SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 22 October 2025

Generated on 22 October 2025

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-62168	Squid is a caching proxy for the Web. In Squid versions prior to 7.2, a failure to redact HTTP authentication credentials in error handling allows information disclosure. The vulnerability allows a script to bypass browser security protections and learn the credentials a trusted client uses to authenticate. This potentially allows a remote client to identify security tokens or credentials used internally by a web application using Squid for backend load balancing. These attacks do not require Squid to be configured with HTTP authentication. The vulnerability is fixed in version 7.2. As a workaround, disable debug information in administrator mailto links generated by Squid by configuring squid.conf with email_err_data off.	10.0	More Details
CVE-2025-10020	Zohocorp ManageEngine ADManager Plus version before 8024 are vulnerable to authenticated command injection vulnerability in the Custom Script component.	9.9	More Details
CVE-2025-62645	The Restaurant Brands International (RBI) assistant platform through 2025-09-06 allows a remote authenticated attacker to obtain a token with administrative privileges for the entire platform via the createToken GraphQL mutation.	9.9	More Details
CVE-2025-10041	The Flex QR Code Generator plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in thesave_qr_code_to_db() function in all versions up to, and including, 1.2.5. 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-2017-20207	The Flickr Gallery plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 1.5.2 via deserialization of untrusted input from the `pager ` parameter. This allows unauthenticated attackers to inject a PHP Object. Attackers were actively exploiting this vulnerability with the WP_Theme() class to create backdoors.	9.8	More Details
CVE-2025-56218	An arbitrary file upload vulnerability in SigningHub v8.6.8 allows attackers to execute arbitrary code via uploading a crafted PDF file.	9.8	More Details
CVE-2025-56221	A lack of rate limiting in the login mechanism of SigningHub v8.6.8 allows attackers to bypass authentication via a brute force attack.	9.8	More Details
CVE-2025-56316	A SQL injection vulnerability in the content_title parameter of the /cms/content/list endpoint in MCMS 5.5.0 allows remote attackers to execute arbitrary SQL queries via unsanitized input in the FreeMarker template rendering.	9.8	More Details

CVE-2025-62515	pyquokka is a framework for making data lakes work for time series. In versions 0.3.1 and prior, the FlightServer class directly uses pickle.loads() to deserialize action bodies received from Flight clients without any sanitization or validation in the do_action() method. The vulnerable code is located in pyquokka/flight.py at line 283 where arbitrary data from Flight clients is directly passed to pickle.loads(). When FlightServer is configured to listen on 0.0.0.0, this allows attackers across the entire network to perform arbitrary remote code execution by sending malicious pickled payloads through the set_configs action. Additional vulnerability points exist in the cache_garbage_collect, do_put, and do_get functions where pickle.loads is used to deserialize untrusted remote data.	9.8	More Details
CVE-2017-20206	The Appointments plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 2.2.1 via deserialization of untrusted input from the `wpmudev_appointments` cookie. This allows unauthenticated attackers to inject a PHP Object. Attackers were actively exploiting this vulnerability with the WP_Theme() class to create backdoors.	9.8	More Details
CVE-2017-20208	The RegistrationMagic – Custom Registration Forms, User Registration, Payment, and User Login plugin for WordPress is vulnerable to PHP Object Injection in all versions up to 3.7.9.3 (exclusive) via deserialization of untrusted input from the is_expired_by_date() function. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain allows attackers to fetch a remote file and install it on the site.	9.8	More Details
CVE-2025-10294	The OwnID Passwordless Login plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.3.4. This is due to the plugin not properly checking if the ownid_shared_secret value is empty prior to authenticating a user via JWT. This makes it possible for unauthenticated attackers to log in as other users, including administrators, on instances where the plugin has not been fully configured yet.	9.8	More Details
CVE-2025-11391	The PPOM – Product Addons & Custom Fields for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the image cropper functionality in all versions up to, and including, 33.0.15. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. While the vulnerable code is in the free version, this only affected users with the paid version of the software installed and activated.	9.8	More Details
CVE-2025-11948	Document Management System developed by Excellent Infotek has an Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	9.8	More Details
CVE-2025-61455	SQL Injection vulnerability exists in Bhabishya-123 E-commerce 1.0, specifically within the signup.inc.php endpoint. The application directly incorporates unsanitized user inputs into SQL queries, allowing unauthenticated attackers to bypass authentication and gain full access.	9.8	More Details
CVE-2025-61303	Hatching Triage Sandbox Windows 10 build 2004 (2025-08-14) and Windows 10 LTSC 2021(2025-08-14) contains a vulnerability in its Windows behavioral analysis engine that allows a submitted malware sample to evade detection and cause denial-of-analysis. The vulnerability is triggered when a sample recursively spawns a large number of child processes, generating high log volume and exhausting system resources. As a result, key malicious behavior, including PowerShell execution and reverse shell activity, may not be recorded or reported, misleading analysts and compromising the integrity and availability of sandboxed analysis results.	9.8	More Details
CVE-2025-53037	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in takeover of Oracle Financial Services Analytical Applications Infrastructure. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2025-53072	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in takeover of Oracle Marketing. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2025-61757	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: REST WebServices). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Identity Manager. Successful attacks of this vulnerability can result in takeover of Identity Manager. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2025-	A path traversal vulnerability in all versions of the Windsurf IDE enables a threat actor to read and write		More

62353	arbitrary local files in and outside of current projects on an end user's system. The vulnerability can be reached directly and through indirect prompt injection.	9.8	Details
CVE-2025-62481	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in takeover of Oracle Marketing. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2025-10611	Due to an insufficient access control implementation in multiple WSO2 Products, authentication and authorization checks for certain REST APIs can be bypassed, allowing them to be invoked without proper validation. Successful exploitation of this vulnerability could lead to a malicious actor gaining administrative access and performing unauthenticated and unauthorized administrative operations.	9.8	More Details
CVE-2025-41018	SQL injection in Sergestec's Exito v8.0. This vulnerability allows an attacker to retrieve, create, update, and delete databases through the 'cat' parameter in '/public.php'.	9.8	More Details
CVE-2023-28815	Some versions of Hikvision's iSecure Center Product contain insufficient parameter validation, resulting in a command injection vulnerability. Attackers may exploit this to gain platform privileges and execute arbitrary commands on the system.iSecure Center is software released for China's domestic market only, with no overseas release.	9.8	More Details
CVE-2023-28814	Some versions of Hikvision's iSecure Center Product have an improper file upload control vulnerability. Due to the improper verification of file to be uploaded, attackers may upload malicious files to the server. iSecure Center is software released for China's domestic market only, with no overseas release.	9.8	More Details
CVE-2025-9967	The Orion SMS OTP Verification plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.1.7. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's password to a one-time password if the attacker knows the user's phone number	9.8	More Details
CVE-2025-11900	The iSherlock developed by HGiga has an OS Command Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary OS commands and execute them on the server.	9.8	More Details
CVE-2025-10742	The Truelysell Core plugin for WordPress is vulnerable to Arbitrary User Password Change in versions up to, and including, 1.8.6. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resources. This makes it possible for unauthenticated attackers to change user passwords and potentially take over administrator accounts. Note: This can only be exploited unauthenticