasan/generic.c:516 ____kasan_slab_free+0x131/0x180 mm/kasan/common.c:241 __kasan_slab_free+0x11/0x20 mm/kasan/common.c:249 kasan_slab_free include/linux/kasan.h:178 [inline] slab_free_hook mm/slub.c:1745 [inline] slab_free_freelist_hook mm/slub.c:1771 [inline mm/slub.c:3686 [inline] kmem_cache_free+0x ---truncated---
CVE-2025-54475	A SQL injection vulnerability in the JS Jobs plugin versions 1.3.2-1.4.4 for Joomla allows low-privilege users to execute arbitrary SQL commands.
CVE-2025-38576	In the Linux kernel, the following vulnerability has been resolved: powerpc/eeh: Make EEH driver device hotplug safe Multiple race conditions existed between the h hotplug driver and the EEH driver, leading to a variety of kernel oopses of the same general nature: <pcie device unplug> <eeh driver trigger> <hotplug removal <pcie tree reconfiguration> <eeh recovery next step> <oops in EEH driver bus iteration loop> A second class of oops is also seen when the underlying bus disapp during device recovery. Refactor the EEH module to be PCI rescan and remove safe. Also clean up a few minor formatting / readability issues.
CVE-2025-38579	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix KMSAN uninit-value in extent_info usage KMSAN reported a use of uninitialized value in `__is_extent_mergeable()` and `__is_back_mergeable()` via the read extent tree path. The root cause is that `get_read_extent_info()` only initializes three fields (`f `blk`, `len`) of `struct extent_info`, leaving the remaining fields uninitialized. This leads to undefined behavior when those fields are accessed later, especially duri merging. Fix it by zero-initializing the `extent_info` struct before population.
CVE-2025-38573	In the Linux kernel, the following vulnerability has been resolved: spi: cs42l43: Property entry should be a null-terminated array The software node does not specify of property entries, so the array must be null-terminated. When unterminated, this can lead to a fault in the downstream cs35l56 amplifier driver, because the nod walks off the end of the array into unknown memory.
CVE-2025-38572	In the Linux kernel, the following vulnerability has been resolved: ipv6: reject malicious packets in ipv6_gso_segment() syzbot was able to craft a packet with very l extension headers leading to an overflow of skb->transport_header. This 16bit field has a limited range. Add skb_reset_transport_header_careful() helper and use i ipv6_gso_segment() WARNING: CPU: 0 PID: 5871 at ./include/linux/skbuff.h:3032 skb_reset_transport_header include/linux/skbuff.h:3032 [inline] WARNING: CPU: 0 at ./include/linux/skbuff.h:3032 ipv6_gso_segment+0x15e2/0x21e0 net/ipv6/ip6_offload.c:151 Modules linked in: CPU: 0 UID: 0 PID: 5871 Comm: syz-executor211 N tainted 6.16.0-rc6-syzkaller-g7abc678e3084 #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 07/12/2025 0010:skb_reset_transport_header include/linux/skbuff.h:3032 [inline] RIP: 0010:ipv6_gso_segment+0x15e2/0x21e0 net/ipv6/ip6_offload.c:151 Call Trace: <TASK> skb_mac_gso_segment+0x31c/0x640 net/core/gso.c:53 nsh_gso_segment+0x54a/0xe10 net/nsh/nsh.c:110 skb_mac_gso_segment+0x31c/0x640 net/core/gso.c:53 __skb_gso_segment+0x342/0x510 net/core/gso.c:124 skb_gso_segment include/net/gso.h:83 [inline] validate_xmit_skb+0x857/0x11b0 net/core/dev.c:3950 validate_xmit_skb_list+0x84/0x120 net/core/dev.c:4000 sch_direct_xmit+0xd3/0x4b0 net/sched/sch_generic.c:329 __dev_xmit_skb net/core/dev.c:4102 [inline] __dev_queue_xmit+0x17b6/0x3a70 net/core/dev.c:4679
CVE-2025-38571	In the Linux kernel, the following vulnerability has been resolved: sunrpc: fix client side handling of tls alerts A security exploit was discovered in NFS over TLS in tls_alert_recv due to its assumption that there is valid data in the msghdr's iterator's kvec. Instead, this patch proposes the rework how control messages are setup by sock_recvmsg(). If no control message structure is setup, kTLS layer will read and process TLS data record types. As soon as it encounters a TLS control messag return an error. At that point, NFS can setup a kvec backed control buffer and read in the control message such as a TLS alert. Scott found that a msg iterator can a the kvec pointer as a part of the copy process thus we need to revert the iterator before calling into the tls_alert_recv.

CVE-2025-38570	In the Linux kernel, the following vulnerability has been resolved: eth: fbnic: unlink NAPIs from queues on error to open CI hit a UaF in fbnic in the AF_XDP portion o queues.py test. The UaF is in the __sk_mark_napi_id_once() call in xsk_bind(), NAPI has been freed. Looks like the device failed to open earlier, and we lack clearing pointer from the queue.
CVE-2025-38574	In the Linux kernel, the following vulnerability has been resolved: pptp: ensure minimal skb length in pptp_xmit() Commit aabc6596ffb3 ("net: ppp: Add bound che skb data on ppp_sync_txmung") fixed ppp_sync_txmunge() We need a similar fix in pptp_xmit(), otherwise we might read uninit data as reported by syzbot. BUG: K uninit-value in pptp_xmit+0xc34/0x2720 drivers/net/ppp/pptp.c:193 pptp_xmit+0xc34/0x2720 drivers/net/ppp/pptp.c:193 ppp_channel_bridge_input drivers/net/ppp/ppp_generic.c:2290 [inline] ppp_input+0x1d6/0xe60 drivers/net/ppp/ppp_generic.c:2314 pppoe_rcv_core+0x1e8/0x760 drivers/net/ppp/pppoe.c:37 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 pppoe_sendmsg+0x15d/0xcb0 drivers/net/ppp/pppoe.c:904 sock_sendmsg_nosec net/socket.c:712 [inline] __sock_sendmsg+0x330/0x3d0 net/socket.c:727 ____sys_sendmsg+0x893/0xd80 net/socket.c:2566 ___sys_sendmsg+0x271/0x3b0 net/socket.c:2620 __sys_sendmmsg+0x2d9/0x7c0 net/socket.c:2709
CVE-2025-38583	In the Linux kernel, the following vulnerability has been resolved: clk: xilinx: vcu: unregister pll_post only if registered correctly If registration of pll_post is failed, it to NULL or ERR, unregistering same will fail with following call trace: Unable to handle kernel NULL pointer dereference at virtual address 008 pc : clk_hw_unregister+0xc/0x20 lr : clk_hw_unregister_fixed_factor+0x18/0x30 sp : ffff800011923850 ... Call trace: clk_hw_unregister+0xc/0x20 clk_hw_unregister_fixed_factor+0x18/0x30 xvcu_unregister_clock_provider+0xcc/0xf4 [xlnx_vcu] xvcu_probe+0x2bc/0x53c [xlnx_vcu]
CVE-2025-38580	In the Linux kernel, the following vulnerability has been resolved: ext4: fix inode use after free in ext4_end_io_rsv_work() In ext4_io_end_defer_completion(), check >list_vec is empty to avoid adding an io_end that requires no conversion to the i_rsv_conversion_list, which in turn prevents starting an unnecessary worker. An ext4_emergency_state() check is also added to avoid attempting to abort the journal in an emergency state. Additionally, ext4_put_io_end_defer() is refactored to c ext4_io_end_defer_completion() directly instead of being open-coded. This also prevents starting an unnecessary worker when EXT4_IO_END_FAILED is set but data_err=abort is not enabled. This ensures that the check in ext4_put_io_end_defer() is consistent with the check in ext4_end_bio(). Otherwise, we might add an i the i_rsv_conversion_list and then call ext4_finish_bio(), after which the inode could be freed before ext4_end_io_rsv_work() is called, triggering a use-after-free issu
CVE-2025-38581	In the Linux kernel, the following vulnerability has been resolved: crypto: ccp - Fix crash when rebind ccp device for ccp.ko When CONFIG_CRYPTO_DEV_CCP_DEBU enabled, rebinding the ccp device causes the following crash: $ echo '0000:0a:00.2' > /sys/bus/pci/drivers/ccp/unbind $ echo '0000:0a:00.2' > /sys/bus/pci/drivers/ 204.976930] BUG: kernel NULL pointer dereference, address: 0000000000000098 [204.978026] #PF: supervisor write access in kernel mode [204.979126] #PF: error_code(0x0002) - not-present page [204.980226] PGD 0 P4D 0 [204.981317] Oops: Oops: 0002 [#1] SMP NOPTI ... [204.997852] Call Trace: [204.999074] <T 205.000297] start_creating+0x9f/0x1c0 [205.001533] debugfs_create_dir+0x1f/0x170 [205.002769] ? srso_return_thunk+0x5/0x5f [205.004000] ccp5_debugfs_setup+0x87/0x170 [ccp] [205.005241] ccp5_init+0x8b2/0x960 [ccp] [205.006469] ccp_dev_init+0xd4/0x150 [ccp] [205.007709] sp_init+0x5f/0x8 205.008942] sp_pci_probe+0x283/0x2e0 [ccp] [205.010165] ? srso_return_thunk+0x5/0x5f [205.011376] local_pci_probe+0x4f/0xb0 [205.012584] pci_device_probe+0xdb/0x230 [205.013810] really_probe+0xed/0x380 [205.015024] __driver_probe_device+0x7e/0x160 [205.016240] device_driver_attach+0x 205.017457] bind_store+0x7c/0xb0 [205.018663] drv_attr_store+0x28/0x40 [205.019868] sysfs_kf_write+0x5f/0x70 [205.021065] kernfs_fop_write_iter+0x145/ 205.022267] vfs_write+0x308/0x440 [205.023453] ksys_write+0x6d/0xe0 [205.024616] __x64_sys_write+0x1e/0x30 [205.025778] x64_sys_call+0x16ba/0x215(205.026942] do_syscall_64+0x56/0x1e0 [205.028108] entry_SYSCALL_64_after_hwframe+0x76/0x7e [205.029276] RIP: 0033:0x7fbc36f10104 [205.030420] Coc 48 c7 c0 ff ff ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 66 90 48 8d 05 e1 08 2e 00 8b 00 85 c0 75 13 b8 01 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 54 f3 c3 66 90 41 54 d4 53 48 89 f5 This patch sets ccp_debugfs_dir to NULL after destroying it in ccp5_debugfs_destroy, allowing the directory dentry to be recreated when rebinding t device. Tested on AMD Ryzen 7 1700X.
CVE-2025-38582	In the Linux kernel, the following vulnerability has been resolved: RDMA/hns: Fix double destruction of rsv_qp rsv_qp may be double destroyed in error flow, first in free_mr_init(), and then in hns_roce_exit(). Fix it by moving the free_mr_init() call into hns_roce_v2_init(). list_del corruption, ffff589732eb9b50->next is LIST_POISC (dead000000000100) WARNING: CPU: 8 PID: 1047115 at lib/list_debug.c:53 __list_del_entry_valid+0x148/0x240 ... Call trace: __list_del_entry_valid+0x148/0x240 hns_roce_qp_remove+0x4c/0x3f0 [hns_roce_hw_v2] hns_roce_v2_destroy_qp_common+0x1dc/0x5f4 [hns_roce_hw_v2] hns_roce_v2_destroy_qp+0x22c/0x46c [hns_roce_hw_v2] free_mr_exit+0x6c/0x120 [hns_roce_hw_v2] hns_roce_v2_exit+0x170/0x200 [hns_roce_hw_v2] hns_roce_exit+0x118/0x350 [hns_roce_hw_v2] __hns_roce_hw_v2_init_instance+0x1c8/0x304 [hns_roce_hw_v2] hns_roce_hw_v2_reset_notify_init+0x170/0x21c [hns_roce_hw_v2] hns_roce_hw_v2_reset_notify+0x6c/0x190 [hns_roce_hw_v2] hclge_notify_roce_client+0x6c/0x160 [hclge] hclge_reset_rebuild+0x150/0x5c0 [hclge] hclge_reset+0x10c/0x140 [hclge] hclge_reset_subtask+0x80/0x104 [hclge] hclge_reset_service_task+0x168/0x3ac [hclge] hclge_service_task+0x50/0x100 [hclge] process_one_work+0x250/0x9a0 worker_thread+0x324/0x990 kthread+0x190/0x210 ret_from_fork+0x10/0x18
CVE-2025-38568	In the Linux kernel, the following vulnerability has been resolved: net/sched: mqprio: fix stack out-of-bounds write in tc entry parsing TCA_MQPRIO_TC_ENTRY_INDE validated using NLA_POLICY_MAX(NLA_U32, TC_QOPT_MAX_QUEUE), which allows the value TC_QOPT_MAX_QUEUE (16). This leads to a 4-byte out-of-bounds stack the fp[] array, which only has room for 16 elements (0–15). Fix this by changing the policy to allow only up to TC_QOPT_MAX_QUEUE - 1.
CVE-2025-38584	In the Linux kernel, the following vulnerability has been resolved: padata: Fix pd UAF once and for all There is a race condition/UAF in padata_reorder that goes bac initial commit. A reference count is taken at the start of the process in padata_do_parallel, and released at the end in padata_serial_worker. This reference count is is) required for padata_replace to function correctly. If padata_replace is never called then there is no issue. In the function padata_reorder which serves as the cor padata, as soon as padata is added to queue->serial.list, and the associated spin lock released, that padata may be processed and the reference count on pd woul away. Fix this by getting the next padata before the squeue->serial lock is released. In order to make this possible, simplify padata_reorder by only calling it once t padata arrives.
CVE-2025-9180	'Same-origin policy bypass in the Graphics: Canvas2D component.' This vulnerability affects Firefox < 142, Firefox ESR < 115.27, Firefox ESR < 128.14, Firefox ESR Thunderbird < 142, Thunderbird < 128.14, and Thunderbird < 140.2.
CVE-2025-38585	In the Linux kernel, the following vulnerability has been resolved: staging: media: atomisp: Fix stack buffer overflow in gmin_get_var_int() When gmin_get_config_v efi.get_variable() and the EFI variable is larger than the expected buffer size, two behaviors combine to create a stack buffer overflow: 1. gmin_get_config_var() do return the proper error code when efi.get_variable() fails. It returns the stale 'ret' value from earlier operations instead of indicating the EFI failure. 2. When efi.get_ returns EFI_BUFFER_TOO_SMALL, it updates *out_len to the required buffer size but writes no data to the output buffer. However, due to bug #1, gmin_get_var_int(the call succeeded. The caller gmin_get_var_int() then performs: - Allocates val[CFG_VAR_NAME_MAX + 1] (65 bytes) on stack - Calls gmin_get_config_var(dev, is_g val, &len) with len=64 - If EFI variable is >64 bytes, efi.get_variable() sets len=required_size - Due to bug #1, thinks call succeeded with len=required_size - Execu val[len] = 0, writing past end of 65-byte stack buffer This creates a stack buffer overflow when EFI variables are larger than 64 bytes. Since EFI variables can be co by firmware or system configuration, this could potentially be exploited for code execution. Fix the bug by returning proper error codes from gmin_get_config_var() EFI status instead of stale 'ret' value. The gmin_get_var_int() function is called during device initialization for camera sensor configuration on Intel Bay Trail and Che platforms using the atomisp camera stack.
CVE-2025-38586	In the Linux kernel, the following vulnerability has been resolved: bpf, arm64: Fix fp initialization for exception boundary In the ARM64 BPF JIT when prog->aux- >exception_boundary is set for a BPF program, find_used_callee_regs() is not called because for a program acting as exception boundary, all callee saved registers saved. find_used_callee_regs() sets `ctx->fp_used = true;` when it sees FP being used in any of the instructions. For programs acting as exception boundary, ctx-> remains false even if frame pointer is used by the program and therefore, FP is not set-up for such programs in the prologue. This can cause the kernel to crash du pagefault. Fix it by setting ctx->fp_used = true for exception boundary programs as fp is always saved in such programs.
CVE-2025-38587	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix possible infinite loop in fib6_info_uses_dev() fib6_info_uses_dev() seems to rely on RCU w explicit protection. Like the prior fix in rt6_nlmsg_size(), we need to make sure fib6_del_route() or fib6_add_rt2node() have not removed the anchor from the list, or an infinite loop.
	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent infinite loop in rt6_nlmsg_size() While testing prior patch, I was able to trigger an in

CVE-2025-38588	in rt6_nlmsg_size() in the following place: list_for_each_entry_rcu(sibling, &f6i->fib6_siblings, fib6_siblings) { rt6_nh_nlmsg_size(sibling->fib6_nh, &nexthop_len); } because fib6_del_route() and fib6_add_rt2node() uses list_del_rcu(), which can confuse rcu readers, because they might no longer see the head of the list. Restart t f6i->fib6_nsiblings is zero.
CVE-2025-9179	An attacker was able to perform memory corruption in the GMP process which processes encrypted media. This process is also heavily sandboxed, but represents s different privileges from the content process. This vulnerability affects Firefox < 142, Firefox ESR < 115.27, Firefox ESR < 128.14, Firefox ESR < 140.2, Thunderbir Thunderbird < 128.14, and Thunderbird < 140.2.
CVE-2025-55303	Astro is a web framework for content-driven websites. In versions of astro before 5.13.2 and 4.16.18, the image optimization endpoint in projects deployed with on rendering allows images from unauthorized third-party domains to be served. On-demand rendered sites built with Astro include an /_image endpoint which returns optimized versions of images. A bug in impacted versions of astro allows an attacker to bypass the third-party domain restrictions by using a protocol-relative URL image source, e.g. /_image?href=//example.com/image.png. This vulnerability is fixed in 5.13.2 and 4.16.18.
CVE-2025-38589	In the Linux kernel, the following vulnerability has been resolved: neighbour: Fix null-ptr-deref in neigh_flush_dev(). kernel test robot reported null-ptr-deref in neigh_flush_dev(). [0] The cited commit introduced per-netdev neighbour list and converted neigh_flush_dev() to use it instead of the global hash table. One thing is that neigh_table_clear() calls neigh_ifdown() with NULL dev. Let's restore the hash table iteration. Note that IPv6 module is no longer unloadable, so neigh_table_ called only when IPv6 fails to initialise, which is unlikely to happen. [0]: IPv6: Attempt to unregister permanent protocol 136 IPv6: Attempt to unregister permanent 17 Oops: general protection fault, probably for non-canonical address 0xdfffffc00000001a0: 0000 [#1] SMP KASAN KASAN: null-ptr-deref in range [0x0000000000000 0x0000000000000d07] CPU: 1 UID: 0 PID: 1 Comm: systemd Tainted: G T 6.12.0-rc6-01246-gf7f52738637f #1 Tainted: [T]=RANDSTRUCT Hardware name: QEMU S PC (i440FX + PIIX, 1996), BIOS 1.16.2-debian-1.16.2-1 04/01/2014 RIP: 0010:neigh_flush_dev.llvm.6395807810224103582+0x52/0x570 Code: c1 e8 03 42 8a 04 3 85 15 05 00 00 31 c0 41 83 3e 0a 0f 94 c0 48 8d 1c c3 48 81 c3 f8 0c 00 00 48 89 d8 48 c1 e8 03 <42> 80 3c 38 00 74 08 48 89 df e8 f7 49 93 fe 4c 8b 3b 4d 85 0000:ffff88810026f408 EFLAGS: 00010206 RAX: 00000000000001a0 RBX: 0000000000000d00 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000 RDI: ffffffffc0631640 RBP: ffff88810026f470 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: 0000000000000000 R13: ffffffffc0625250 R14: ffffffffc0631640 R15: dffffc0000000000 FS: 00007f575cb83940(0000) GS:ffff8883aee00000(0000) knlGS:0000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f575db40008 CR3: 00000002bf936000 CR4: 00000000000406f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __neigh_ifdown.llvm.6395807810224103582+0x44/0x390 neigh_table_clear+0xb1/0x268 ndisc_cleanup+0x21/0x38 [ipv6] init_module+0x2f5/0x468 [ipv6] do_one_initcall+0x1ba/0x628 do_init_module+0x21a/0x530 load_module+0x2550/0x2ea0 __se_sys_finit_module+0x3d2/0x620 __x64_sys_finit_module+0x76/0x88 x64_sys_call+0x7ff/0xde8 do_syscall_64+0xfb/0x1e8 entry_SYSCALL_64_after_hwframe+0x67/0x6f RIP: 0033:0x7f575d6f2719 Code: 08 89 e8 5b 5d c3 66 2e 0f 1f 00 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d b7 06 0d 00 f7 d8 64 89 01 48 RSP: 002b:00007fff82a2a268 EFLAGS: 00000246 ORIG_RAX: 0000000000000139 RAX: ffffffffffffffda RBX: 0000557827b45310 RCX: 00007f575d6f2719 RDX: 0000000 RSI: 00007f575d584efd RDI: 0000000000000004 RBP: 00007f575d584efd R08: 0000000000000000 R09: 0000557827b47b00 R10: 0000000000000004 R11: 0000000000000246 R12: 0000000000020000 R13: 0000000000000000 R14: 0000557827b470e0 R15: 00007f575dbb4270 </TASK> Modules linked in: ipv6(+)
CVE-2025-38569	In the Linux kernel, the following vulnerability has been resolved: benet: fix BUG when creating VFs benet crashes as soon as SRIOV VFs are created: kernel BUG at mm/vmalloc.c:3457! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI CPU: 4 UID: 0 PID: 7408 Comm: test.sh Kdump: loaded Not tainted 6.16.0+ #1 PREEMPT(v [...] RIP: 0010:vunmap+0x5f/0x70 [...] Call Trace: <TASK> __iommu_dma_free+0xe8/0x1c0 be_cmd_set_mac_list+0x3fe/0x640 [be2net] be_cmd_set_mac+0xaf/0x [be2net] be_vf_eth_addr_config+0x19f/0x330 [be2net] be_vf_setup+0x4f7/0x990 [be2net] be_pci_sriov_configure+0x3a1/0x470 [be2net] sriov_numvfs_store+0x2 kernfs_fop_write_iter+0x354/0x530 vfs_write+0x9b9/0xf60 ksys_write+0xf3/0x1d0 do_syscall_64+0x8c/0x3d0 be_cmd_set_mac_list() calls dma_free_coherent() un spin_lock_bh. Fix it by freeing only after the lock has been released.
CVE-2025-38564	In the Linux kernel, the following vulnerability has been resolved: perf/core: Handle buffer mapping fail correctly in perf_mmap() After successful allocation of a buf successful attachment to an existing buffer perf_mmap() tries to map the buffer read only into the page table. If that fails, the already set up page table entries are but the other perf specific side effects of that failure are not handled. The calling code just cleans up the VMA and does not invoke perf_mmap_close(). This leaks re counts, corrupts user->vm accounting and also results in an unbalanced invocation of event::event_mapped(). Cure this by moving the event::event_mapped() invo before the map_range() call so that on map_range() failure perf_mmap_close() can be invoked without causing an unbalanced event::event_unmapped() call. perf_mmap_close() undoes the reference counts and eventually frees buffers.
CVE-2025-38567	In the Linux kernel, the following vulnerability has been resolved: nfsd: avoid ref leak in nfsd_open_local_fh() If two calls to nfsd_open_local_fh() race and both succ call nfsd_file_acquire_local(), they will both get an extra reference to the net to accompany the file reference stored in *pnf. One of them will fail to store (using xch file reference in *pnf and will drop that reference but WON'T drop the accompanying reference to the net. This leak means that when the nfs server is shut down it in nfsd_shutdown_net() waiting for &nn->nfsd_net_free_done. This patch adds the missing nfsd_net_put().
CVE-2025-38566	In the Linux kernel, the following vulnerability has been resolved: sunrpc: fix handling of server side tls alerts Scott Mayhew discovered a security exploit in NFS ov tls_alert_recv() due to its assumption it can read data from the msg iterator's kvec.. kTLS implementation splits TLS non-data record payload between the control m buffer (which includes the type such as TLS aler or TLS cipher change) and the rest of the payload (say TLS alert's level/description) which goes into the msg paylo This patch proposes to rework how control messages are setup and used by sock_recvmsg(). If no control message structure is setup, kTLS layer will read and proc data record types. As soon as it encounters a TLS control message, it would return an error. At that point, NFS can setup a kvec backed msg buffer and read in the message such as a TLS alert. Msg iterator can advance the kvec pointer as a part of the copy process thus we need to revert the iterator before calling into the tls_alert_recv.
CVE-2024-12573	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2025-24752 Reason: This candidate is a reservation duplicate of CVE-2025- Notes: All CVE users should reference CVE-2025-24752 instead of this candidate. All references and descriptions in this candidate have been removed to prevent a usage.
CVE-2025-55736	flaskBlog is a blog app built with Flask. In 2.8.0 and earlier, an arbitrary user can change his role to "admin", giving its relative privileges (e.g. delete users, posts, c etc.). The problem is in the routes/adminPanelUsers file.
CVE-2025-55735	flaskBlog is a blog app built with Flask. In 2.8.0 and earlier, when creating a post, there's no validation of the content of the post stored in the variable "postConten vulnerability arises when displaying the content of the post using the | safe filter, that tells the engine to not escape the rendered content. This can lead to a stored inside the content of the post. The code that causes the problem is in template/routes.html.
CVE-2011-10009	S40 CMS v0.4.2 contains a path traversal vulnerability in its index.php page handler. The p parameter is not properly sanitized, allowing attackers to traverse the fi and access arbitrary files outside the web root. This can be exploited remotely without authentication by appending traversal sequences and a null byte to bypass extension checks.
CVE-2025-55734	flaskBlog is a blog app built with Flask. In 2.8.0 and earlier, the code checks if the userRole is "admin" only when visiting the /admin page, but not when visiting its subroutes. Specifically, only the file routes/adminPanel.py checks the user role when a user is trying to access the admin page, but that control is not done for the routes/adminPanelComments.py and routes/adminPanelPosts.py. Thus, an unauthorized user can bypass the intended restrictions, leaking sensitive data and acces following pages: /admin/posts, /adminpanel/posts, /admin/comments, and /adminpanel/comments.
CVE-2025-9187	Memory safety bugs present in Firefox 141 and Thunderbird 141. Some of these bugs showed evidence of memory corruption and we presume that with enough ef of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 142 and Thunderbird < 142.

CVE-2025-43738	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.8, 2025.Q1.0 through 2025.Q1.15, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.1 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.19 allows a remote authenticated user to inject JavaScript code via _com_liferay_expando_web_portlet_ExpandoPortlet_displayType parameter.
CVE-2025-9186	Spoofing issue in the Address Bar component of Firefox Focus for Android. This vulnerability affects Firefox < 142.
CVE-2025-9185	Memory safety bugs present in Firefox ESR 115.26, Firefox ESR 128.13, Thunderbird ESR 128.13, Firefox ESR 140.1, Thunderbird ESR 140.1, Firefox 141 and Thund 141. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary This vulnerability affects Firefox < 142, Firefox ESR < 115.27, Firefox ESR < 128.14, Firefox ESR < 140.2, Thunderbird < 142, Thunderbird < 128.14, and Thunderb 140.2.
CVE-2025-9184	Memory safety bugs present in Firefox ESR 140.1, Thunderbird ESR 140.1, Firefox 141 and Thunderbird 141. Some of these bugs showed evidence of memory corr we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 142, Firefox ESR < 140.2, Thunderbird < 142, and Thunderbird < 140.2.
CVE-2025-9183	Spoofing issue in the Address Bar component. This vulnerability affects Firefox < 142 and Firefox ESR < 140.2.
CVE-2025-8904	Amazon EMR Secret Agent creates a keytab file containing Kerberos credentials. This file is stored in the /tmp/ directory. A user with access to this directory and ar account can potentially decrypt the keys and escalate to higher privileges. Users are advised to upgrade to Amazon EMR version 7.5 or higher. For Amazon EMR re between 6.10 and 7.4, we strongly recommend that you run the bootstrap script and RPM files with the fix provided in the location below.
CVE-2025-8782	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this car have been removed to prevent accidental usage.
CVE-2025-9182	'Denial-of-service due to out-of-memory in the Graphics: WebRender component.' This vulnerability affects Firefox < 142, Firefox ESR < 140.2, Thunderbird < 142, Thunderbird < 140.2.
CVE-2025-9181	Uninitialized memory in the JavaScript Engine component. This vulnerability affects Firefox < 142, Firefox ESR < 128.14, Firefox ESR < 140.2, Thunderbird < 142, Thunderbird < 128.14, and Thunderbird < 140.2.
CVE-2025-38554	In the Linux kernel, the following vulnerability has been resolved: mm: fix a UAF when vma->mm is freed after vma->vm_refcnt got dropped By inducing delays in places, Jann Horn created a reproducer for a hard to hit UAF issue that became possible after VMAs were allowed to be recycled by adding SLAB_TYPESAFE_BY_RCU cache. Race description is borrowed from Jann's discovery report: lock_vma_under_rcu() looks up a VMA locklessly with mas_walk() under rcu_read_lock(). At that p VMA may be concurrently freed, and it can be recycled by another process. vma_start_read() then increments the vma->vm_refcnt (if it is in an acceptable range), succeeds, vma_start_read() can return a recycled VMA. In this scenario where the VMA has been recycled, lock_vma_under_rcu() will then detect the mismatching pointer and drop the VMA through vma_end_read(), which calls vma_refcount_put(). vma_refcount_put() drops the refcount and then calls rcuwait_wake_up() using vma->vm_mm. This is wrong: It implicitly assumes that the caller is keeping the VMA's mm alive, but in this scenario the caller has no relation to the VMA's mm, so rcuwait_wake_up() can cause UAF. The diagram depicting the race: T1 T2 T3 == == == lock_vma_under_rcu mas_walk <VMA gets removed from mm> mmap <th VMA is reallocated> vma_start_read __refcount_inc_not_zero_limited_acquire munmap __vma_enter_locked refcount_add_not_zero vma_end_read vma_refcount_pu __refcount_dec_and_test rcuwait_wait_event <finish operation> rcuwait_wake_up [UAF] Note that rcuwait_wait_event() in T3 does not block because refcount was dropped by T1. At this point T3 can exit and free the mm causing UAF in T1. To avoid this we move vma->vm_mm verification into vma_start_read() and grab vma to stabilize it before vma_refcount_put() operation. [surenb@google.com: v3]
CVE-2025-38555	In the Linux kernel, the following vulnerability has been resolved: usb: gadget : fix use-after-free in composite_dev_cleanup() 1. In func configfs_composite_bind() - composite_os_desc_req_prepare(): if kmalloc fails, the pointer cdev->os_desc_req will be freed but not set to NULL. Then it will return a failure to the upper-level fu in func configfs_composite_bind() -> composite_dev_cleanup(): it will checks whether cdev->os_desc_req is NULL. If it is not NULL, it will attempt to use it.This will use-after-free issue. BUG: KASAN: use-after-free in composite_dev_cleanup+0xf4/0x2c0 Read of size 8 at addr 0000004827837a00 by task init/1 CPU: 10 PID: 1 Co Tainted: G O 5.10.97-oh #1 kasan_report+0x188/0x1cc __asan_load8+0xb4/0xbc composite_dev_cleanup+0xf4/0x2c0 configfs_composite_bind+0x210/0x7ac udc_bind_to_driver+0xb4/0x1ec usb_gadget_probe_driver+0xec/0x21c gadget_dev_desc_UDC_store+0x264/0x27c
CVE-2025-38556	In the Linux kernel, the following vulnerability has been resolved: HID: core: Harden s32ton() against conversion to 0 bits Testing by the syzbot fuzzer showed that core gets a shift-out-of-bounds exception when it tries to convert a 32-bit quantity to a 0-bit quantity. Ideally this should never occur, but there are buggy devices might have a report field with size set to zero; we shouldn't reject the report or the device just because of that. Instead, harden the s32ton() routine so that it retur reasonable result instead of crashing when it is called with the number of bits set to 0 -- the same as what snto32() does.
CVE-2025-38557	In the Linux kernel, the following vulnerability has been resolved: HID: apple: validate feature-report field count to prevent NULL pointer dereference A malicious H with quirk APPLE_MAGIC_BACKLIGHT can trigger a NULL pointer dereference whilst the power feature-report is toggled and sent to the device in apple_magic_backlight_report_set(). The power feature-report is expected to have two data fields, but if the descriptor declares one field then accessing field[1] an dereferencing it in apple_magic_backlight_report_set() becomes invalid since field[1] will be NULL. An example of a minimal descriptor which can cause the crash is something like the following where the report with ID 3 (power report) only references a single 1-byte field. When hid core parses the descriptor it will encounter th feature tag, allocate a hid_report (all members of field[] will be zeroed out), create field structure and populate it, increasing the maxfield to 1. The subsequent fiel access and dereference causes the crash. Usage Page (Vendor Defined 0xFF00) Usage (0x0F) Collection (Application) Report ID (1) Usage (0x01) Logical Minimum Maximum (255) Report Size (8) Report Count (1) Feature (Data,Var,Abs) Usage (0x02) Logical Maximum (32767) Report Size (16) Report Count (1) Feature (Data,V Report ID (3) Usage (0x03) Logical Minimum (0) Logical Maximum (1) Report Size (8) Report Count (1) Feature (Data,Var,Abs) End Collection Here we see the KASA when the kernel dereferences the NULL pointer and crashes: [15.164723] Oops: general protection fault, probably for non-canonical address 0xdffffc0000000006: SMP KASAN NOPTI [15.165691] KASAN: null-ptr-deref in range [0x0000000000000030-0x0000000000000037] [15.165691] CPU: 0 UID: 0 PID: 10 Comm: kworker/ tainted 6.15.0 #31 PREEMPT(voluntary) [15.165691] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.2-debian-1.16.2-1 04/01/2014 [15.165 0010:apple_magic_backlight_report_set+0xbf/0x210 [15.165691] Call Trace: [15.165691] <TASK> [15.165691] apple_probe+0x571/0xa20 [15.165691] hid_device_probe+0x2e2/0x6f0 [15.165691] really_probe+0x1ca/0x5c0 [15.165691] __driver_probe_device+0x24f/0x310 [15.165691] driver_probe_device+0x4 15.165691] __device_attach_driver+0x169/0x220 [15.165691] bus_for_each_drv+0x118/0x1b0 [15.165691] __device_attach+0x1d5/0x380 [15.165691] device_initial_probe+0x12/0x20 [15.165691] bus_probe_device+0x13d/0x180 [15.165691] device_add+0xd87/0x1510 [...] To fix this issue we should validate the of fields that the backlight and power reports have and if they do not have the required number of fields then bail.
	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: uvc: Initialize frame-based format color matching descriptor Fix NULL pointer crash i uvcg_framebased_make due to uninitialized color matching descriptor for frame-based format which was added in commit f5e7bdd34aca ("usb: gadget: uvc: Allow new color matching descriptors") that added handling for uncompressed and mjpeg format. Crash is seen when userspace configuration (via configfs) does not exp define the color matching descriptor. If color_matching is not found, config_group_find_item() returns NULL. The code then jumps to out_put_cm, where it calls config_item_put(color_matching);. If color_matching is NULL, this will dereference a null pointer, leading to a crash. [2.746440] Unable to handle kernel NULL point dereference at virtual address 000000000000008c [2.756273] Mem abort info: [2.760080] ESR = 0x0000000096000005 [2.764872] EC = 0x25: DABT (current E

CVE-2025-38558	bits [2.771068] SET = 0, FnV = 0 [2.771069] EA = 0, S1PTW = 0 [2.771070] FSC = 0x05: level 1 translation fault [2.771071] Data abort info: [2.771072] ISV = 0 0x00000005, ISS2 = 0x00000000 [2.771073] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [2.771074] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [2.771075] user p 4k pages, 39-bit VAs, pgdp=00000000a3e59000 [2.771077] [0000000000000008c] pgd=0000000000000000, p4d=0000000000000000, pud=0000000000000000 2.771081] Internal error: Oops: 0000000096000005 [#1] PREEMPT SMP [2.771084] Dumping ftrace buffer: [2.771085] (ftrace buffer empty) [2.771138] CPU: 7 PI Comm: ln Tainted: G W E 6.6.58-android15 [2.771139] Hardware name: Qualcomm Technologies, Inc. SunP QRD HDK (DT) [2.771140] pstate: 61400005 (nZCv da UAO -TCO +DIT -SSBS BTYPE=--) [2.771141] pc : __uvcg_fill_strm+0x198/0x2cc [2.771145] lr : __uvcg_iter_strm_cls+0xc8/0x17c [2.771146] sp : ffffffc08140bbb0 2.771146] x29: ffffffc08140bbb0 x28: ffffff803bc81380 x27: ffffff8023bbd250 [2.771147] x26: ffffff8023bbd250 x25: ffffff803c361348 x24: ffffff803d8e6768 [2.77 x23: 0000000000000004 x22: 0000000000000003 x21: ffffffc08140bc48 [2.771149] x20: 0000000000000000 x19: ffffffc08140bc48 x18: ffffffe9f8cf4a00 [2.7711 000000001bf64ec3 x16: 000000001bf64ec3 x15: ffffff8023bbd250 [2.771151] x14: 000000000000000f x13: 004c4b40000f4240 x12: 000a2c2a00051615 [2.771 0000000000000004f x10: ffffffe9f76b40ec x9 : ffffffe9f7e389d0 [2.771153] x8 : ffffff803d0d31ce x7 : 000f4240000a2c2a x6 : 0005161500028b0a [2.771154] x5 : ffffff803d0d31ce x4 : 0000000000000003 x3 : 0000000000000000 [2.771155] x2 : ffffffc08140bc50 x1 : ffffffc08140bc48 x0 : 0000000000000000 [2.771156] Ca 2.771157] __uvcg_fill_strm+0x198/0x2cc [2.771157] __uvcg_iter_strm_cls+0xc8/0x17c [2.771158] uvcg_streaming_class_allow_link+0x240/0x290 [2.771159] configfs_symlink+0x1f8/0x630 [2.771161] vfs_symlink+0x114/0x1a0 [2.771163] do_symlinkat+0x94/0x28c [2.771164] __arm64_sys_symlinkat+0x54/0x70 [2.7 invoke_syscall+0x58/0x114 [2.771166] el0_svc_common+0x80/0xe0 [2.771168] do_el0_svc+0x1c/0x28 [2.771169] el0_svc+0x3c/0x70 [2.771172] el0t_64_sync_handler+0x68/0xbc [2.771173] el0t_64_sync+0x1a8/0x1ac Initialize color matching descriptor for frame-based format to prevent NULL pointer crash mirroring the handling done for uncompressed and mjpeg formats.
CVE-2025-38559	In the Linux kernel, the following vulnerability has been resolved: platform/x86/intel/pmt: fix a crashlog NULL pointer access Usage of the intel_pmt_read() for binar requires a pcidev. The current use of the endpoint value is only valid for telemetry endpoint usage. Without the ep, the crashlog usage causes the following NULL p exception: BUG: kernel NULL pointer dereference, address: 0000000000000000 Oops: Oops: 0000 [#1] SMP NOPTI RIP: 0010:intel_pmt_read+0x3b/0x70 [pmt_clas Call Trace: <TASK> ? sysfs_kf_bin_read+0xc0/0xe0 kernfs_fop_read_iter+0xac/0x1a0 vfs_read+0x26d/0x350 ksys_read+0x6b/0xe0 __x64_sys_read+0x1d/0x30 x64_sys_call+0x1bc8/0x1d70 do_syscall_64+0x6d/0x110 Augment struct intel_pmt_entry with a pointer to the pcidev to avoid the NULL pointer exception.
CVE-2025-38560	In the Linux kernel, the following vulnerability has been resolved: x86/sev: Evict cache lines during SNP memory validation An SNP cache coherency vulnerability re cache line eviction mitigation when validating memory after a page state change to private. The specific mitigation is to touch the first and last byte of each 4K pa being validated. There is no need to perform the mitigation when performing a page state change to shared and rescinding validation. CPUID bit Fn8000001F_EBX[defines the COHERENCY_SFW_NO CPUID bit that, when set, indicates that the software mitigation for this vulnerability is not needed. Implement the mitigation and when validating memory (making it private) and the COHERENCY_SFW_NO bit is not set, indicating the SNP guest is vulnerable.
CVE-2025-38561	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix Preauh_HashValue race condition If client send multiple session setup requests to ksm Preauh_HashValue race condition could happen. There is no need to free sess->Preauh_HashValue at session setup phase. It can be freed together with session at connection termination phase.
CVE-2025-38562	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix null pointer dereference error in generate_encryptionkey If client send two session set krb5 authenticate to ksmbd, null pointer dereference error in generate_encryptionkey could happen. sess->Preauth_HashValue is set to NULL if session is valid. So skip generate encryption key if session is valid.
CVE-2025-38563	In the Linux kernel, the following vulnerability has been resolved: perf/core: Prevent VMA split of buffer mappings The perf mmap code is careful about mmap()'ing page with the ringbuffer and additionally the auxiliary buffer, when the event supports it. Once the first mapping is established, subsequent mapping have to use t offset and the same size in both cases. The reference counting for the ringbuffer and the auxiliary buffer depends on this being correct. Though perf does not preve related mapping is split via mmap(2), munmap(2) or mremap(2). A split of a VMA results in perf_mmap_open() calls, which take reference counts, but then the sub perf_mmap_close() calls are not longer fulfilling the offset and size checks. This leads to reference count leaks. As perf already has the requirement for subsequent to match the initial mapping, the obvious consequence is that VMA splits, caused by resizing of a mapping or partial unmapping, have to be prevented. Implement vm_operations_struct::may_split() callback and return unconditionally -EINVAL. That ensures that the mapping offsets and sizes cannot be changed after the fact. Remapping to a different fixed address with the same size is still possible as it takes the references for the new mapping and drops those of the old mapping.
CVE-2025-38591	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject narrower access to pointer ctx fields The following BPF program, simplified from a syz repro, causes a kernel warning: r0 = *(u8 *)(r1 + 169); exit; With pointer field sk being at offset 168 in __sk_buff. This access is detected as a narrower read in bpf_skb_is_valid_access because it doesn't match offsetof(struct __sk_buff, sk). It is therefore allowed and later proceeds to bpf_convert_ctx_access. Note that for t "is_narrower_load" case in the convert_ctx_accesses(), the insn->off is aligned, so the cnt may not be 0 because it matches the offsetof(struct __sk_buff, sk) in the bpf_convert_ctx_access. However, the target_size stays 0 and the verifier errors with a kernel warning: verifier bug: error during ctx access conversion(1) This patc that to return a proper "invalid bpf_context access off=X size=Y" error on the load instruction. The same issue affects multiple other fields in context structures tha narrow access. Some other non-affected fields (for sk_msg, sk_lookup, and sockopt) were also changed to use bpf_ctx_range_ptr for consistency. Note this syzkalle was reported in the "Closes" link below, which used to be about a different bug, fixed in commit fce7bd8e385a ("bpf/verifier: Handle BPF_LOAD_ACQ instructions in insn_def_regno()"). Because syzbot somehow confused the two bugs, the new crash and repro didn't get reported to the mailing list.
CVE-2025-38565	In the Linux kernel, the following vulnerability has been resolved: perf/core: Exit early on perf_mmap() fail When perf_mmap() fails to allocate a buffer, it still invok event_mapped() callback of the related event. On X86 this might increase the perf_rdpmc_allowed reference counter. But nothing undoes this as perf_mmap_close called in this case, which causes another reference count leak. Return early on failure to prevent that.
CVE-2025-38590	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Remove skb secpath if xfrm state is not found Hardware returns a unique identifier fo decrypted packet's xfrm state, this state is looked up in an xarray. However, the state might have been freed by the time of this lookup. Currently, if the state is no only a counter is incremented. The secpath (sp) extension on the skb is not removed, resulting in sp->len becoming 0. Subsequently, functions like __xfrm_policy_c attempt to access fields such as xfrm_input_state(skb)->xso.type (which dereferences sp->xvec[sp->len - 1]) without first validating sp->len. This leads to a crash dereferencing an invalid state pointer. This patch prevents the crash by explicitly removing the secpath extension from the skb if the xfrm state is not found after h decryption. This ensures downstream functions do not operate on a zero-length secpath. BUG: unable to handle page fault for address: ffffffff000002c8 #PF: super access in kernel mode #PF: error_code(0x0000) - not-present page PGD 282e067 P4D 282e067 PUD 0 Oops: Oops: 0000 [#1] SMP CPU: 12 UID: 0 PID: 0 Comm: sw Not tainted 6.15.0-rc7_for_upstream_min_debug_2025_05_27_22_44 #1 NONE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0-gf21b5a prebuilt.qemu.org 04/01/2014 RIP: 0010:__xfrm_policy_check+0x61a/0xa30 Code: b6 77 7f 83 e6 02 74 14 4d 8b af d8 00 00 00 41 0f b6 45 05 c1 e0 03 48 98 49 8b 45 00 83 e8 01 48 98 49 8b 44 c5 10 <0f> b6 80 c8 02 00 00 83 e0 0c 3c 04 0f 84 0c 02 00 00 31 ff 80 fa RSP: 0018:ffff88885fb04918 EFLAGS: 00010297 RAX ffffffff00000000 RBX: 0000000000000002 RCX: 0000000000000000 RDX: 0000000000000002 RSI: 0000000000000002 RDI: 0000000000000000 RBP: ffffffff8311a 0000000000000020 R09: 00000000c2eda353 R10: ffff88812be2bbc8 R11: 000000001faab533 R12: ffff88885fb049c8 R13: ffff88812be2bbc8 R14: 0000000000000 ffff88811896ae00 FS: 0000000000000000(0000) GS:ffff8888dca82000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR ffffffff000002c8 CR3: 0000000243050002 CR4: 0000000000372eb0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <IRQ> ? try_to_wake_up+0x108/0x4c0 ? udp4_lib_lookup2+0xbe/0x150 ? udp_lib_lport_inuse+0x100/ __udp4_lib_lookup+0x2b0/0x410 __xfrm_policy_check2.constprop.0+0x11e/0x130 udp_queue_rcv_one_skb+0x1d/0x530 udp_unicast_rcv_skb+0x76/0x90 __udp4_lib_rcv+0xa64/0xe90 ip_protocol_deliver_rcu+0x20/0x130 ip_local_deliver_finish+0x75/0xa0 ip_local_deliver+0xc1/0xd0 ? ip_protocol_deliver_rcu+0x130/0 ip_sublist_rcv+0x1f9/0x240 ? ip_rcv_finish_core+0x430/0x430 ip_list_rcv+0xfc/0x130 __netif_receive_skb_list_core+0x181/0x1e0 netif_receive_skb_list_internal+0x200/0x360 ? mlx5e_build_rx_skb+0x1bc/0xda0 [mlx5_core] gro_receive_skb+0xfd/0x210 mlx5e_handle_rx_cqe_mpwrq+0x141/0 [mlx5_core] mlx5e_poll_rx_cq+0xcc/0x8e0 [mlx5_core] ? mlx5e_handle_rx_dim+0x91/0xd0 [mlx5_core] mlx5e_napi_poll+0x114/0xab0 [mlx5_core] __napi_poll+0x net_rx_action+0x32d/0x3a0 ? mlx5_eq_comp_int+0x8d/0x280 [mlx5_core] ? notifier_call_chain+0x33/0xa0 handle_softirqs+0xda/0x250 irq_exit_rcu+0x6d/0xc0 common_interrupt+0x81/0xa0 </IRQ>
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: drm/rockchip: vop2: fail cleanly if missing a primary plane for a video-port Each window of a vop2 by a specific set of video ports, so while binding the vop2, we look through the list of available windows trying to find one designated as primary-plane and usable specific port. The code later wants to use drm_crtc_init_with_planes with that found primary plane, but nothing has checked so far if a primary plane was actually f

38597	whatever reason, the rk3576 vp2 does not have a usable primary window (if vp0 is also in use) which brought the issue to light and ended in a null-pointer derefere further down. As we expect a primary-plane to exist for a video-port, add a check at the end of the window-iteration and fail probing if none was found.
CVE-2025-38592	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_devcd_dump: fix out-of-bounds via dev_coredumpv Currently both dev_coredumpv skb_put_data in hci_devcd_dump use hdev->dump.head. However, dev_coredumpv can free the buffer. From dev_coredumpm_timeout documentation, which is us dev_coredumpv: > Creates a new device coredump for the given device. If a previous one hasn't > been read yet, the new coredump is discarded. The data lifetim determined > by the device coredump framework and when it is no longer needed the @free > function will be called to free the data. If the data has not been rea userspace yet, dev_coredumpv will discard new buffer, freeing hdev->dump.head. This leads to vmalloc-out-of-bounds error when skb_put_data tries to access hde >dump.head. A crash report from syzbot illustrates this: == KASAN: vmalloc-out-of-bounds in skb_put_data include/linux/skbuff.h:2752 [inline] BUG: KASAN: vmalloc-out-of-bounds in hci_devcd_dump+0x142/0x240 net/bluetooth/coredump.c:258 Read of size 140 at addr ffffc90004ed5000 by task kworker/u9:2/5844 CPU: 1 UID: 0 PID: 5844 Comm: kworker/u9:2 Not tainted 6.1 syzkaller-10892-g4e82c87058f4 #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 02/12/2025 Workqueue: hci_devcd_timeout Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x116/0x1f0 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:408 [inline] print_report+0xc3/0x670 mm/kasan/report.c:521 kasan_report+0xe0/0x110 mm/kasan/report.c:634 check_region_inline mm/kasan/generic.c:183 [inline] kasan_check_range+0xef/0x1a0 mm/kasan/generic.c:189 __asan_memcpy+0x23/0x60 mm/kasan/shadow.c:105 skb_put_data include/linux/skbuff.h:2752 [inline] hci_devcd_dump+0x142/0x240 net/bluetooth/coredump.c:258 hci_devcd_timeout+0xb5/0x2e0 net/bluetooth/coredump.c:413 process_one_work+0x9cc/0x1b70 kernel/workqueue.c:3238 process_scheduled_works kernel/workqueue.c:3319 [inline] worker_thread+0x6c8/0xf10 kernel/workqueue.c:3400 kthread+0x3c2/0x780 kernel/kthread.c:464 ret_from_fork+0x45/0x80 arch/x86/kernel/process.c:153 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 </TASK> The buggy address ffffc90004ed5000 belongs to a vmalloc virtual mapping Memory state around the buggy address: ffffc90004ed4f00: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ffffc90004ed4f80: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 >ffffc90004ed5000: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ^ ffffc90004ed5080: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ffffc90004ed5100: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 == To avoid this issue, reorder dev_coredumpv to be ca skb_put_data that does not free the data.
CVE-2025-38593	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: fix double free in 'hci_discovery_filter_clear()' Function 'hci_discovery_filter_c frees 'uuids' array and then sets it to NULL. There is a tiny chance of the following race: 'hci_cmd_sync_work()' 'update_passive_scan_sync()' 'hci_update_passive_scan_sync()' 'hci_discovery_filter_clear()' kfree(uuids); <------------------------preempted--------------------------------> 'start_service_discovery()' 'hci_discovery_filter_clear()' kfree(uuids); // DOUBLE FREE <------------------------preempted--------------------------------> uuids = NULL; To fix it let's add locking around 'k and NULL pointer assignment. Otherwise the following backtrace fires: [ ] ------------[cut here]------------ [ ] kernel BUG at mm/slub.c:547! [ ] Internal error: Oops - BU 00000000f2000800 [#1] PREEMPT SMP [ ] CPU: 3 UID: 0 PID: 246 Comm: bluetoothd Tainted: G O 6.12.19-kernel #1 [ ] Tainted: [O]=OOT_MODULE [ ] pstate: 6040 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [ ] pc : __slab_free+0xf8/0x348 [ ] lr : __slab_free+0x48/0x348 ... [ ] Call trace: [ ] __slab_free+0xf8/0x348 [ ] kfree+0x164/0x27c [ ] start_service_discovery+0x1d0/0x2c0 [ ] hci_sock_sendmsg+0x518/0x924 [ ] __sock_sendmsg+0x54/0x60 [ ] sock_write_iter+0x98/0xf8 [ ] do_iter_readv_writev+0xe4/0x1c8 [ ] vfs_writev+0x128/0x2b0 [ ] do_writev+0xfc/0x118 [ ] __arm64_sys_writev+0x20/0x2c [ ] invoke_syscall+0x68/0xf0 [ ] el0_svc_common.constprop.0+0x40/0xe0 [ ] do_el0_svc+0x1c/0x28 [ ] el0_svc+0x30/0xd0 [ ] el0t_64_sync_handler+0x100/0x12c [ ] el0t_64_sync+0x194/0x198 [8b0002e6 eb17031f 54fffbe1 d503201f (d4210000) [ ] ---[end trace 0000000000000000]---
CVE-2025-38612	In the Linux kernel, the following vulnerability has been resolved: staging: fbtft: fix potential memory leak in fbtft_framebuffer_alloc() In the error paths after fb_info is successfully allocated, the memory allocated in fb_deferred_io_init() for info->pagerefs is not freed. Fix that by adding the cleanup function on the error path.
CVE-2025-38613	In the Linux kernel, the following vulnerability has been resolved: staging: gpib: fix unset padding field copy back to userspace The introduction of a padding field i gpib_board_info_ioctl is showing up as initialized data on the stack frame being copyied back to userspace in function board_info_ioctl. The simplest fix is to initializ entire struct to zero to ensure all unassigned padding fields are zero'd before being copied back to userspace.
CVE-2025-38614	In the Linux kernel, the following vulnerability has been resolved: eventpoll: Fix semi-unbounded recursion Ensure that epoll instances can never form a graph deep EP_MAX_NESTS+1 links. Currently, ep_loop_check_proc() ensures that the graph is loop-free and does some recursion depth checks, but those recursion depth che limit the depth of the resulting tree for two reasons: - They don't look upwards in the tree. - If there are multiple downwards paths of different lengths, only one of t is actually considered for the depth check since commit 28d82dc1c4ed ("epoll: limit paths"). Essentially, the current recursion depth check in ep_loop_check_proc() serves to prevent it from recursing too deeply while checking for loops. A more thorough check is done in reverse_path_check() after the new graph edge has alrea created; this checks, among other things, that no paths going upwards from any non-epoll file with a length of more than 5 edges exist. However, this check does n to non-epoll files. As a result, it is possible to recurse to a depth of at least roughly 500, tested on v6.15. (I am unsure if deeper recursion is possible; and this may changed with commit 8c44dac8add7 ("eventpoll: Fix priority inversion problem").) To fix it: 1. In ep_loop_check_proc(), note the subtree depth of each visited node subtree depths for the total depth calculation even when a subtree has already been visited. 2. Add ep_get_upwards_depth_proc() for similarly determining the ma depth of an upwards walk. 3. In ep_loop_check(), use these values to limit the total path length between epoll nodes to EP_MAX_NESTS edges.
CVE-2025-54473	An authenticated RCE vulnerability in Phoca Commander component 1.0.0-4.0.0 and 5.0.0-5.0.1 for Joomla was discovered. The issue allows code execution via the feature.
CVE-2025-8916	Allocation of Resources Without Limits or Throttling vulnerability in Legion of the Bouncy Castle Inc. Bouncy Castle for Java bcpkix, bcprov, bcpkix-fips on All (API m allows Excessive Allocation. This vulnerability is associated with program files https://github.Com/bcgit/bc-java/blob/main/pkix/src/main/java/org/bouncycastle/pkix/jcajce/PKIXCertP... https://github.Com/bcgit/bc-java/blob/main/pkix/src/main/java/org/bouncycastle/pkix/jcajce/PKIXCertPathReviewer.java , https://github.Com/bcgit/bc-java/blob/main/prov/src/main/java/org/bouncycastle/x509/PKIXCertPathRevi... https://github.Com/bcgit/bc-java/blob/main/prov/src/main/java/org/bouncycastle/x509/PKIXCertPathReviewer.java . This issue affects Bouncy Castle for Java: from BC 1.44 through 1.78, from B FIPS 1.0.0 through 1.0.7, from BCPKIX FIPS 2.0.0 through 2.0.7.
CVE-2025-38615	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: cancle set bad inode after removing name fails The reproducer uses a file0 on a ntfs3 file with a corrupted i_link. When renaming, the file0's inode is marked as a bad inode because the file name cannot be deleted. The underlying bug is that make_bad_ called on a live inode. In some cases it's "icache lookup finds a normal inode, d_splice_alias() is called to attach it to dentry, while another thread decides to call make_bad_inode() on it - that would evict it from icache, but we'd already found it there earlier". In some it's outright "we have an inode attached to dentry - that's got it in the first place; let's call make_bad_inode() on it just for shits and giggles".
CVE-2025-54464	This vulnerability exists in ZKTeco WL20 due to storage of admin and user credentials without encryption in the device firmware. An attacker with physical access c exploit this vulnerability by extracting the firmware and reverse engineer the binary data to access the unencrypted credentials stored in the firmware of targeted
CVE-2025-54465	This vulnerability exists in ZKTeco WL20 due to hard-coded MQTT credentials and endpoints stored in plaintext within the device firmware. An attacker with physic could exploit this vulnerability by extracting the firmware and analyzing the binary data to retrieve the hard-coded MQTT credentials and endpoints from the target device. Successful exploitation of this vulnerability could allow the attacker to gain unauthorized access to the MQTT broker and manipulate the communications o targeted device.
CVE-2024-5477	A potential security vulnerability has been identified in the System BIOS for some HP PC products which may allow escalation of privilege, arbitrary code execution, service, or information disclosure via a physical attack that requires specialized equipment and knowledge. HP is releasing firmware mitigation for the potential vul

CVE-2025-55737	flaskBlog is a blog app built with Flask. In 2.8.0 and earlier, when deleting a comment, there's no validation of the ownership of the comment. Every user can delet arbitrary comment of another user on every post, by simply intercepting the delete request and changing the commentID. The code that causes the problem is in routes/post.py.
CVE-2025-54411	Discourse is an open-source discussion platform. Welcome banner user name string for logged in users can be vulnerable to XSS attacks, which affect the user the or an admin impersonating them. Admins can temporarily alter the welcome_banner.header.logged_in_members site text to remove the preferred_display_name placeholder, or not impersonate any users for the time being. This vulnerability is fixed in 3.5.0.beta8.
CVE-2025-54880	Mermaid is a JavaScript based diagramming and charting tool that uses Markdown-inspired text definitions and a renderer to create and modify complex diagrams. default configuration of mermaid 11.9.0 and earlier, user supplied input for architecture diagram icons is passed to the d3 html() method, creating a sink for cross scripting. This vulnerability is fixed in 11.10.0.
CVE-2025-54881	Mermaid is a JavaScript based diagramming and charting tool that uses Markdown-inspired text definitions and a renderer to create and modify complex diagrams. default configuration of mermaid 10.9.0-rc.1 to 11.9.0, user supplied input for sequence diagram labels is passed to innerHTML during calculation of element size, XSS.
CVE-2025-55279	This vulnerability exists in ZKTeco WL20 due to hard-coded private key stored in plaintext within the device firmware. An attacker with physical access could explo vulnerability by extracting the firmware and analyzing the binary data to retrieve private key stored in the firmware of the targeted device. Successful exploitation vulnerability could allow the attacker to perform unauthorized decryption of sensitive data and Man-in-the-Middle (MitM) attacks on the targeted device.
CVE-2025-34153	Hyland OnBase versions prior to 17.0.2.87 (other versions may be affected) are vulnerable to unauthenticated remote code execution via insecure deserialization .NET Remoting TCP channel. The service registers a listener on port 6031 with the URI endpoint TimerServer, implemented in Hyland.Core.Timers.dll. This endpoint deserializes untrusted input using the .NET BinaryFormatter, allowing attackers to execute arbitrary code under the context of NT AUTHORITY\SYSTEM.
CVE-2025-55153	Rejected reason: This CVE is a duplicate of another CVE.
CVE-2025-2184	A credential management flaw in Palo Alto Networks Cortex XDR® Broker VM causes different Broker VM images to share identical default credentials for internal s Users knowing these default credentials could access internal services on other Broker VM installations. The attacker must have network access to the Broker VM t this issue.
CVE-2025-55280	This vulnerability exists in ZKTeco WL20 due to storage of Wi-Fi credentials, configuration data and system data in plaintext within the device firmware. An attacke physical access could exploit this vulnerability by extracting the firmware and reverse engineer the binary data to access the plaintext sensitive data stored in the device. Successful exploitation of this vulnerability could allow the attacker to gain unauthorized network access, retrieve and manipulate data on the targeted dev
CVE-2025-54074	Cherry Studio is a desktop client that supports for multiple LLM providers. From versions 1.2.5 to 1.5.1, Cherry Studio is vulnerable to OS Command Injection during connection with a malicious MCP server in HTTP Streamable mode. Attackers can setup a malicious MCP server with compatible OAuth authorization server endpoi trick victims into connecting it, leading to OS command injection in vulnerable clients. This issue has been patched in version 1.5.2.
CVE-2025-2183	An insufficient certificate validation issue in the Palo Alto Networks GlobalProtect™ app enables attackers to connect the GlobalProtect app to arbitrary servers. Thi enable a local non-administrative operating system user or an attacker on the same subnet to install malicious root certificates on the endpoint and subsequently i malicious software signed by the malicious root certificates on that endpoint.
CVE-2025-43744	A stored DOM-based Cross-Site Scripting (XSS) vulnerability in Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.5, 2025.Q1.0 thr 2025.Q1.15, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.19 and 7.4 GA through up exists in the Asset Publisher configuration UI within the Source.js module. This vulnerability allows attackers to inject arbitrary JavaScript via DDM structure field lab are then inserted into the DOM using innerHTML without proper encoding.
CVE-2025-2182	A problem with the implementation of the MACsec protocol in Palo Alto Networks PAN-OS® results in the cleartext exposure of the connectivity association key (CA issue is only applicable to PA-7500 Series devices which are in an NGFW cluster. A user who possesses this key can read messages being sent between devices in Cluster. There is no impact in non-clustered firewalls or clusters of firewalls that do not enable MACsec.
CVE-2025-2181	A sensitive information disclosure vulnerability in Palo Alto Networks Checkov by Prisma® Cloud can result in the cleartext exposure of Prisma Cloud access keys in Checkov's output.
CVE-2025-2180	An unsafe deserialization vulnerability in Palo Alto Networks Checkov by Prisma® Cloud allows an authenticated user to execute arbitrary code as a non administra by scanning a malicious terraform file when using Checkov in Prisma® Cloud. This issue impacts Checkov 3.0 versions earlier than Checkov 3.2.415.
CVE-2025-43743	Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.5, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 th 2024.Q2.13, 2024.Q1.1 through 2024.Q1.15 and 7.4 GA through update 92 allows any authenticated remote user to view other calendars by allowing them to enur names of other users, given an attacker the possibility to send phishing to these users.
CVE-2025-43737	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.8 and 2025.Q1.0 through 2025.Q1.15 remote authenticated user to inject JavaScript code via _com_liferay_journal_web_portlet_JournalPortlet_backURL parameter.
CVE-2025-43745	A CSRF vulnerability in Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.7, 2025.Q1.0 through 2025.Q1.14, 2024.Q4.0 through 2 2024.Q3.1 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 remote attackers to perform origin request on behalf of the authenticated user via the endpoint parameter.
CVE-2025-38611	In the Linux kernel, the following vulnerability has been resolved: vmci: Prevent the dispatching of uninitialized payloads The reproducer executes the host's unlock call in two different tasks. When init_context fails, the struct vmci_event_ctx is not fully initialized when executing vmci_datagram_dispatch() to send events to all v contexts. This affects the datagram taken from the datagram queue of its context by another task, because the datagram payload is not initialized according to the payload_size, which causes the kernel data to leak to the user space. Before dispatching the datagram, and before setting the payload content, explicitly set the pa content to 0 to avoid data leakage caused by incomplete payload initialization.
CVE-2025-54143	Sandboxed iframes on webpages could potentially allow downloads to the device, bypassing the expected sandbox restrictions declared on the parent page This vulnerability affects Firefox for iOS < 141.
CVE-2025-38610	In the Linux kernel, the following vulnerability has been resolved: powercap: dtpm_cpu: Fix NULL pointer dereference in get_pd_power_uw() The get_pd_power_uw(can crash with a NULL pointer dereference when em_cpu_get() returns NULL. This occurs when a CPU becomes impossible during runtime, causing get_cpu_device return NULL, which propagates through em_cpu_get() and leads to a crash when em_span_cpus() dereferences the NULL pointer. Add a NULL check after em_cpu_g return 0 if unavailable, matching the existing fallback behavior in __dtpm_cpu_setup(). [rjw: Drop an excess empty code line]

CVE-2025-38601	In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: clear initialized flag for deinit-ed srng lists In a number of cases we see kernel panics resume due to ath11k kernel page fault, which happens under the following circumstances: 1) First ath11k_hal_dump_srng_stats() call Last interrupt received for e ath11k_pci 0000:01:00.0: group_id 0 22511ms before ath11k_pci 0000:01:00.0: group_id 1 14440788ms before [..] ath11k_pci 0000:01:00.0: failed to receive cont response completion, polling.. ath11k_pci 0000:01:00.0: Service connect timeout ath11k_pci 0000:01:00.0: failed to connect to HTT: -110 ath11k_pci 0000:01:00.0 start core: -110 ath11k_pci 0000:01:00.0: firmware crashed: MHI_CB_EE_RDDM ath11k_pci 0000:01:00.0: already resetting count 2 ath11k_pci 0000:01:00.0: failed wlan mode request (mode 4): -110 ath11k_pci 0000:01:00.0: qmi failed to send wlan mode off: -110 ath11k_pci 0000:01:00.0: failed to reconfigure driver on crash [..] 2) At this point reconfiguration fails (we have 2 resets) and ath11k_core_reconfigure_on_crash() calls ath11k_hal_srng_deinit() which destroys srng lists. Howeve not reset per-list ->initialized flag. 3) Second ath11k_hal_dump_srng_stats() call sees stale ->initialized flag and attempts to dump srng stats: Last interrupt receive each group: ath11k_pci 0000:01:00.0: group_id 0 66785ms before ath11k_pci 0000:01:00.0: group_id 1 14485062ms before ath11k_pci 0000:01:00.0: group_id 2 14485062ms before ath11k_pci 0000:01:00.0: group_id 3 14485062ms before ath11k_pci 0000:01:00.0: group_id 4 14780845ms before ath11k_pci 0000:01:00.0: 5 14780845ms before ath11k_pci 0000:01:00.0: group_id 6 14485062ms before ath11k_pci 0000:01:00.0: group_id 7 66814ms before ath11k_pci 0000:01:00.0: gr 68997ms before ath11k_pci 0000:01:00.0: group_id 9 67588ms before ath11k_pci 0000:01:00.0: group_id 10 69511ms before BUG: unable to handle page fault for ffffa007404eb010 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 100000067 P4D 100000067 PUD 10022d067 PMD 100b01067 PTE 0 Oops: 0000 [#1] PREEMPT SMP NOPTI RIP: 0010:ath11k_hal_dump_srng_stats+0x2b4/0x3b0 [ath11k] Call Trace: <TASK> ? __die_body+0xae/0x page_fault_oops+0x381/0x3e0 ? exc_page_fault+0x69/0xa0 ? asm_exc_page_fault+0x22/0x30 ? ath11k_hal_dump_srng_stats+0x2b4/0x3b0 [ath11k (HASH:6cea 4 ath11k_qmi_driver_event_work+0xbd/0x1050 [ath11k (HASH:6cea 4)] worker_thread+0x389/0x930 kthread+0x149/0x170 Clear per-list ->initialized flag in ath11k_hal_srng_deinit().
CVE-2025-38594	In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Fix UAF on sva unbind with pending IOPFs Commit 17fce9d2336d ("iommu/vt-d: Put enablement in domain attach path") disables IOPF on device by removing the device from its IOMMU's IOPF queue when the last IOPF-capable domain is detached device. Unfortunately, it did this in a wrong place where there are still pending IOPFs. As a result, a use-after-free error is potentially triggered and eventually a ker with a kernel trace similar to the following: refcount_t: underflow; use-after-free. WARNING: CPU: 3 PID: 313 at lib/refcount.c:28 refcount_warn_saturate+0xd8/0xe(Workqueue: iopf_queue/dmar0-iopfq iommu_sva_handle_iopf Call Trace: <TASK> iopf_free_group+0xe/0x20 process_one_work+0x197/0x3d0 worker_thread+0x23 rescuer_thread+0x4a0/0x4a0 kthread+0xf8/0x230 ? finish_task_switch.isra.0+0x81/0x260 ? kthreads_online_cpu+0x110/0x110 ? kthreads_online_cpu+0x110/0x1 ret_from_fork+0x13b/0x170 ? kthreads_online_cpu+0x110/0x110 ret_from_fork_asm+0x11/0x20 </TASK> ---[end trace 0000000000000000]--- The intel_pasid_tear_down_entry() function is responsible for blocking hardware from generating new page faults and flushing all in-flight ones. Therefore, moving iopf_for_domain_remove() after this function should resolve this.
CVE-2025-38595	In the Linux kernel, the following vulnerability has been resolved: xen: fix UAF in dmabuf_exp_from_pages() [dma_buf_fd() fixes; no preferences regarding the tree through - up to xen folks] 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 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 k 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 combinatio reserving a descriptor and fd_install(). gntdev dmabuf_exp_from_pages() calls it and then proceeds to access the objects destroyed on close - starting with gntdev_ itself. Fix that by doing reserving descriptor before anything else and do fd_install() only when everything had been set up.
CVE-2025-38596	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Fix UAF in panthor_gem_create_with_handle() debugfs code The object is potentially gone after the drm_gem_object_put(). In general the object should be fully constructed before calling drm_gem_handle_create(), except the debugfs tracking uses separate lock and list and separate flag to denotate whether the object is actually initialized. Since I'm touching this all anyway simplify this by only adding the obj debugfs when it's ready for that, which allows us to delete that separate flag. panthor_gem_debugfs_bo_rm() already checks whether we've actually been added to this is some error path cleanup. v2: Fix build issues for !CONFIG_DEBUGFS (Adrián) v3: Add linebreak and remove outdated comment (Liviu)
CVE-2025-55163	Netty is an asynchronous, event-driven network application framework. Prior to versions 4.1.124.Final and 4.2.4.Final, Netty is vulnerable to MadeYouReset DDoS. logical vulnerability in the HTTP/2 protocol, that uses malformed HTTP/2 control frames in order to break the max concurrent streams limit - which results in resour exhaustion and distributed denial of service. This issue has been patched in versions 4.1.124.Final and 4.2.4.Final.
CVE-2025-38598	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix use-after-free in amdgpu_userq_suspend+0x51a/0x5a0 [+0.000020] BUG: KAS use-after-free in amdgpu_userq_suspend+0x51a/0x5a0 [amdgpu] [+0.000817] Read of size 8 at addr ffff88812eec8c58 by task amd_pci_unplug/1733 [+0.00002 UID: 0 PID: 1733 Comm: amd_pci_unplug Tainted: G W 6.14.0+ #2 [+0.000009] Tainted: [W]=WARN [+0.000003] Hardware name: ASUS System Product Name/P B550-F GAMING (WI-FI), BIOS 1401 12/03/2020 [+0.000004] Call Trace: [+0.000004] <TASK> [+0.000003] dump_stack_lvl+0x76/0xa0 [+0.000011] print_report+0xce/0x600 [+0.000009] ? srso_return_thunk+0x5/0x5f [+0.000006] ? kasan_complete_mode_report_info+0x76/0x200 [+0.000007] ? kasan_addr_to_slab+0xd/0xb0 [+0.000006] ? amdgpu_userq_suspend+0x51a/0x5a0 [amdgpu] [+0.000707] kasan_report+0xbe/0x110 [+0.000006] ? amdgpu_userq_suspend+0x51a/0x5a0 [amdgpu] [+0.000541] __asan_report_load8_noabort+0x14/0x30 [+0.000005] amdgpu_userq_suspend+0x51a/0x5a0 [am +0.000535] ? stop_cpsch+0x396/0x600 [amdgpu] [+0.000556] ? stop_cpsch+0x429/0x600 [amdgpu] [+0.000536] ? __pfx_amdgpu_userq_suspend+0x10/0x10 [[+0.000536] ? srso_return_thunk+0x5/0x5f [+0.000004] ? kgd2kfd_suspend+0x132/0x1d0 [amdgpu] [+0.000542] amdgpu_device_fini_hw+0x581/0xe90 [amdg +0.000485] ? down_write+0xbb/0x140 [+0.000007] ? __mutex_unlock_slowpath.constprop.0+0x317/0x360 [+0.000005] ? __pfx_amdgpu_device_fini_hw+0x10/0 [amdgpu] [+0.000482] ? __kasan_check_write+0x14/0x30 [+0.000004] ? srso_return_thunk+0x5/0x5f [+0.000004] ? up_write+0x55/0xb0 [+0.000007] ? srso_return_thunk+0x5/0x5f [+0.000005] ? blocking_notifier_chain_unregister+0x6c/0xc0 [+0.000008] amdgpu_driver_unload_kms+0x69/0x90 [amdgpu] [+0.0 amdgpu_pci_remove+0x93/0x130 [amdgpu] [+0.000482] pci_device_remove+0xae/0x1e0 [+0.000008] device_remove+0xc7/0x180 [+0.000008] device_release_driver_internal+0x3d4/0x5a0 [+0.000007] device_release_driver+0x12/0x20 [+0.000004] pci_stop_bus_device+0x104/0x150 [+0.000006] pci_stop_and_remove_bus_device_locked+0x1b/0x40 [+0.000005] remove_store+0xd7/0xf0 [+0.000005] ? __pfx_remove_store+0x10/0x10 [+0.000006] ? __pfx__copy_from_iter+0x10/0x10 [+0.000006] ? __pfx_dev_attr_store+0x10/0x10 [+0.000006] dev_attr_store+0x3f/0x80 [+0.000006] sysfs_kf_write+0x125/0x +0.000004] ? srso_return_thunk+0x5/0x5f [+0.000005] ? __kasan_check_write+0x14/0x30 [+0.000005] kernfs_fop_write_iter+0x2ea/0x490 [+0.000005] ? rw_verify_area+0x70/0x420 [+0.000005] ? __pfx_kernfs_fop_write_iter+0x10/0x10 [+0.000006] vfs_write+0x90d/0xe70 [+0.000005] ? srso_return_thunk+0x5/0 +0.000005] ? __pfx_vfs_write+0x10/0x10 [+0.000004] ? local_clock+0x15/0x30 [+0.000008] ? srso_return_thunk+0x5/0x5f [+0.000004] ? __kasan_slab_free+0x +0.000005] ? srso_return_thunk+0x5/0x5f [+0.000004] ? __kasan_check_read+0x11/0x20 [+0.000004] ? srso_return_thunk+0x5/0x5f [+0.000004] ? fdget_pos+0x1d3/0x500 [+0.000007] ksys_write+0x119/0x220 [+0.000005] ? putname+0x1c/0x30 [+0.000006] ? __pfx_ksys_write+0x10/0x10 [+0.000007] __x64_sys_write+0x72/0xc0 [+0.000006] x64_sys_call+0x18ab/0x26f0 [+0.000006] do_syscall_64+0x7c/0x170 [+0.000004] ? srso_return_thunk+0x5/0x5f [+0 ? __pfx___x64_sys_openat+0x10/0x10 [+0.000006] ? srso_return_thunk+0x5/0x5f [+0.000004] ? __kasan_check_read+0x11/0x20 [+0.000003] ? srso_return_thunk+0x5/0x5f [+0.000004] ? fpregs_assert_state_consistent+0x21/0xb0 [+0.000006] ? srso_return_thunk+0x5/0x5f [+0.000004] ? syscall_exit_to_user_mode+0x4e/0x240 [+0.000005] ? srso_return_thunk+0x5/0x5f [+0.000004] ? do_syscall_64+0x88/0x170 [+0.000003] ? srso_return_thunk+ [+0.000004] ? irqentry_exit+0x43/0x50 [+0.000004] ? srso_return_thunk+0x5 ---truncated---
CVE-2025-8364	A crafted URL using a blob: URI could have hidden the true origin of the page, resulting in a potential spoofing attack. *Note: This issue only affected Android opera systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 141.
CVE-2025-38599	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7996: Fix possible OOB access in mt7996_tx() Fis possible Out-Of-Boundary access mt7996_tx routine if link_id is set to IEEE80211_LINK_UNSPECIFIED
CVE-2025-38600	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7925: fix off by one in mt7925_mcu_hw_scan() The ssid->ssids[] and sreq->ssids[] have MT7925_RNR_SCAN_MAX_BSSIDS elements so this >= needs to be > to prevent an out of bounds access.
CVE-	

2025-8042	Firefox for Android allowed a sandboxed iframe without the `allow-downloads` attribute to start downloads. This vulnerability affects Firefox < 141.
CVE-2025-8041	In the address bar, Firefox for Android truncated the display of URLs from the end instead of prioritizing the origin. This vulnerability affects Firefox < 141.
CVE-2025-55033	Dragging JavaScript links to the URL bar in Focus for iOS could be utilized to run malicious scripts, potentially resulting in XSS attacks This vulnerability affects Focu < 142.
CVE-2025-55032	Focus for iOS would not respect a Content-Disposition header of type Attachment and would incorrectly display the content inline, potentially allowing for XSS attac vulnerability affects Focus for iOS < 142.
CVE-2025-38602	In the Linux kernel, the following vulnerability has been resolved: iwlwifi: Add missing check for alloc_ordered_workqueue Add check for the return value of alloc_ordered_workqueue since it may return NULL pointer.
CVE-2025-54144	The URL scheme used by Firefox to facilitate searching of text queries could incorrectly allow attackers to open arbitrary website URLs or internal pages if a user w into clicking a link This vulnerability affects Firefox for iOS < 141.
CVE-2025-38603	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix slab-use-after-free in amdgpu_userq_mgr_fini+0x70c The issue was reproduced using IGT pci_unplug test. It is expected that `amdgpu_driver_postclose_kms()` is called prior to `amdgpu_drm_release()`. However, the bug is that `amdgpu_fpriv freed in `amdgpu_driver_postclose_kms()`, and then later accessed in `amdgpu_drm_release()` via a call to `amdgpu_userq_mgr_fini()`. As a result, KASAN detect after-free condition, as shown in the log below. The proposed fix is to move the calls to `amdgpu_eviction_fence_destroy()` and `amdgpu_userq_mgr_fini()` into `amdgpu_driver_postclose_kms()`, so they are invoked before `amdgpu_fpriv` is freed. This also ensures symmetry with the initialization path in `amdgpu_driver_open_kms()`, where the following components are initialized: - `amdgpu_userq_mgr_init()` - `amdgpu_eviction_fence_init()` - `amdgpu_ctx_mgr_i Correspondingly, in `amdgpu_driver_postclose_kms()` we should clean up using: - `amdgpu_userq_mgr_fini()` - `amdgpu_eviction_fence_destroy()` - `amdgpu_ctx_mgr_fini()` This change eliminates the use-after-free and improves consistency in resource management between open and close paths. [+0.09436 == [+0.000026] BUG: KASAN: slab-use-after-free in amdgpu_userq_mgr_fini+0x70c/0x730 [amdgpu] [+0.000866] Write of size 8 at addr ffff88811c068c60 by task amd_pci_unplug/1737 [+0.000026] CPU: 3 UID: 0 Comm: amd_pci_unplug Not tainted 6.14.0+ #2 [+0.000008] Hardware name: ASUS System Product Name/ROG STRIX B550-F GAMING (WI-FI), BIOS 1401 12/03/2 +0.000004] Call Trace: [+0.000004] <TASK> [+0.000003] dump_stack_lvl+0x76/0xa0 [+0.000010] print_report+0xce/0x600 [+0.000009] ? amdgpu_userq_mgr_fini+0x70c/0x730 [amdgpu] [+0.000790] ? srso_return_thunk+0x5/0x5f [+0.000007] ? kasan_complete_mode_report_info+0x76/0x200 [+0 ? amdgpu_userq_mgr_fini+0x70c/0x730 [amdgpu] [+0.000684] kasan_report+0xbe/0x110 [+0.000007] ? amdgpu_userq_mgr_fini+0x70c/0x730 [amdgpu] [+0.0 __asan_report_store8_noabort+0x17/0x30 [+0.000007] amdgpu_userq_mgr_fini+0x70c/0x730 [amdgpu] [+0.000801] ? __pfx_amdgpu_userq_mgr_fini+0x10/0x1 [amdgpu] [+0.000819] ? srso_return_thunk+0x5/0x5f [+0.000008] amdgpu_drm_release+0xa3/0xe0 [amdgpu] [+0.000604] __fput+0x354/0xa90 [+0.000010] __fput_sync+0x59/0x80 [+0.000005] __x64_sys_close+0x7d/0xe0 [+0.000006] x64_sys_call+0x2505/0x26f0 [+0.000006] do_syscall_64+0x7c/0x170 [+0.0000 kasan_record_aux_stack+0xae/0xd0 [+0.000005] ? srso_return_thunk+0x5/0x5f [+0.000004] ? kmem_cache_free+0x398/0x580 [+0.000006] ? __fput+0x543/0x +0.000006] ? srso_return_thunk+0x5/0x5f [+0.000004] ? __fput+0x543/0xa90 [+0.000004] ? __kasan_check_read+0x11/0x20 [+0.000007] ? srso_return_thunk [+0.000004] ? __kasan_check_read+0x11/0x20 [+0.000003] ? srso_return_thunk+0x5/0x5f [+0.000004] ? fpregs_assert_state_consistent+0x21/0xb0 [+0.0000 srso_return_thunk+0x5/0x5f [+0.000004] ? syscall_exit_to_user_mode+0x4e/0x240 [+0.000005] ? srso_return_thunk+0x5/0x5f [+0.000004] ? do_syscall_64+0x [+0.000003] ? srso_return_thunk+0x5/0x5f [+0.000004] ? do_syscall_64+0x88/0x170 [+0.000004] ? srso_return_thunk+0x5/0x5f [+0.000004] ? irqentry_exit+ [+0.000004] ? srso_return_thunk+0x5/0x5f [+0.000004] ? exc_page_fault+0x7c/0x110 [+0.000006] entry_SYSCALL_64_after_hwframe+0x76/0x7e [+0.000005] 0033:0x7ffff7b14f67 [+0.000005] Code: ff e8 0d 16 02 00 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 f3 0f 1e fa 64 8b 04 25 18 00 00 00 85 c0 75 10 b8 03 00 00 00 0 <48> 3d 00 f0 ff ff 77 41 c3 48 83 ec 18 89 7c 24 0c e8 73 ba f7 ff [+0.000004] RSP: 002b:00007fffffffe358 EFLAGS: 00000246 ORIG_RAX: 0000000000000003 [+0.000006] RAX: ffffffffff ---truncated---
CVE-2025-38604	In the Linux kernel, the following vulnerability has been resolved: wifi: rtl818x: Kill URBs before clearing tx status queue In rtl8187_stop() move the call of usb_kill_anchored_urbs() before clearing b_tx_status.queue. This change prevents callbacks from using already freed skb due to anchor was not killed before freein skb. BUG: kernel NULL pointer dereference, address: 0000000000000080 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page P4D 0 Oops: Oops: 0000 [#1] SMP NOPTI CPU: 7 UID: 0 PID: 0 Comm: swapper/7 Not tainted 6.15.0 #8 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i4 PIIX, 1996), BIOS 0.0.0 02/06/2015 RIP: 0010:ieee80211_tx_status_irqsafe+0x21/0xc0 [mac80211] Call Trace: <IRQ> rtl8187_tx_cb+0x116/0x150 [rtl8187] __usb_hcd_giveback_urb+0x9d/0x120 usb_giveback_urb_bh+0xbb/0x140 process_one_work+0x19b/0x3c0 bh_worker+0x1a7/0x210 tasklet_action+0x10/0x30 handle_softirqs+0xf0/0x340 __irq_exit_rcu+0xcd/0xf0 common_interrupt+0x85/0xa0 </IRQ> Tested on RTL8187BvE device. Found by Linux Verification Center (linuxtesting.org) with SVACE.
CVE-2025-38605	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: Pass ab pointer directly to ath12k_dp_tx_get_encap_type() In ath12k_dp_tx_get_enca the arvif parameter is only used to retrieve the ab pointer. In vdev delete sequence the arvif->ar could become NULL and that would trigger kernel panic. Since the ath12k_dp_tx() already has a valid ab pointer, pass it directly to avoid panic and unnecessary dereferencing. PC points to "ath12k_dp_tx+0x228/0x988 [ath12k]" L "ath12k_dp_tx+0xc8/0x988 [ath12k]". The Backtrace obtained is as follows: ath12k_dp_tx+0x228/0x988 [ath12k] ath12k_mac_tx_check_max_limit+0x608/0x920 [ieee80211_process_measurement_req+0x320/0x348 [mac80211] ieee80211_tx_dequeue+0x9ac/0x1518 [mac80211] ieee80211_tx_dequeue+0xb14/0x1518 [ma ieee80211_tx_prepare_skb+0x224/0x254 [mac80211] ieee80211_xmit+0xec/0x100 [mac80211] __ieee80211_subif_start_xmit+0xc50/0xf40 [mac80211] ieee80211_subif_start_xmit+0x2e8/0x308 [mac80211] netdev_start_xmit+0x150/0x18c dev_hard_start_xmit+0x74/0xc0 Tested-on: QCN9274 hw2.0 PCI WLAN.WE 00173-QCAHKSWPL_SILICONZ-1
CVE-2025-38606	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: Avoid accessing uninitialized arvif->ar during beacon miss During beacon miss hand ath12k driver iterates over active virtual interfaces (vifs) and attempts to access the radio object (ar) via arvif->deflink->ar. However, after commit aa80f12f3bed (ath12k: defer vdev creation for MLO"), arvif is linked to a radio only after vdev creation, typically when a channel is assigned or a scan is requested. For P2P capabl a default P2P interface is created by wpa_supplicant along with regular station interfaces, these serve as dummy interfaces for P2P-capable stations, lack an associ netdev and initiate frequent scans to discover neighbor p2p devices. When a scan is initiated on such P2P vifs, driver selects destination radio (ar) based on scan fr creates a scan vdev, and attaches arvif to the radio. Once the scan completes or is aborted, the scan vdev is deleted, detaching arvif from the radio and leaving ar uninitialized. While handling beacon miss for station interfaces, P2P interface is also encountered in the vif iteration and ath12k_mac_handle_beacon_miss_iter() tri dereference the uninitialized arvif->deflink->ar. Fix this by verifying that vdev is created for the arvif before accessing its ar during beacon miss handling and simil iterator callbacks. == wlp6s0: detected bea from AP (missed 7 beacons) - probing KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] CPU: 5 UID: 0 PID: 0 Comm: swapper/5 Not tai 6.16.0-rc1-wt-ath+ #2 PREEMPT(full) RIP: 0010:ath12k_mac_handle_beacon_miss_iter+0xb5/0x1a0 [ath12k] Call Trace: __iterate_interfaces+0x11a/0x410 [mac80 ieee80211_iterate_active_interfaces_atomic+0x61/0x140 [mac80211] ath12k_mac_handle_beacon_miss+0xa1/0xf0 [ath12k] ath12k_roam_event+0x393/0x560 [a ath12k_wmi_op_rx+0x1486/0x28c0 [ath12k] ath12k_htc_process_trailer.isra.0+0x2fb/0x620 [ath12k] ath12k_htc_rx_completion_handler+0x448/0x830 [ath12k] ath12k_ce_recv_process_cb+0x549/0x9e0 [ath12k] ath12k_ce_per_engine_service+0xbe/0xf0 [ath12k] ath12k_pci_ce_workqueue+0x69/0x120 [ath12k] process_one_work+0xe3a/0x1430 Tested-on: QCN9274 hw2.0 PCI WLAN.WBE.1.4.1-00199-QCAHKSWPL_SILICONZ-1 Tested-on: WCN7850 hw2.0 PCI WLAN.HMT.1.1 00284.1-QCAHMTSWPL_V1.0_V2.0_SILICONZ-3
CVE-	In the Linux kernel, the following vulnerability has been resolved: bpf: handle jset (if a & b ...) as a jump in CFG computation BPF_JSET is a conditional jump and cur

2025-38607	verifier.c:can_jump() does not know about that. This can lead to incorrect live registers and SCC computation. E.g. in the following example: 1: r0 = 1; 2: r2 = 2; 3: 0x7 goto +1; 4: exit; 5: r0 = r2; 6: exit; W/o this fix insn_successors(3) will return only (4), a jump to (5) would be missed and r2 won't be marked as alive at (3).
CVE-2025-38608	In the Linux kernel, the following vulnerability has been resolved: bpf, ktls: Fix data corruption when using bpf_msg_pop_data() in ktls When sending plaintext data initially calculated the corresponding ciphertext length. However, if we later reduced the plaintext data length via socket policy, we failed to recalculate the ciphert length. This results in transmitting buffers containing uninitialized data during ciphertext transmission. This causes uninitialized bytes to be appended after a comp "Application Data" packet, leading to errors on the receiving end when parsing TLS record.
CVE-2025-38609	In the Linux kernel, the following vulnerability has been resolved: PM / devfreq: Check governor before using governor->name Commit 96ffcdf239de ("PM / devfreq redundant governor_name from struct devfreq") removes governor_name and uses governor->name to replace it. But devfreq->governor may be NULL and directl devfreq->governor->name may cause null pointer exception. Move the check of governor to before using governor->name.
CVE-2025-55031	Malicious pages could use Firefox for iOS to pass FIDO: links to the OS and trigger the hybrid passkey transport. An attacker within Bluetooth range could have use trick the user into using their passkey to log the attacker's computer into the target account. This vulnerability affects Firefox for iOS < 142 and Focus for iOS < 14
CVE-2025-55030	Firefox for iOS would not respect a Content-Disposition header of type Attachment and would incorrectly display the content inline rather than downloading, potent allowing for XSS attacks This vulnerability affects Firefox for iOS < 142.
CVE-2025-55029	Malicious scripts could bypass the popup blocker to spam new tabs, potentially resulting in denial of service attacks This vulnerability affects Firefox for iOS < 142.
CVE-2025-55028	Malicious scripts utilizing repetitive JavaScript alerts could prevent client user interaction in some scenarios and allow for denial of service attacks This vulnerability Firefox for iOS < 142.
CVE-2025-54145	The QR scanner could allow arbitrary websites to be opened if a user was tricked into scanning a malicious link that leveraged Firefox's open-text URL scheme This vulnerability affects Firefox for iOS < 141.
CVE-2025-54474	A SQLi vulnerability in DJ-Classifieds component 3.9.2-3.10.1 for Joomla was discovered. The issue allows privileged users to execute arbitrary SQL commands.
CVE-2012-10058	RabidHamster R4 v1.25 contains a stack-based buffer overflow vulnerability due to unsafe use of sprintf() when logging malformed HTTP requests. A remote attack exploit this flaw by sending a specially crafted URI, resulting in arbitrary code execution under the context of the web server process.
CVE-2011-10010	QuickShare File Server 1.2.1 contains a path traversal vulnerability in its FTP service due to improper sanitation of user-supplied file paths. Authenticated users car this flaw by submitting crafted sequences to access or write files outside the intended virtual directory. When the "Writable" option is enabled (default during accou creation), this allows attackers to upload arbitrary files to privileged locations such as system32, enabling remote code execution via MOF injection or executable p
CVE-2025-38541	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7925: Fix null-ptr-deref in mt7925_thermal_init() devm_kasprintf() returns NULL on Currently, mt7925_thermal_init() does not check for this case, which results in a NULL pointer dereference. Add NULL check after devm_kasprintf() to prevent this i
CVE-2025-38547	In the Linux kernel, the following vulnerability has been resolved: iio: adc: axp20x_adc: Add missing sentinel to AXP717 ADC channel maps The AXP717 ADC chann missing a sentinel entry at the end. This causes a KASAN warning. Add the missing sentinel entry.
CVE-2025-38546	In the Linux kernel, the following vulnerability has been resolved: atm: clip: Fix memory leak of struct clip_vcc. ioctl(ATMARP_MKIP) allocates struct clip_vcc and set >user_back. The code assumes that vcc_destroy_socket() passes NULL skb to vcc->push() when the socket is close()d, and then clip_push() frees clip_vcc. Howeve ioctl(ATMARPD_CTRL) sets NULL to vcc->push() in atm_init_atmarp(), resulting in memory leak. Let's serialise two ioctl() by lock_sock() and check vcc->push() in atm_init_atmarp() to prevent memleak.
CVE-2025-38545	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: ti: am65-cpsw-nuss: Fix skb size by accounting for skb_shared_info While transition netdev_alloc_ip_align() to build_skb(), memory for the "skb_shared_info" member of an "skb" was not allocated. Fix this by allocating "PAGE_SIZE" as the skb length accounting for the packet length, headroom and tailroom, thereby including the required memory space for skb_shared_info.
CVE-2025-38544	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix bug due to prealloc collision When userspace is using AF_RXRPC to provide a server, it preallocate incoming calls and assign to them call IDs that will be used to thread related recvmsg() and sendmsg() together. The preallocated call IDs will automati attached to calls as they come in until the pool is empty. To the kernel, the call IDs are just arbitrary numbers, but userspace can use the call ID to hold a pointer t prepared structs. In any case, the user isn't permitted to create two calls with the same call ID (call IDs become available again when the call ends) and EBADSLT s result from sendmsg() if an attempt is made to preallocate a call with an in-use call ID. However, the cleanup in the error handling will trigger both assertions in rxrpc_cleanup_call() because the call isn't marked complete and isn't marked as having been released. Fix this by setting the call state in rxrpc_service_prealloc_or then marking it as being released before calling the cleanup function.
CVE-2025-38543	In the Linux kernel, the following vulnerability has been resolved: drm/tegra: nvdec: Fix dma_alloc_coherent error check Check for NULL return value with dma_alloc_coherent, in line with Robin's fix for vic.c in 'drm/tegra: vic: Fix DMA API misuse'.
CVE-2025-38542	In the Linux kernel, the following vulnerability has been resolved: net: appletalk: Fix device refcount leak in atrtr_create() When updating an existing route entry in atrtr_create(), the old device reference was not being released before assigning the new device, leading to a device refcount leak. Fix this by calling dev_put() to re old device reference before holding the new one.
CVE-2025-38540	In the Linux kernel, the following vulnerability has been resolved: HID: quirks: Add quirk for 2 Chicony Electronics HP 5MP Cameras The Chicony Electronics HP 5MP (USB ID 04F2:B824 & 04F2:B82C) report a HID sensor interface that is not actually implemented. Attempting to access this non-functional sensor via iio_info causes hangs as runtime PM tries to wake up an unresponsive sensor. Add these 2 devices to the HID ignore list since the sensor interface is non-functional by design and not be exposed to userspace.
CVE-2025-38549	In the Linux kernel, the following vulnerability has been resolved: efivarfs: Fix memory leak of efivarfs_fs_info in fs_context error paths When processing mount opt efivarfs allocates efivarfs_fs_info (sfi) early in fs_context initialization. However, sfi is associated with the superblock and typically freed when the superblock is des the fs_context is released (final put) before fill_super is called—such as on error paths or during reconfiguration—the sfi structure would leak, as ownership never tr the superblock. Implement the .free callback in efivarfs_context_ops to ensure any allocated sfi is properly freed if the fs_context is torn down before fill_super, pre this memory leak.

CVE-2025-38539	In the Linux kernel, the following vulnerability has been resolved: tracing: Add down_write(trace_event_sem) when adding trace event When a module is loaded, it trace events defined by the module. It may also need to modify the modules trace printk formats to replace enum names with their values. If two modules are load same time, the adding of the event to the ftrace_events list can corrupt the walking of the list in the code that is modifying the printk format strings and crash the The addition of the event should take the trace_event_sem for write while it adds the new event. Also add a lockdep_assert_held() on that semaphore in __trace_add_event_dirs() as it iterates the list.
CVE-2025-38538	In the Linux kernel, the following vulnerability has been resolved: dmaengine: nbpfaxi: Fix memory corruption in probe() The nbpf->chan[] array is allocated earlier nbpf_probe() function and it has "num_channels" elements. These three loops iterate one element farther than they should and corrupt memory. The changes to th loop are more involved. In this case, we're copying data from the irqbuf[] array into the nbpf->chan[] array. If the data in irqbuf[i] is the error IRQ then we skip it, s iterators are not in sync. I added a check to ensure that we don't go beyond the end of the irqbuf[] array. I'm pretty sure this can't happen, but it seemed harmless check. On the other hand, after the loop has ended there is a check to ensure that the "chan" iterator is where we expect it to be. In the original code we went one beyond the end of the array so the iterator wasn't in the correct place and it would always return -EINVAL. However, now it will always be in the correct place. I del check since we know the result.
CVE-2025-38537	In the Linux kernel, the following vulnerability has been resolved: net: phy: Don't register LEDs for genphy If a PHY has no driver, the genphy driver is probed/remo directly in phy_attach/detach. If the PHY's ofnode has an "leds" subnode, then the LEDs will be (un)registered when probing/removing the genphy driver. This could the leds are for a non-generic driver that isn't loaded for whatever reason. Synchronously removing the PHY device in phy_detach leads to the following deadlock: ndo_close() ... phy_detach() phy_remove() phy_leds_unregister() led_classdev_unregister() led_trigger_set() netdev_trigger_deactivate() unregister_netdevice_notifi rtnl_lock() There is a corresponding deadlock on the open/register side of things (and that one is reported by lockdep), but it requires a race while this one is deterr Generic PHYs do not support LEDs anyway, so don't bother registering them.
CVE-2025-38536	In the Linux kernel, the following vulnerability has been resolved: net: airoha: fix potential use-after-free in airoha_npu_get() np->name was being used after calling of_node_put(np), which releases the node and can lead to a use-after-free bug. Previously, of_node_put(np) was called unconditionally after of_find_device_by_node which could result in a use-after-free if pdev is NULL. This patch moves of_node_put(np) after the error check to ensure the node is only released after both the erro success cases are handled appropriately, preventing potential resource issues.
CVE-2025-38535	In the Linux kernel, the following vulnerability has been resolved: phy: tegra: xusb: Fix unbalanced regulator disable in UTMI PHY mode When transitioning from USB_ROLE_DEVICE to USB_ROLE_NONE, the code assumed that the regulator should be disabled. However, if the regulator is marked as always-on, regulator_is_en continues to return true, leading to an incorrect attempt to disable a regulator which is not enabled. This can result in warnings such as: [250.155624] WARNING: PID: 7326 at drivers/regulator/core.c:3004 _regulator_disable+0xe4/0x1a0 [250.155652] unbalanced disables for VIN_SYS_5V0 To fix this, we move the regulator c logic into tegra186_xusb_padctl_id_override() function since it's directly related to the ID override state. The regulator is now only disabled when the role transition USB_ROLE_HOST to USB_ROLE_NONE, by checking the VBUS_ID register. This ensures that regulator enable/disable operations are properly balanced and only occu actually transitioning to/from host mode.
CVE-2025-38534	In the Linux kernel, the following vulnerability has been resolved: netfs: Fix copy-to-cache so that it performs collection with ceph+fscache The netfs copy-to-cache used by Ceph with local caching sets up a new request to write data just read to the cache. The request is started and then left to look after itself whilst the app co The request gets notified by the backing fs upon completion of the async DIO write, but then tries to wake up the app because NETFS_RREQ_OFFLOAD_COLLECTIO - but the app isn't waiting there, and so the request just hangs. Fix this by setting NETFS_RREQ_OFFLOAD_COLLECTION which causes the notification from the back filesystem to put the collection onto a work queue instead.
CVE-2025-38548	In the Linux kernel, the following vulnerability has been resolved: hwmon: (corsair-cpro) Validate the size of the received input buffer Add buffer_recv_size to store of the received bytes. Validate buffer_recv_size in send_usb_cmd().
CVE-2025-38550	In the Linux kernel, the following vulnerability has been resolved: ipv6: mcast: Delay put pmc->idev in mld_del_delrec() pmc->idev is still used in ip6_mc_clear_src mld_clear_delrec() does, the reference should be put after ip6_mc_clear_src() return.
CVE-2011-10011	WeBid 1.0.2 contains a remote code injection vulnerability in the converter.php script, where unsanitized input in the to parameter of a POST request is written dire includes/currencies.php. This allows unauthenticated attackers to inject arbitrary PHP code, resulting in persistent remote code execution when the modified script accessed or included by the application.
CVE-2023-4130	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix wrong next length validation of ea buffer in smb2_set_ea() There are multiple smb2_ea buffers in FILE_FULL_EA_INFORMATION request from client. ksmbd find next smb2_ea_info using ->NextEntryOffset of current smb2_ea_info. ksmbd need to validat length Before accessing the next ea. ksmbd should check buffer length using buf_len, not next variable. next is the start offset of current ea that got from previous
CVE-2025-55284	Claude Code is an agentic coding tool. Prior to version 1.0.4, it's possible to bypass the Claude Code confirmation prompts to read a file and then send file contents network without user confirmation due to an overly broad allowlist of safe commands. Reliably exploiting this requires the ability to add untrusted content into a Cl Code context window. Users on standard Claude Code auto-update received this fix automatically after release. Current users of Claude Code are unaffected, as ve prior to 1.0.24 are deprecated and have been forced to update.
CVE-2025-7971	A security issues exists within Studio 5000 Logix Designer due to unsafe handling of environment variables. If the specified path lacks a valid file, Logix Designer cr However, it may be possible to execute malicious code without triggering a crash.
CVE-2025-7972	A security issue exists within the FactoryTalk Linx Network Browser. By modifying the process.env.NODE_ENV to ‘development’, the attacker can disable FTSP toke validation. This bypass allows access to create, update, and delete FTLinx drivers.
CVE-2025-9041	A security issue exists due to improper handling of CIP Class 32’s request when a module is inhibited on the 5094-IF8 device. It causes the module to enter a fault s the Module LED flashing red. Upon un-inhibiting, the module returns a connection fault (Code 16#0010), and the module cannot recover without a power cycle.
CVE-2025-9042	A security issue exists due to improper handling of CIP Class 32’s request when a module is inhibited on the 5094-IY8 device. It causes the module to enter a fault s the Module LED flashing red. Upon un-inhibiting, the module returns a connection fault (Code 16#0010), and the module cannot recover without a power cycle.
CVE-2023-4515	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate command request size In commit 2b9b8f3b68ed ("ksmbd: validate command pa size"), except for SMB2_OPLOCK_BREAK_HE command, the request size of other commands is not checked, it's not expected. Fix it by add check for request size of commands.
CVE-2023-3867	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix out of bounds read in smb2_sess_setup ksmbd does not consider the case of that smb setup is in compound request. If this is the second payload of the compound, OOB read issue occurs while processing the first payload in the smb2_sess_setup().
CVE-2025-38551	In the Linux kernel, the following vulnerability has been resolved: virtio-net: fix recursived rtnl_lock() during probe() The deadlock appears in a stack trace like: virtnet_probe() rtnl_lock() virtio_config_changed_work() netdev_notify_peers() rtnl_lock() It happens if the VMM sends a VIRTIO_NET_S_ANNOUNCE request while the driver is still probing. The config_work in probe() will get scheduled until virtnet_open() enables the config change notification via virtio_config_driver_enable().

CVE-2023-3866	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate session id and tree id in the compound request This patch validate session id and compound request. If first operation in the compound is SMB2 ECHO request, ksmbd bypass session and tree validation. So work->sess and work->tcon could be N secound request in the compound access work->sess or tcon, It cause NULL pointer dereferecing error.
CVE-2023-3865	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix out-of-bound read in smb2_write ksmbd_smb2_check_message doesn't validate hdr->NextCommand. If ->NextCommand is bigger than Offset + Length of smb2 write, It will allow oversized smb2 write length. It will cause OOB read in smb2_write.
CVE-2023-32249	In the Linux kernel, the following vulnerability has been resolved: ksmbd: not allow guest user on multichannel This patch return STATUS_NOT_SUPPORTED if bindi is guest.
CVE-2023-32246	In the Linux kernel, the following vulnerability has been resolved: ksmbd: call rcu_barrier() in ksmbd_server_exit() racy issue is triggered the bug by racing betwee connection and rmmod. In ksmbd, rcu_barrier() is not called at module unload time, so nothing prevents ksmbd from getting unloaded while it still has RCU callbac pending. It leads to trigger unintended execution of kernel code locally and use to defeat protections such as Kernel Lockdown
CVE-2025-53631	flaskBlog is a blog app built with Flask. In versions 2.8.1 and prior, improper sanitization of postContent when submitting POST requests to /createpost leads to arbi JavaScript execution (XSS) on all pages the post is reflected on including /, /post/[ID], /admin/posts, and /user/[ID] of the user that made the post. At time of publica there are no public patches available.
CVE-2025-38552	In the Linux kernel, the following vulnerability has been resolved: mptcp: plug races between subflow fail and subflow creation We have races similar to the one ad by the previous patch between subflow failing and additional subflow creation. They are just harder to trigger. The solution is similar. Use a separate flag to track t condition 'socket state prevent any additional subflow creation' protected by the fallback lock. The socket fallback makes such flag true, and also receiving or send MP_FAIL option. The field 'allow_infinite_fallback' is now always touched under the relevant lock, we can drop the ONCE annotation on write.
CVE-2025-38533	In the Linux kernel, the following vulnerability has been resolved: net: libwx: fix the using of Rx buffer DMA The wx_rx_buffer structure contained two DMA address 'dma' and 'page_dma'. However, only 'page_dma' was actually initialized and used to program the Rx descriptor. But 'dma' was uninitialized and used in some path could lead to undefined behavior, including DMA errors or use-after-free, if the uninitialized 'dma' was used. Although such error has not yet occurred, it is worth fi the code.
CVE-2025-38532	In the Linux kernel, the following vulnerability has been resolved: net: libwx: properly reset Rx ring descriptor When device reset is triggered by feature changes su toggling Rx VLAN offload, wx->do_reset() is called to reinitialize Rx rings. The hardware descriptor ring may retain stale values from previous sessions. And only se length to 0 in rx_desc[0] would result in building malformed SKBs. Fix it to ensure a clean slate after device reset. [549.186435] [C16] ------------[cut here]---------- 549.186457] [C16] kernel BUG at net/core/skbuff.c:2814! [549.186468] [C16] Oops: invalid opcode: 0000 [#1] SMP NOPTI [549.186472] [C16] CPU: 16 UID: 0 PI Comm: swapper/16 Kdump: loaded Not tainted 6.16.0-rc4+ #23 PREEMPT(voluntary) [549.186476] [C16] Hardware name: Micro-Star International Co., Ltd. MS-7I GAMING PLUS WIFI (MS-7E16), BIOS 1.90 12/31/2024 [549.186478] [C16] RIP: 0010:__pskb_pull_tail+0x3ff/0x510 [549.186484] [C16] Code: 06 f0 ff 4f 34 74 7b 24 c8 00 00 00 45 8b 84 24 c0 00 00 00 e9 c8 fd ff ff 48 c7 44 24 08 00 00 00 00 e9 5e fe ff ff <0f> 0b 31 c0 e9 23 90 5b ff 41 f7 c6 ff 0f 00 00 75 bf 49 8b 06 a8 [549.186487] [C16] RSP: 0018:ffffb391c0640d70 EFLAGS: 00010282 [549.186490] [C16] RAX: 00000000ffffffff2 RBX: ffff8fe7e4d40200 RCX: 00000000ffffffff2 [549 [C16] RDX: ffff8fe7c3a4bf8e RSI: 0000000000000180 RDI: ffff8fe7c3a4bf40 [549.186494] [C16] RBP: ffffb391c0640da8 R08: ffff8fe7c3a4c0c0 R09: 00000000000 549.186496] [C16] R10: ffffb391c0640d88 R11: 0000000000000000e R12: ffff8fe7e4d40200 [549.186497] [C16] R13: 00000000ffffffff2 R14: ffff8fe7fa01a000 R15 00000000ffffffff2 [549.186499] [C16] FS: 0000000000000000(0000) GS:ffff8fef5ae40000(0000) knlGS:0000000000000000 [549.186502] [C16] CS: 0010 DS: 000 0000 CR0: 0000000080050033 [549.186503] [C16] CR2: 00007f77d81d6000 CR3: 000000051a032000 CR4: 0000000000750ef0 [549.186505] [C16] PKRU: 555 549.186507] [C16] Call Trace: [549.186510] [C16] <IRQ> [549.186513] [C16] ? srso_alias_return_thunk+0x5/0xfbef5 [549.186517] [C16] __skb_pad+0xc7/0x 549.186523] [C16] wx_clean_rx_irq+0x355/0x3b0 [libwx] [549.186533] [C16] wx_poll+0x92/0x120 [libwx] [549.186540] [C16] __napi_poll+0x28/0x190 [549.1 C16] net_rx_action+0x301/0x3f0 [549.186548] [C16] ? srso_alias_return_thunk+0x5/0xfbef5 [549.186551] [C16] ? __raw_spin_lock_irqsave+0x1e/0x50 [549.18 C16] ? srso_alias_return_thunk+0x5/0xfbef5 [549.186557] [C16] ? wake_up_nohz_cpu+0x35/0x160 [549.186559] [C16] ? srso_alias_return_thunk+0x5/0xfbef5 [549.186563] [C16] handle_softirqs+0xf9/0x2c0 [549.186568] [C16] __irq_exit_rcu+0xc7/0x130 [549.186572] [C16] common_interrupt+0xb8/0xd0 [549.18657 </IRQ> [549.186577] [C16] <TASK> [549.186579] [C16] asm_common_interrupt+0x22/0x40 [549.186582] [C16] RIP: 0010:cpuidle_enter_state+0xc2/0x420 [549.186585] [C16] Code: 00 00 e8 11 0e 5e ff e8 ac f0 ff ff 49 89 c5 0f 1f 44 00 00 31 ff e8 0d ed 5c ff 45 84 ff 0f 85 40 02 00 00 fb 0f 1f 44 00 00 <45> 85 f6 0f 8 00 00 49 63 d6 48 8d 04 52 48 8d 04 82 49 8d [549.186587] [C16] RSP: 0018:ffffb391c0277e78 EFLAGS: 00000246 [549.186590] [C16] RAX: ffff8fef5ae40000 F 0000000000000003 RCX: 0000000000000000 [549.186591] [C16] RDX: 0000007fde0faac5 RSI: ffffffff826e53f6 RDI: ffffffff826fa9b3 [549.186593] [C16] RBP: ffff8fe7c3a20800 R08: 0000000000000002 R09: 0000000000000000 [549.186595] [C16] R10: 0000000000000000 R11: 000000000000ffff R12: ffffffff82ed7a40 [549.186596] [C16] R13: 0000007fde0faac5 R14: 0000000000000003 R15: 0000000000000000 [549.186601] [C16] ? cpuidle_enter_state+0xb3/0x420 [549.186 C16] cpuidle_en ---truncated---
CVE-2025-38531	In the Linux kernel, the following vulnerability has been resolved: iio: common: st_sensors: Fix use of uninitialize device structs Throughout the various probe funct &indio_dev->dev is used before it is initialized. This caused a kernel panic in st_sensors_power_enable() when the call to devm_regulator_bulk_get_enable() fails an calls dev_err_probe() with the uninitialized device. This seems to only cause a panic with dev_err_probe(), dev_err(), dev_warn() and dev_info() don't seem to cause but are fixed as well. The issue is reported and traced here: [1]
CVE-2025-38507	In the Linux kernel, the following vulnerability has been resolved: HID: nintendo: avoid bluetooth suspend/resume stalls Ensure we don't stall or panic the kernel wh bluetooth-connected controllers. This was reported as an issue on android devices using kernel 6.6 due to the resume hook which had been added for usb joycons. a new state value to JOYCON_CTLR_STATE_SUSPENDED in a newly-added nintendo_hid_suspend. This makes sure we will not stall out the kernel waiting for input re during led classdev suspend. The stalls could happen if connectivity is unreliable or lost to the controller prior to suspend. Second, since we lose connectivity durin suspend, do not try joycon_init() for bluetooth controllers in the nintendo_hid_resume path. Tested via multiple suspend/resume flows when using the controller bo and bluetooth modes.
CVE-2025-38513	In the Linux kernel, the following vulnerability has been resolved: wifi: zd1211rw: Fix potential NULL pointer dereference in zd_mac_tx_to_dev() There is a potential pointer dereference in zd_mac_tx_to_dev(). For example, the following is possible: T0 T1 zd_mac_tx_to_dev() /* len == skb_queue_len(q) */ while (len > ZD_MAC_MAX_ACK_WAITERS) { filter_ack() spin_lock_irqsave(&q->lock, flags); /* position == skb_queue_len(q) */ for (i=1; i<position; i++) skb = __skb_dequeue(q >type == NL80211_IFTYPE_AP) skb = __skb_dequeue(q); spin_unlock_irqrestore(&q->lock, flags); skb_dequeue() -> NULL Since there is a small gap between check queue length and skb being unconditionally dequeued in zd_mac_tx_to_dev(), skb_dequeue() can return NULL. Then the pointer is passed to zd_mac_tx_status() wh dereferenced. In order to avoid potential NULL pointer dereference due to situations like above, check if skb is not NULL before passing it to zd_mac_tx_status(). Fo Linux Verification Center (linuxtesting.org) with SVACE.
CVE-2025-38512	In the Linux kernel, the following vulnerability has been resolved: wifi: prevent A-MSDU attacks in mesh networks This patch is a mitigation to prevent the A-MSDU vulnerability for mesh networks. The initial update to the IEEE 802.11 standard, in response to the FragAttacks, missed this case (CVE-2025-27558). It can be consi variant of CVE-2020-24588 but for mesh networks. This patch tries to detect if a standard MSDU was turned into an A-MSDU by an adversary. This is done by parsi received A-MSDU as a standard MSDU, calculating the length of the Mesh Control header, and seeing if the 6 bytes after this header equal the start of an rfc1042 h equal, this is a strong indication of an ongoing attack attempt. This defense was tested with mac80211_hwsim against a mesh network that uses an empty Mesh A Extension field, i.e., when four addresses are used, and when using a 12-byte Mesh Address Extension field, i.e., when six addresses are used. Functionality of norr MSDUs and A-MSDUs was also tested, and confirmed working, when using both an empty and 12-byte Mesh Address Extension field. It was also tested with mac80211_hwsim that A-MSDU attacks in non-mesh networks keep being detected and prevented. Note that the vulnerability being patched, and the defense bein implemented, was also discussed in the following paper and in the following IEEE 802.11 presentation: https://papers.mathyvanhoef.com/wisec2025.pdf https://mentor.ieee.org/802.11/dcn/25/11-25-0949-00-000m-a-msdu-mesh-spoof-protection.docx

CVE-2025-38511	In the Linux kernel, the following vulnerability has been resolved: drm/xe/pf: Clear all LMTT pages on alloc Our LMEM buffer objects are not cleared by default on al during VF provisioning we only setup LMTT PTEs for the actually provisioned LMEM range. But beyond that valid range we might leave some stale data that could e to some other VFs allocations or even to the PF pages. Explicitly clear all new LMTT page to avoid the risk that a malicious VF would try to exploit that gap. While a asserts to catch any undesired PTE overwrites and low-level debug traces to track LMTT PT life-cycle. (cherry picked from commit 3fae6918a3e27cce20ded2551f863fb05d4bef8d)
CVE-2025-38510	In the Linux kernel, the following vulnerability has been resolved: kasan: remove kasan_find_vm_area() to prevent possible deadlock find_vm_area() couldn't be cal atomic_context. If find_vm_area() is called to reports vm area information, kasan can trigger deadlock like: CPU0 CPU1 vmalloc(); alloc_vmap_area(); spin_lock(&vn >busy.lock) spin_lock_bh(&some_lock); <interrupt occurs> <in softirq> spin_lock(&some_lock); <access invalid address> kasan_report(); print_report(); print_address_description(); kasan_find_vm_area(); find_vm_area(); spin_lock(&vn->busy.lock) // deadlock! To prevent possible deadlock while kasan reports, remo kasan_find_vm_area().
CVE-2025-38509	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: reject VHT opmode for unsupported channel widths VHT operating mode notifica not defined for channel widths below 20 MHz. In particular, 5 MHz and 10 MHz are not valid under the VHT specification and must be rejected. Without this check, r notifications using these widths may reach ieee80211_chan_width_to_rx_bw(), leading to a WARN_ON due to invalid input. This issue was reported by syzbot. Rejec unsupported widths early in sta_link_apply_parameters() when opmode_notif is used. The accepted set includes 20, 40, 80, 160, and 80+80 MHz, which are valid fo While 320 MHz is not defined for VHT, it is allowed to avoid rejecting HE or EHT clients that may still send a VHT opmode notification.
CVE-2025-38508	In the Linux kernel, the following vulnerability has been resolved: x86/sev: Use TSC_FACTOR for Secure TSC frequency calculation When using Secure TSC, the GUEST_TSC_FREQ MSR reports a frequency based on the nominal P0 frequency, which deviates slightly (typically ~0.2%) from the actual mean TSC frequency due clocking parameters. Over extended VM uptime, this discrepancy accumulates, causing clock skew between the hypervisor and a SEV-SNP VM, leading to early tim interrupts as perceived by the guest. The guest kernel relies on the reported nominal frequency for TSC-based timekeeping, while the actual frequency set during SNP_LAUNCH_START may differ. This mismatch results in inaccurate time calculations, causing the guest to perceive hrtimers as firing earlier than expected. Utilize TSC_FACTOR from the SEV firmware's secrets page (see "Secrets Page Format" in the SNP Firmware ABI Specification) to calculate the mean TSC frequency, ensuri accurate timekeeping and mitigating clock skew in SEV-SNP VMs. Use early_ioremap_encrypted() to map the secrets page as ioremap_encrypted() uses kmalloc() w not available during early TSC initialization and causes a panic. [bp: Drop the silly dummy var: https://lore.kernel.org/r/20250630192726.GBaGLIHl84xIopx4Pt@fat_crate.local]
CVE-2025-38506	In the Linux kernel, the following vulnerability has been resolved: KVM: Allow CPU to reschedule while setting per-page memory attributes When running an SEV-SN with a sufficiently large amount of memory (1TB+), the host can experience CPU soft lockups when running an operation in kvm_vm_set_mem_attributes() to set m attributes on the whole range of guest memory. watchdog: BUG: soft lockup - CPU#8 stuck for 26s! [qemu-kvm:6372] CPU: 8 UID: 0 PID: 6372 Comm: qemu-kvm K loaded Not tainted 6.15.0-rc7.20250520.el9uek.rc1.x86_64 #1 PREEMPT(voluntary) Hardware name: Oracle Corporation ORACLE SERVER E4-2c/Asm,MB Tray,2U,E4 78016600 11/13/2024 RIP: 0010:xas_create+0x78/0x1f0 Code: 00 00 00 41 80 fc 01 0f 84 82 00 00 00 ba 06 00 00 00 bd 06 00 00 00 49 8b 45 08 4d 8d 65 08 41 20 83 ed 06 48 85 c0 <74> 67 48 89 c2 83 e2 03 48 83 fa 02 75 0c 48 3d 00 10 00 00 0f 87 RSP: 0018:ffffad890a34b940 EFLAGS: 00000286 RAX: ffff96f30b261da ffffad890a34b9c8 RCX: 0000000000000000 RDX: 000000000000001e RSI: 0000000000000000 RDI: 0000000000000000 RBP: 0000000000000018 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffad890a356868 R13: ffffad890a356860 R14: 0000000000 R15: ffffad890a356868 FS: 00007f5578a2a400(0000) GS:ffff97ed317e1000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 000000008005003 00007f015c70fb18 CR3: 00000001109fd006 CR4: 0000000000f70ef0 PKRU: 55555554 Call Trace: <TASK> xas_store+0x58/0x630 __xa_store+0xa5/0x130 xa_store+0x2c/0x50 kvm_vm_set_mem_attributes+0x343/0x710 [kvm] kvm_vm_ioctl+0x796/0xab0 [kvm] __x64_sys_ioctl+0xa3/0xd0 do_syscall_64+0x8c/0x7a0 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7f5578d031bb Code: ff ff ff 85 c0 79 9b 49 c7 c4 ff ff ff ff 5b 5d 4c 89 e0 41 5c c3 66 0f 1f 84 00 00 00 1e fa b8 10 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 2d 4c 0f 00 f7 d8 64 89 01 48 RSP: 002b:00007ffe0a742b88 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 000000004020aed2 RCX: 00007f5578d031bb RDX: 00007ffe0a742c80 RSI: 000000004020aed2 RDI: 0000000000000 0000010000000000 R08: 0000010000000000 R09: 0000017680000000 R10: 0000000000000080 R11: 0000000000000246 R12: 00005575e5f95120 R13: 00007ffe0a742c80 R14: 0000000000000008 R15: 00005575e5f961e0 While looping through the range of memory setting the attributes, call cond_resched() to giv scheduler a chance to run a higher priority task on the runqueue if necessary and avoid staying in kernel mode long enough to trigger the lockup.
CVE-2025-38530	In the Linux kernel, the following vulnerability has been resolved: comedi: pcl812: Fix bit shift out of bounds When checking for a supported IRQ number, the follow used: if ((1 << it->options[1]) & board->irq_bits) { However, `it->options[i]` is an unchecked `int` value from userspace, so the shift amount could be negative or bounds. Fix the test by requiring `it->options[1]` to be within bounds before proceeding with the original test. Valid `it->options[1]` values that select the IRQ will range [1,15]. The value 0 explicitly disables the use of interrupts.
CVE-2025-38505	In the Linux kernel, the following vulnerability has been resolved: wifi: mwifiex: discard erroneous disassoc frames on STA interface When operating in concurrent S mode with host MLME enabled, the firmware incorrectly sends disassociation frames to the STA interface when clients disconnect from the AP interface. This cause warnings as the STA interface processes disconnect events that don't apply to it: [1303.240540] WARNING: CPU: 0 PID: 513 at net/wireless/mlme.c:141 cfg80211_process_disassoc+0x78/0xec [cfg80211] [1303.250861] Modules linked in: 8021q garp stp mrp llc rfcomm bnep btnxpuart nls_iso8859_1 nls_cp437 onb 1303.327651] CPU: 0 UID: 0 PID: 513 Comm: kworker/u9:2 Not tainted 6.16.0-rc1+ #3 PREEMPT [1303.335937] Hardware name: Toradex Verdin AM62 WB on Ver Development Board (DT) [1303.343588] Workqueue: MWIFIEX_RX_WORK_QUEUE mwifiex_rx_work_queue [mwifiex] [1303.350856] pstate: 60000005 (nZCv daif - -TCO -DIT -SSBS BTYPE=--) [1303.357904] pc : cfg80211_process_disassoc+0x78/0xec [cfg80211] [1303.364065] lr : cfg80211_process_disassoc+0x70/0xec [cfg 1303.370221] sp : ffff800083053be0 [1303.373590] x29: ffff800083053be0 x28: 0000000000000000 x27: 0000000000000000 [1303.380855] x26: 00000000000 x25: 00000000ffffffff x24: ffff000002c5b8ae [1303.388120] x23: ffff000002c5b884 x22: 0000000000000001 x21: 0000000000000008 [1303.395382] x20: ffff000002c5b8ae x19: ffff0000064dd408 x18: 0000000000000006 [1303.402646] x17: 3a36333a61623a30 x16: 32206d6f72662063 x15: ffff800080bfe048 [130 x14: ffff000003625300 x13: 0000000000000001 x12: 0000000000000000 [1303.417173] x11: 0000000000000002 x10: ffff000003958600 x9 : ffff000003625300 1303.424434] x8 : ffff00003fd9ef40 x7 : ffff0000039fc280 x6 : 0000000000000002 [1303.431695] x5 : ffff0000038976d4 x4 : 0000000000000000 x3 : 00000000 [1303.438956] x2 : 000000004836ba20 x1 : 0000000000006986 x0 : 00000000d00479de [1303.446221] Call trace: [1303.448722] cfg80211_process_disassoc+0x78/0xec [cfg80211] (P) [1303.454894] cfg80211_rx_mlme_mgmt+0x64/0xf8 [cfg80211] [1303.460362] mwifiex_process_mgmt_packet+0x1ec/0x460 [mwifiex] [1303.466380] mwifiex_process_sta_rx_packet+0x1bc/0x2a0 [mwifiex] [1303.472573] mwifiex_handle_rx_packet+0xb4/0x13c [mwifiex] [1303.478243] mwifiex_rx_work_queue+0x158/0x198 [mwifiex] [1303.483734] process_one_work+0x14c/0x28 1303.487845] worker_thread+0x2cc/0x3d4 [1303.491680] kthread+0x12c/0x208 [1303.495014] ret_from_fork+0x10/0x20 Add validation in the STA receive path that disassoc/deauth frames originate from the connected AP. Frames that fail this check are discarded early, preventing them from reaching the MLME layer and t WARN_ON(). This filtering logic is similar with that used in the ieee80211_rx_mgmt_disassoc() function in mac80211, which drops disassoc frames that don't match current BSSID (!ether_addr_equal(mgmt->bssid, sdata->vif.cfg.ap_addr)), ensuring only relevant frames are processed. Tested on: - 8997 with FW 16.68.1.p197
CVE-2025-38504	In the Linux kernel, the following vulnerability has been resolved: io_uring/zcrx: fix pp destruction warnings With multiple page pools and in some other cases we c allocated niovs on page pool destruction. Remove a misplaced warning checking that all niovs are returned to zcrx on io_pp_zc_destroy(). It was reported before bu apparently got lost.
	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix assertion when building free space tree When building the free space tree with the block tree feature enabled, we can hit an assertion failure like this: BTRFS info (device loop0 state M): rebuilding free space tree assertion failed: ret == 0, in fs/btrfs/free tree.c:1102 ----------[cut here]---------- kernel BUG at fs/btrfs/free-space-tree.c:1102! Internal error: Oops - BUG: 00000000f2000800 [#1] SMP Modules linked in: UID: 0 PID: 6592 Comm: syz-executor322 Not tainted 6.15.0-rc7-syzkaller-gd7fa1af5b33e #0 PREEMPT Hardware name: Google Google Compute Engine/Google Cc Engine, BIOS Google 05/07/2025 pstate: 60400005 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : populate_free_space_tree+0x514/0x518 fs/btrfs/free-spa tree.c:1102 lr : populate_free_space_tree+0x514/0x518 fs/btrfs/free-space-tree.c:1102 sp : ffff8000a4ce7600 x29: ffff8000a4ce76e0 x28: ffff0000c9bc6000 x27: ffff0000ddfff3d8 x26: ffff0000ddfff378 x25: dfff800000000000 x24: 0000000000000001 x23: ffff8000a4ce7660 x22: ffff70001499cecc x21: ffff0000e1d8c160 x20: ffff0000e1cb7800 x19: ffff0000e1d8c0b0 x18: 00000000ffffffff x17: ffff800092f39000 x16: ffff80008ad27e48 x15: ffff700011e740c0 x14: 1ffff00011e740c0 x13: 0000000000000004 x12: ffffffffffffffff x11: ffff700011e740c0 x10: 0000000000ff0100 x9 : 94ef24f55d2dbc00 x8 : 94ef24f55d2dbc00 x7 : 0000000000000001 x6 :

CVE-2025-38503	0000000000000001 x5 : ffff8000a4ce6f98 x4 : ffff80008f415ba0 x3 : ffff800080548ef0 x2 : 0000000000000000 x1 : 0000000100000000 x0 : 000000000000003e populate_free_space_tree+0x514/0x518 fs/btrfs/free-space-tree.c:1102 (P) btrfs_rebuild_free_space_tree+0x14c/0x54c fs/btrfs/free-space-tree.c:1337 btrfs_start_pre_rw_mount+0xa78/0xe10 fs/btrfs/disk-io.c:3074 btrfs_remount_rw fs/btrfs/super.c:1319 [inline] btrfs_reconfigure+0x828/0x2418 fs/btrfs/super.c:154 reconfigure_super+0x1d4/0x6f0 fs/super.c:1083 do_remount fs/namespace.c:3365 [inline] path_mount+0xb34/0xde0 fs/namespace.c:4200 do_mount fs/namespac [inline] __do_sys_mount fs/namespace.c:4432 [inline] __se_sys_mount fs/namespace.c:4409 [inline] __arm64_sys_mount+0x3e8/0x468 fs/namespace.c:4409 __invoke_syscall arch/arm64/kernel/syscall.c:35 [inline] invoke_syscall+0x98/0x2b8 arch/arm64/kernel/syscall.c:49 el0_svc_common+0x130/0x23c arch/arm64/kernel/syscall.c:132 do_el0_svc+0x48/0x58 arch/arm64/kernel/syscall.c:151 el0_svc+0x58/0x17c arch/arm64/kernel/entry-common.c:767 el0t_64_sync_handler+0x78/0x108 arch/arm64/kernel/entry-common.c:786 el0t_64_sync+0x198/0x19c arch/arm64/kernel/entry.S:600 Code: f0047182 91178042 9771d47b (d4210000) ---[end trace 0000000000000000]--- This happens because we are processing an empty block group, which has no extents allocated from i are no items for this block group, including the block group item since block group items are stored in a dedicated tree when using the block group tree feature. It means this is the block group with the highest start offset, so there are no higher keys in the extent root, hence btrfs_search_slot_for_read() returns 1 (no higher ke Fix this by asserting 'ret' is 0 only if the block group tree feature is not enabled, in which case we should find a block group item for the block group since it's store extent root and block group item keys are greater than extent item keys (the value for BTRFS_BLOCK_GROUP_ITEM_KEY is 192 and for BTRFS_EXTENT_ITEM_KEY a BTRFS_METADATA_ITEM_KEY the values are 168 and 169 respectively). In case 'ret' is 1, we just need to add a record to the free space tree which spans the whole group, and we can achieve this by making 'ret == 0' as the while loop's condition.
CVE-2025-38502	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix oob access in cgroup local storage Lonial reported that an out-of-bounds access in cgroup storage can be crafted via tail calls. Given two programs each utilizing a cgroup local storage with a different value size, and one program doing a tail call into the verifier will validate each of the indivial programs just fine. However, in the runtime context the bpf_cg_run_ctx holds an bpf_prog_array_item which contains the B program as well as any cgroup local storage flavor the program uses. Helpers such as bpf_get_local_storage() pick this up from the runtime context: ctx = container_of(current->bpf_ctx, struct bpf_cg_run_ctx, run_ctx); storage = ctx->prog_item->cgroup_storage[stype]; if (stype == BPF_CGROUP_STORAGE_SHARED) &READ_ONCE(storage->buf)->data[0]; else ptr = this_cpu_ptr(storage->percpu_buf); For the second program which was called from the originally attached one, th bpf_get_local_storage() will pick up the former program's map, not its own. With mismatching sizes, this can result in an unintended out-of-bounds access. To fix th we need to extend bpf_map_owner with an array of storage_cookie[] to match on i) the exact maps from the original program if the second program was using bpf_get_local_storage(), or ii) allow the tail call combination if the second program was not using any of the cgroup local storage maps.
CVE-2025-55192	HomeAssistant-Tapo-Control offers Control for Tapo cameras as a Home Assistant component. Prior to commit 2a3b80f, there is a code injection vulnerability in the Actions workflow .github/workflows/issues.yml. It does not affect users of the Home Assistant integration itself — it only impacts the GitHub Actions environment fo repository. The vulnerable workflow directly inserted user-controlled content from the issue body (github.event.issue.body) into a Bash conditional without proper sanitization. A malicious GitHub user could craft an issue body that executes arbitrary commands on the GitHub Actions runner in a privileged context whenever ar opened. The potential impact is limited to the repository's CI/CD environment, which could allow access to repository contents or GitHub Actions secrets. This issue patched via commit 2a3b80f. Workarounds involve disabling the affected workflow (issues.yml), replacing the unsafe Bash comparison with a safe quoted grep (or GitHub Actions expression check), or ensuring minimal permissions in workflows (permissions: block) to reduce possible impact.
CVE-2025-38501	In the Linux kernel, the following vulnerability has been resolved: ksmbd: limit repeated connections from clients with the same IP Repeated connections from clien the same IP address may exhaust the max connections and prevent other normal client connections. This patch limit repeated connections from clients with the sa
CVE-2025-38514	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix oops due to non-existence of prealloc backlog struct If an AF_RXRPC service socket is o and bound, but calls are preallocated, then rxrpc_alloc_incoming_call() will oops because the rxrpc_backlog struct doesn't get allocated until the first preallocation Fix this by returning NULL from rxrpc_alloc_incoming_call() if there is no backlog struct. This will cause the incoming call to be aborted.
CVE-2025-38515	In the Linux kernel, the following vulnerability has been resolved: drm/sched: Increment job count before swapping tail spsc queue A small race exists between spsc_queue_push and the run-job worker, in which spsc_queue_push may return not-first while the run-job worker has already idled due to the job count being zero race occurs, job scheduling stops, leading to hangs while waiting on the job's DMA fences. Seal this race by incrementing the job count before appending to the SP This race was observed on a drm-tip 6.16-rc1 build with the Xe driver in an SVM test case.
CVE-2025-38516	In the Linux kernel, the following vulnerability has been resolved: pinctrl: qcom: msm: mark certain pins as invalid for interrupts On some platforms, the UFS-reset interrupt logic in TLMM but is nevertheless registered as a GPIO in the kernel. This enables the user-space to trigger a BUG() in the pinctrl-msm driver by running, f example: `gpiomon -c 0 113` on RB2. The exact culprit is requesting pins whose intr_detection_width setting is not 1 or 2 for interrupts. This hits a BUG() in msm_gpio_irq_set_type(). Potentially crashing the kernel due to an invalid request from user-space is not optimal, so let's go through the pins and mark those that the check as invalid for the irq chip as we should not even register them as available irqs. This function can be extended if we determine that there are more corne like this.
CVE-2025-38517	In the Linux kernel, the following vulnerability has been resolved: lib/alloc_tag: do not acquire non-existent lock in alloc_tag_top_users() alloc_tag_top_users() attem lock alloc_tag_cttype->mod_lock even when the alloc_tag_cttype is not allocated because: 1) alloc tagging is disabled because mem profiling is disabled (!alloc_tag 2) alloc tagging is enabled, but not yet initialized (!alloc_tag_cttype) 3) alloc tagging is enabled, but failed initialization (!alloc_tag_cttype or IS_ERR(alloc_tag_cttyp cases, alloc_tag_cttype is not allocated, and therefore alloc_tag_top_users() should not attempt to acquire the semaphore. This leads to a crash on memory allocati by attempting to acquire a non-existent semaphore: Oops: general protection fault, probably for non-canonical address 0xdfffffc000000001b: 0000 [#3] SMP KASAN KASAN: null-ptr-deref in range [0x00000000000000d8-0x00000000000000df] CPU: 2 UID: 0 PID: 1 Comm: systemd Tainted: G D 6.16.0-rc2 #1 VOLUNTARY Tainted Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.2-debian-1.16.2-1 04/01/2014 RIP: 0010:down_read_trylock+0xaa/0x3b0 Code: d0 7c 08 84 c a0 02 00 00 8b 0d df 31 dd 04 85 c9 75 29 48 b8 00 00 00 00 00 fc ff df 48 8d 6b 68 48 89 ea 48 c1 ea 03 <80> 3c 02 00 0f 85 88 02 00 00 48 3b 5b 68 0f 85 53 65 ff RSP: 0000:ffff8881002ce9b8 EFLAGS: 00010016 RAX: dfffffc0000000000 RBX: 0000000000000070 RCX: 0000000000000000 RDX: 000000000000001b RSI: 000000000000000a RDI: 0000000000000070 RBP: 00000000000000d8 R08: 0000000000000001 R09: ffffed107dde49d1 R10: ffff8883eef24e8b R11: ffff8881002c 1ffff11020059d37 R13: 00000000003fff7b R14: ffff8881002cec20 R15: dfffffc0000000000 FS: 00007f963f21d940(0000) GS:ffff888458ca6000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f963f5edf71 CR3: 0000000010672c000 CR4: 0000000000350ef0 Call <TASK> codetag_trylock_module_list+0xd/0x20 alloc_tag_top_users+0x369/0x4b0 __show_mem+0x1cd/0x6e0 warn_alloc+0x2b1/0x390 __alloc_frozen_pages_noprof+0x12b9/0x21a0 alloc_pages_mpol+0x135/0x3e0 alloc_slab_page+0x82/0xe0 new_slab+0x212/0x240 ___slab_alloc+0x82a/0xe00 </ David Wang points out, this issue became easier to trigger after commit 780138b12381 ("alloc_tag: check mem_profiling_support in alloc_tag_init"). Before the cor issue occurred only when it failed to allocate and initialize alloc_tag_cttype or if a memory allocation fails before alloc_tag_init() is called. After the commit, it can b triggered when memory profiling is compiled but disabled at boot. To properly determine whether alloc_tag_init() has been called and its data structures initialized that alloc_tag_cttype is a valid pointer before acquiring the semaphore. If the variable is NULL or an error value, it has not been properly initialized. In such a case, and do not attempt to acquire the semaphore. [harry.yoo@oracle.com: v3]
CVE-2025-38518	In the Linux kernel, the following vulnerability has been resolved: x86/CPU/AMD: Disable INVLPGB on Zen2 AMD Cyan Skillfish (Family 17h, Model 47h, Stepping 0h issue that causes system oopses and panics when performing TLB flush using INVLPGB. However, the problem is that that machine has misconfigured CPUID and s report the INVLPGB bit in the first place. So zap the kernel's representation of the flag so that nothing gets confused. [bp: Massage.]
CVE-2025-38519	In the Linux kernel, the following vulnerability has been resolved: mm/damon: fix divide by zero in damon_get_intervals_score() The current implementation allows zero size regions with no special reasons, but damon_get_intervals_score() gets crashed by divide by zero when the region size is zero. [29.403950] Oops: divide e [#1] SMP NOPTI This patch fixes the bug, but does not disallow zero size regions to keep the backward compatibility since disallowing zero size regions might be a change for some users. In addition, the same crash can happen when intervals_goal.access_bp is zero so this should be fixed in stable trees as well.
	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Don't call mmput from MMU notifier callback If the process is exiting, the mmput ins notifier callback from compactd or fork or numa balancing could release the last reference of mm struct to call exit_mmap and free_pgtable, this triggers deadlock below backtrace. The deadlock will leak kfd process as mmu notifier release is not called and cause VRAM leaking. The fix is to take mm reference mmget_non_zer

CVE-2025-38520	adding prange to the deferred list to pair with mmput in deferred list work. If prange split and add into pchild list, the pchild work_item.mm is not used, so remove parameter from svm_range_unmap_split and svm_range_add_child. The backtrace of hung task: INFO: task python:348105 blocked for more than 64512 seconds. __schedule+0x1c3/0x550 schedule+0x46/0xb0 rwsem_down_write_slowpath+0x24b/0x4c0 unlink_anon_vmas+0xb1/0x1c0 free_pgtables+0xa9/0x130 exit_mmap+0xbc/0x1a0 mmput+0x5a/0x140 svm_range_cpu_invalidate_pagetables+0x2b/0x40 [amdgpu] mn_itree_invalidate+0x72/0xc0 __mmu_notifier_invalidate_range_start+0x48/0x60 try_to_unmap_one+0x10fa/0x1400 rmap_walk_anon+0x196/0x460 try_to_unmap+0xbb/0x210 migrate_page_unmap+0x54d/0x7e0 migrate_pages_batch+0x1c3/0xae0 migrate_pages_sync+0x98/0x240 migrate_pages+0x25c/0x520 compact_zone+0x29d/0x compact_zone_order+0xb6/0xf0 try_to_compact_pages+0xbe/0x220 __alloc_pages_direct_compact+0x96/0x1a0 __alloc_pages_slowpath+0x410/0x930 __alloc_pages_nodemask+0x3a9/0x3e0 do_huge_pmd_anonymous_page+0xd7/0x3e0 __handle_mm_fault+0x5e3/0x5f0 handle_mm_fault+0xf7/0x2e0 hmm_vma_fault.isra.0+0x4d/0xa0 walk_pmd_range.isra.0+0xa8/0x310 walk_pud_range+0x167/0x240 walk_pgd_range+0x55/0x100 __walk_page_range+0x87/0x walk_page_range+0xf6/0x160 hmm_range_fault+0x4f/0x90 amdgpu_hmm_range_get_pages+0x123/0x230 [amdgpu] amdgpu_ttm_tt_get_user_pages+0xb1/0x15 [amdgpu] init_user_pages+0xb1/0x2a0 [amdgpu] amdgpu_amdkfd_gpuvm_alloc_memory_of_gpu+0x543/0x7d0 [amdgpu] kfd_ioctl_alloc_memory_of_gpu+0x24c/ [amdgpu] kfd_ioctl+0x29d/0x500 [amdgpu] (cherry picked from commit a29e067bd38946f752b0ef855f3dfff87e77bec7)
CVE-2025-38521	In the Linux kernel, the following vulnerability has been resolved: drm/imagination: Fix kernel crash when hard resetting the GPU The GPU hard reset sequence call pm_runtime_force_suspend() and pm_runtime_force_resume(), which according to their documentation should only be used during system-wide PM transitions to s states. The main issue though is that depending on some internal runtime PM state as seen by pm_runtime_force_suspend() (whether the usage count is <= 1), pm_runtime_force_resume() might not resume the device unless needed. If that happens, the runtime PM resume callback pvr_power_device_resume() is not called clocks are not re-enabled, and the kernel crashes on the next attempt to access GPU registers as part of the power-on sequence. Replace calls to pm_runtime_force_suspend() and pm_runtime_force_resume() with direct calls to the driver's runtime PM callbacks, pvr_power_device_suspend() and pvr_power_device_resume(), to ensure clocks are re-enabled and avoid the kernel crash.
CVE-2025-9092	Uncontrolled Resource Consumption vulnerability in Legion of the Bouncy Castle Inc. Bouncy Castle for Java - BC-FJA 2.1.0 bc-fips (API modules) allows Excessive Al This vulnerability is associated with program files org.Bouncycastle.Crypto.Fips.NativeLoader. This issue affects Bouncy Castle for Java - BC-FJA 2.1.0: from BC-FJA 2 through 2.1.0.
CVE-2025-38522	In the Linux kernel, the following vulnerability has been resolved: sched/ext: Prevent update_locked_rq() calls with NULL rq Avoid invoking update_locked_rq() when runqueue (rq) pointer is NULL in the SCX_CALL_OP and SCX_CALL_OP_RET macros. Previously, calling update_locked_rq(NULL) with preemption enabled could trigg following warning: BUG: using __this_cpu_write() in preemptible [00000000] This happens because __this_cpu_write() is unsafe to use in preemptible context. rq is when an ops invoked from an unlocked context. In such cases, we don't need to store any rq, since the value should already be NULL (unlocked). Ensure that update_locked_rq() is only called when rq is non-NULL, preventing calling __this_cpu_write() on preemptible context.
CVE-2025-38523	In the Linux kernel, the following vulnerability has been resolved: cifs: Fix the smbd_response slab to allow usercopy The handling of received data in the smbdirec code involves using copy_to_iter() to copy data from the smbd_reponse struct's packet trailer to a folioq buffer provided by netfslib that encapsulates a chunk of pa If, however, CONFIG_HARDENED_USERCOPY=y, this will result in the checks then performed in copy_to_iter() oopsing with something like the following: CIFS: Atten mount //172.31.9.1/test CIFS: VFS: RDMA transport established usercopy: Kernel memory exposure attempt detected from SLUB object 'smbd_response_00000000 (offset 81, size 63)! ------------[cut here]------------ kernel BUG at mm/usercopy.c:102! ... RIP: 0010:usercopy_abort+0x6c/0x80 ... Call Trace: <TASK> __check_heap_object+0xe3/0x120 __check_object_size+0x4dc/0x6d0 smbd_recv+0x77f/0xfe0 [cifs] cifs_readv_from_socket+0x276/0x8f0 [cifs] cifs_read_from_socket+0xcd/0x120 [cifs] cifs_demultiplex_thread+0x7e9/0x2d50 [cifs] kthread+0x396/0x830 ret_from_fork+0x2b8/0x3b0 ret_from_fork_asm+0x1 The problem is that the smbd_response slab's packet field isn't marked as being permitted for usercopy. Fix this by passing parameters to kmem_slab_create() to i that copy_to_iter() is permitted from the packet region of the smbd_response slab objects, less the header space.
CVE-2025-38524	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix recv-recv race of completed call If a call receives an event (such as incoming data), the placed on the socket's queue and a thread in recvmsg can be awakened to go and process it. Once the thread has picked up the call off of the queue, further event cause it to be requeued, and once the socket lock is dropped (recvmsg uses call->user_mutex to allow the socket to be used in parallel), a second thread can come its recvmsg can pop the call off the socket queue again. In such a case, the first thread will be receiving stuff from the call and the second thread will be blocked on >user_mutex. The first thread can, at this point, process both the event that it picked call for and the event that the second thread picked the call for and may see terminate - in which case the call will be "released", decoupling the call from the user call ID assigned to it (RXRPC_USER_CALL_ID in the control message). The first will return okay, but then the second thread will wake up holding the user_mutex and, if it sees that the call has been released by the first thread, it will BUG thusly BUG at net/rxrpc/recvmsg.c:474! Fix this by just dequeuing the call and ignoring it if it is seen to be already released. We can't tell userspace about it anyway as th call ID has become stale.
CVE-2025-38525	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix irq-disabled in local_bh_enable() The rxrpc_assess_MTU_size() function calls down into t layer to find out the MTU size for a route. When accepting an incoming call, this is called from rxrpc_new_incoming_call() which holds interrupts disabled across the calls down to it. Unfortunately, the IP layer uses local_bh_enable() which, config dependent, throws a warning if IRQs are enabled: WARNING: CPU: 1 PID: 5544 at kernel/softirq.c:387 __local_bh_enable_ip+0x43/0xd0 ... RIP: 0010:__local_bh_enable_ip+0x43/0xd0 ... Call Trace: <TASK> rt_cache_route+0x7e/0xa0 rt_set_nexthop.isra.0+0x3b3/0x3f0 __mkroute_output+0x43a/0x460 ip_route_output_key_hash+0xf7/0x140 ip_route_output_flow+0x1b/0x90 rxrpc_assess_MTU_size.isra.0+0x2a0/0x590 rxrpc_new_incoming_peer+0x46/0x120 rxrpc_alloc_incoming_call+0x1b1/0x400 rxrpc_new_incoming_call+0x1da/0x5e rxrpc_input_packet+0x827/0x900 rxrpc_io_thread+0x403/0xb60 kthread+0x2f7/0x310 ret_from_fork+0x2a/0x230 ret_from_fork_asm+0x1a/0x30 ... hardirqs last e (23): _raw_spin_unlock_irq+0x24/0x50 hardirqs last disabled at (24): _raw_read_lock_irq+0x17/0x70 softirqs last enabled at (0): copy_process+0xc61/0x2730 softi disabled at (25): rt_add_uncached_list+0x3c/0x90 Fix this by moving the call to rxrpc_assess_MTU_size() out of rxrpc_init_peer() and further up the stack where it c done without interrupts disabled. It shouldn't be a problem for rxrpc_new_incoming_call() to do it after the locks are dropped as pmtud is going to be performed by thread - and we're in the I/O thread at this point.
CVE-2025-38526	In the Linux kernel, the following vulnerability has been resolved: ice: add NULL check in eswitch lag check The function ice_lag_is_switchdev_running() is being cal outside of the LAG event handler code. This results in the lag->upper_netdev being NULL sometimes. To avoid a NULL-pointer dereference, there needs to be a che it is dereferenced.
CVE-2025-38527	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix use-after-free in cifs_oplock_break A race condition can occur in cifs_oplock_break to a use-after-free of the cinode structure when unmounting: cifs_oplock_break() _cifsFileInfo_put(cfile) cifsFileInfo_put_final() cifs_sb_deactive() [last ref, start relea kill_sb() kill_anon_super() generic_shutdown_super() evict_inodes() dispose_list() evict() destroy_inode() call_rcu(&inode->i_rcu, i_callback) spin_lock(&cinode->open_file_lock) <- OK [later] i_callback() cifs_free_inode() kmem_cache_free(cinode) spin_unlock(&cinode->open_file_lock) <- UAF cifs_done_oplock_break(cinode The issue occurs when umount has already released its reference to the superblock. When _cifsFileInfo_put() calls cifs_sb_deactive(), this releases the last referenc triggering the immediate cleanup of all inodes under RCU. However, cifs_oplock_break() continues to access the cinode after this point, resulting in use-after-free. I holding an extra reference to the superblock during the entire oplock break operation. This ensures that the superblock and its inodes remain valid until the oplock completes.
CVE-2025-38528	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject %p% format string in bprintf-like helpers static const char fmt[] = "%p%"; bpf_trace_p sizeof(fmt)); The above BPF program isn't rejected and causes a kernel warning at runtime: Please remove unsupported %\x00 in format string WARNING: CPU: 1 P at lib/vsprintf.c:2680 format_decode+0x49c/0x5d0 This happens because bpf_bprintf_prepare skips over the second %, detected as punctuation, while processing patch fixes it by not skipping over punctuation. %\x00 is then processed in the next iteration and rejected.
CVE-2025-38529	In the Linux kernel, the following vulnerability has been resolved: comedi: aio_iiro_16: Fix bit shift out of bounds When checking for a supported IRQ number, the fo test is used: if ((1 << it->options[1]) & 0xdcfc) { However, `it->options[i]` is an unchecked `int` value from userspace, so the shift amount could be negative or ou bounds. Fix the test by requiring `it->options[1]` to be within bounds before proceeding with the original test. Valid `it->options[1]` values that select the IRQ will range [1,15]. The value 0 explicitly disables the use of interrupts.

CVE-2025-55286	z2d is a pure Zig 2D graphics library. z2d v0.7.0 released with a new multi-sample anti-aliasing (MSAA) method, which uses a new buffering mechanism for storing data. This differs from the standard alpha mask surface used for the previous super-sample anti-aliasing (SSAA) method. Under certain circumstances where the pa drawn existed in whole or partly outside of the rendering surface, incorrect bounding could cause out-of-bounds access within the coverage buffer. This affects the level drawing operations, such as Context.fill, Context.stroke, painter.fill, and painter.stroke, when either the .default or .multisample_4x anti-aliasing modes were .supersample_4x was not affected, nor was drawing without anti-aliasing. In non-safe optimization modes (consumers compiling with ReleaseFast or ReleaseSmall) could potentially lead to invalid memory accesses or corruption. z2d v0.7.1 fixes this issue, and it's recommended to upgrade to v0.7.1, or, given the small period v0.7.0 has been released, use v0.7.1 immediately, skipping v0.7.0.
CVE-2025-9036	A security issue in the runtime event system allows unauthenticated connections to receive a reusable API token. This token is broadcasted over a WebSocket and intercepted by any local client listening on the connection.
CVE-2025-7973	A security issue exists in FactoryTalk ViewPoint version 14.0 or below due to improper handling of MSI repair operations. During a repair, attackers can hijack the c console window, which runs with SYSTEM privileges. This can be exploited to spawn an elevated command prompt, enabling full privilege escalation.
CVE-2025-57723	Rejected reason: Not used
CVE-2025-38553	In the Linux kernel, the following vulnerability has been resolved: net/sched: Restrict conditions for adding duplicating netems to qdisc tree netem_enqueue's dupli prevention logic breaks when a netem resides in a qdisc tree with other netems - this can lead to a soft lockup and OOM loop in netem_dequeue, as seen in [1]. En a duplicating netem cannot exist in a tree with other netems. Previous approaches suggested in discussions in chronological order: 1) Track duplication status or tt sk_buff struct. Considered too specific a use case to extend such a struct, though this would be a resilient fix and address other previous and potential future DOS the one described in loopy fun [2]. 2) Restrict netem_enqueue recursion depth like in act_mirred with a per cpu variable. However, netem_dequeue can call enqueu child, and the depth restriction could be bypassed if the child is a netem. 3) Use the same approach as in 2, but add metadata in netem_skb_cb to handle the netem_dequeue case and track a packet's involvement in duplication. This is an overly complex approach, and Jamal notes that the skb cb can be overwritten to ci this safeguard. 4) Prevent the addition of a netem to a qdisc tree if its ancestral path contains a netem. However, filters and actions can cause a packet to change when re-enqueued to the root from netem duplication, leading us to the current solution: prevent a duplicating netem from inhabiting the same tree as other neter https://lore.kernel.org/netdev/8DuRWwfqjoRDLDmBMIlfbrsZg9Gx50DHJc1ilxsEBNe2D6NMoigR_eIRIG0LOjMc3r10nUUZtArXx4oZBIdUfZQrwjcQhdinnMis_0G7VEk=@w [2] https://lwn.net/Articles/719297/
CVE-2025-55725	Rejected reason: Not used
CVE-2025-34154	UnForm Server Manager versions prior to 10.1.12 expose an unauthenticated file read vulnerability via its log file analysis interface. The flaw resides in the arc end which accepts a fl parameter to specify the log file to be opened. Due to insufficient input validation and lack of path sanitization, attackers can supply relative pat access arbitrary files on the host system — including sensitive OS-level files — without authentication.
CVE-2025-55193	Active Record connects classes to relational database tables. Prior to versions 7.1.5.2, 7.2.2.2, and 8.0.2.1, the ID passed to find or similar methods may be logged escaping. If this is directly to the terminal it may include unescaped ANSI sequences. This issue has been patched in versions 7.1.5.2, 7.2.2.2, and 8.0.2.1.
CVE-2025-57725	Rejected reason: Not used
CVE-2025-57724	Rejected reason: Not used
CVE-2025-57722	Rejected reason: Not used
CVE-2025-55723	Rejected reason: Not used
CVE-2025-57721	Rejected reason: Not used
CVE-2025-57720	Rejected reason: Not used
CVE-2025-57719	Rejected reason: Not used
CVE-2025-57718	Rejected reason: Not used
CVE-2025-57717	Rejected reason: Not used
CVE-2025-55196	External Secrets Operator is a Kubernetes operator that integrates external secret management systems. From version 0.15.0 to before 0.19.2, a vulnerability was discovered where the List() calls for Kubernetes Secret and SecretStore resources performed by the PushSecret controller did not apply a namespace selector. This allowed an attacker to use label selectors to list and read secrets/secret-stores across the cluster, bypassing intended namespace restrictions. An attacker with the create or update PushSecret resources and control SecretStore configurations could exploit this vulnerability to exfiltrate sensitive data from arbitrary namespaces could lead to full disclosure of Kubernetes secrets, including credentials, tokens, and other sensitive information stored in the cluster. This vulnerability has been p version 0.19.2. A workaround for this issue includes auditing and restricting RBAC permissions so that only trusted service accounts can create or update PushSecr SecretStore resources.

CVE-2012-10060	Sysax Multi Server versions prior to 5.55 contains a stack-based buffer overflow in its SSH service. When a remote attacker supplies an overly long username durin authentication, the server copies the input to a fixed-size stack buffer without proper bounds checking. This allows remote code execution under the context of the
CVE-2012-10059	Dolibarr ERP/CRM versions <= 3.1.1 and <= 3.2.0 contain a post-authenticated OS command injection vulnerability in its database backup feature. The export.php fails to sanitize the sql_compat parameter, allowing authenticated users to inject arbitrary system commands, resulting in remote code execution on the server.
CVE-2025-9043	The service executable path in Seagate Toolkit on Versions prior to 2.34.0.33 on Windows allows an attacker with Admin privileges to exploit a vulnerability as clas under CWE-428: Unquoted Search Path or Element. An attacker with write permissions to the root could place a malicious Program.exe file, which would execute w SYSTEM privileges.
CVE-2012-10057	Lattice Semiconductor ispVM System v18.0.2 contains a buffer overflow vulnerability in its handling of .xcf project files. When parsing the version attribute of the is tag, the application fails to properly validate input length, allowing a specially crafted file to overwrite memory on the stack. This can result in arbitrary code execu the context of the user who opens the file. The vulnerability is triggered locally by opening a malicious .xcf file and does not require elevated privileges.
CVE-2012-10056	PHP Volunteer Management System v1.0.2 contains an arbitrary file upload vulnerability in its document upload functionality. Authenticated users can upload files mods/documents/uploads/ directory without any restriction on file type or extension. Because this directory is publicly accessible and lacks execution controls, atta upload a malicious PHP payload and execute it remotely. The application ships with default credentials, making exploitation trivial. Once authenticated, the attacke upload a PHP shell and trigger it via a direct GET request.
CVE-2012-10055	ComSndFTP FTP Server version 1.3.7 Beta contains a format string vulnerability in its handling of the USER command. By sending a specially crafted username con format specifiers, a remote attacker can overwrite a hardcoded function pointer in memory (specifically WSACleanup from Ws2_32.dll). This allows the attacker to execution flow and bypass DEP protections using a ROP chain, ultimately leading to arbitrary code execution. The vulnerability is exploitable without authentication affects default configurations.
CVE-2012-10054	Umbraco CMS versions prior to 4.7.1 are vulnerable to unauthenticated remote code execution via the codeEditorSave.asmx SOAP endpoint, which exposes a Save operation that permits arbitrary file uploads without authentication. By exploiting a path traversal flaw in the fileName parameter, attackers can write malicious AS directly into the web-accessible /umbraco/ directory and execute them remotely.
CVE-2025-55726	Rejected reason: Not used
CVE-2011-10019	Spreecommerce versions prior to 0.60.2 contains a remote command execution vulnerability in its search functionality. The application fails to properly sanitize inp via the search[send][] parameter, which is dynamically invoked using Ruby's send method. This allows attackers to execute arbitrary shell commands on the serve authentication.
CVE-2011-10017	Snort Report versions < 1.3.2 contains a remote command execution vulnerability in the nmap.php and nbtscan.php scripts. These scripts fail to properly sanitize passed via the target GET parameter, allowing attackers to inject arbitrary shell commands. Exploitation requires no authentication and can result in full compromi underlying system.
CVE-2011-10016	Real Networks Netzip Classic version 7.5.1.86 is vulnerable to a stack-based buffer overflow when parsing a specially crafted ZIP archive. The vulnerability is trigge the application attempts to process a file name within the archive that exceeds the expected buffer size. Exploitation allows arbitrary code execution under the cor the victim user when the ZIP file is opened.
CVE-2025-43740	A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.3.120 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.8, 2025.Q1.0 through 2025 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.1 through 2024.Q2.13 and 2024.Q1.9 through 2024.Q1.19 allows an remote authenticated to inject JavaScript through the message boards feature available via the web interface.
CVE-2011-10015	Cytel Studio version 9.0 and earlier is vulnerable to a stack-based buffer overflow triggered by parsing a malformed .CY3 file. The vulnerability occurs when the app copies user-controlled strings into a fixed-size stack buffer (256 bytes) without proper bounds checking. Exploitation allows arbitrary code execution when the craft opened.
CVE-2025-43739	Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.6, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 th 2024.Q2.13, 2024.Q1.1 through 2024.Q1.16 and 7.4 GA through update 92 allow any authenticated user to modify the content of emails sent through the calendar allowing an attacker to send phishing emails to any other user in the same organization.
CVE-2011-10014	GTA San Andreas Multiplayer (SA-MP) server version 0.3.1.1 is vulnerable to a stack-based buffer overflow triggered by parsing a malformed server.cfg configuratio vulnerability allows local attackers to execute arbitrary code when the server binary (samp-server.exe) processes a crafted echo directive containing excessive inp original 'sa-mp.com' site is defunct, but the community maintains mirrors and forks that may be vulnerable.
CVE-2011-10013	Traq versions 2.0 through 2.3 contain a remote code execution vulnerability in the admincp/common.php script. The flawed authorization logic fails to halt executio failed access check, allowing unauthenticated users to reach admin-only functionality. This can be exploited via plugins.php to inject and execute arbitrary PHP coc
CVE-2011-10012	NetOp (now part of Impero Software) Remote Control Client v9.5 is vulnerable to a stack-based buffer overflow when processing .dws configuration files. If a .dws f contains a string longer than 520 bytes, the application fails to perform proper bounds checking, allowing an attacker to execute arbitrary code when the file is ope
CVE-2025-55724	Rejected reason: Not used
CVE-2024-7402	Netskope has identified a potential gap in its agent (Netskope Client) in which a malicious insider can potentially tamper the Netskope Client configuration by perfo MITM (Man-in-the-Middle) activity on the Netskope Client communication channel. A successful exploitation would require administrative privileges on the machine could result in temporarily altering the configuration of Netskope Client or permanently disabling or removing the agent from the machine.
CVE-2025-57700	DIAEnergie - Stored Cross-site Scripting
CVE-2025-43733	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.7 allows a remote authenticated atta inject JavaScript code via the content page's name field. This malicious payload is then reflected and executed within the user's browser when viewing the "docum Usages" page.
CVE-2025-	Genealogy is a family tree PHP application. Prior to 4.4.0, Authenticated Stored Cross-Site Scripting (XSS) vulnerability was identified in the Genealogy application. Authenticated attackers could run arbitrary JavaScript in another user's session, leading to session hijacking, data theft, and UI manipulation. This vulnerability is fi

55287	4.4.0.
CVE-2025-55214	Copier library and CLI app for rendering project templates. From 7.1.0 to before 9.9.1, Copier suggests that it's safe to generate a project from a safe template, i.e. doesn't use unsafe features like custom Jinja extensions which would require passing the --UNSAFE,--trust flag. As it turns out, a safe template can currently write f outside the destination path where a project shall be generated or updated. This is possible when rendering a generated directory structure whose rendered path i relative parent path or an absolute path. Constructing such paths is possible using Copier's builtin pathjoin Jinja filter and its builtin _copier_conf.sep variable, whicl platform-native path separator. This way, a malicious template author can create a template that overwrites arbitrary files (according to the user's write permissio to cause havoc. This vulnerability is fixed in 9.9.1.
CVE-2025-55201	Copier library and CLI app for rendering project templates. Prior to 9.9.1, a safe template can currently read and write arbitrary files because Copier exposes a few pathlib.Path objects in the Jinja context which have unconstrained I/O methods. This effectively renders the security model w.r.t. filesystem access useless. This vu is fixed in 9.9.1.
CVE-2025-3639	Liferay Portal 7.3.0 through 7.4.3.132, and Liferay DXP 2025.Q1 through 2025.Q1.6, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 thro 2024.Q2.13, 2024.Q1.1 through 2024.Q1.15, 7.4 GA through update 92 and 7.3 GA through update 36 allows unauthenticated users with valid credentials to bypas login process by changing the POST method to GET, once the site has MFA enabled.
CVE-2025-4962	An Insecure Direct Object Reference (IDOR) vulnerability was identified in the `POST /v1/templates` endpoint of the Lunary API, affecting versions up to 0.8.8. This vulnerability allows authenticated users to create templates in another user's project by altering the `projectId` query parameter. The root cause of this issue is th of server-side validation to ensure that the authenticated user owns the specified `projectId`. The vulnerability has been addressed in version 1.9.23.
CVE-2025-43732	Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.10, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.1 t 2024.Q2.13, 2024.Q1.1 through 2024.Q1.17 and 7.4 GA through update 92 is vulnerable to Insecure Direct Object Reference (IDOR) in the groupId parameter of th _com_liferay_roles_selector_web_portlet_RolesSelectorPortlet_groupId. When an organization administrator modifies this parameter id value, they can gain unautho access to user lists from other organizations.
CVE-2025-47206	An out-of-bounds write vulnerability has been reported to affect File Station 5. If a remote attacker gains a user account, they can then exploit the vulnerability to r corrupt memory. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.4933 and later
CVE-2025-0309	An insufficient validation on the server connection endpoint in Netskope Client allows local users to elevate privileges on the system. The insufficient validation allo Netskope Client to connect to any other server with Public Signed CA TLS certificates and send specially crafted responses to elevate privileges.
CVE-2025-7353	A security issue exists due to the web-based debugger agent enabled on Rockwell Automation ControlLogix® Ethernet Modules. If a specific IP address is used to c the WDB agent, it can allow remote attackers to perform memory dumps, modify memory, and control execution flow.
CVE-2025-7773	A security issue exists within the 5032 16pt Digital Configurable module’s web server. The web server’s session number increments at an interval that correlates to two consecutive sign in session interval, making it predictable.
CVE-2025-7774	A security issue exists within the 5032 16pt Digital Configurable module’s web server. Intercepted session credentials can be used within a 3-minute timeout windo allowing unauthorized users to perform privileged actions.
CVE-2025-57703	DIAEnergie - Reflected Cross-site Scripting
CVE-2025-57702	DIAEnergie - Reflected Cross-site Scripting
CVE-2025-57701	DIAEnergie - Reflected Cross-site Scripting
CVE-2025-44201	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it security issue. Notes: none.
CVE-2025-55718	Rejected reason: Not used
CVE-2025-43490	A potential security vulnerability has been identified in the HPAudioAnalytics service included in the HP Hotkey Support software, which might allow escalation of p HP is releasing software updates to mitigate the potential vulnerability.
CVE-2025-55300	Komari is a lightweight, self-hosted server monitoring tool designed to provide a simple and efficient solution for monitoring server performance. Prior to 1.0.4-fix1 WebSocket upgrader has disabled origin checking, enabling Cross-Site WebSocket Hijacking (CSWSH) attacks against authenticated users. Any third party website requests to the terminal websocket endpoint with browser's cookies, resulting in remote code execution. This vulnerability is fixed in 1.0.4-fix1.
CVE-2025-7693	A security issue exists due to improper handling of malformed CIP Forward Close packets during fuzzing. The controller enters a solid red Fault LED state and becor unresponsive. Upon power cycle, the controller will enter recoverable fault where the MS LED and Fault LED become flashing red and reports fault code 0xF015. To recover, clear the fault.
CVE-2025-43731	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.8, 2024.Q4.0 through 2 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.16 and 7.4 GA through update 92 allows an remote authenticated use JavaScript in message board threads and categories.
CVE-2025-55213	OpenFGA is a high-performance and flexible authorization/permission engine built for developers and inspired by Google Zanzibar. OpenFGA v1.9.3 to v1.9.4 (oper 0.2.40 <= Helm chart <= openfga-0.2.41, v1.9.3 <= docker <= v.1.9.4) are vulnerable to improper policy enforcement when certain Check and ListObject calls ar executed. This vulnerability is fixed in 1.9.5.
CVE-2025-	Rejected reason: Not used

55719	
CVE-2025-55720	Rejected reason: Not used
CVE-2025-7961	Improper Control of Generation of Code ('Code Injection') vulnerability in Wulkano KAP on MacOS allows TCC Bypass.This issue affects KAP: 3.6.0.
CVE-2025-8066	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Bunkerity Bunker Web on Linux allows Phishing.This issue affects Bunker Web: 1.6.2.
CVE-2025-7761	Lepszy BIP is vulnerable to Reflected Cross-Site Scripting (XSS). Improper input validation in index.php form in one of the parameters allows arbitrary JavaScript to executed on victim's browser when specially crafted URL is opened. The vendor was contacted early about this disclosure but did not respond in any way. Potentia versions are vulnerable.
CVE-2025-55207	Astro is a web framework for content-driven websites. Following CVE-2025-54793 there's still an Open Redirect vulnerability in a subset of Astro deployment scena to version 9.4.1. Astro 5.12.8 addressed CVE-2025-54793 where https://example.com//astro.build/press would redirect to the external origin //astro.build/press. Ho with the Node deployment adapter in standalone mode and trailingSlash set to "always" in the Astro configuration, https://example.com//astro.build/press still redi //astro.build/press. This affects any user who clicks on a specially crafted link pointing to the affected domain. Since the domain appears legitimate, victims may be into trusting the redirected page, leading to possible credential theft, malware distribution, or other phishing-related attacks. This issue has been patched in versio
CVE-2025-27388	Loading arbitrary external URLs through WebView components introduces malicious JS code that can steal arbitrary user tokens.
CVE-2025-55721	Rejected reason: Not used
CVE-2025-5942	Netskope was notified about a potential gap in its agent (NS Client) on Windows systems. If this gap is successfully exploited, an unprivileged user can trigger a he overflow in the epdlpdrv.sys driver, leading to a Blue-Screen-of-Death (BSOD). Successful exploitation can also potentially be performed by an unprivileged user wh Client is configured to use Endpoint DLP. A successful exploit can result in a denial-of-service for the local machine.
CVE-2025-5941	Netskope is notified about a potential gap in its agent (NS Client) in which a malicious actor could trigger a memory leak by sending a crafted DNS packet to a mac successful exploitation may require administrative privileges on the machine, based on the exact configuration. A successful exploit can potentially result in user-controllable memory being leaked in a domain name stored on the local machine.
CVE-2025-55722	Rejected reason: Not used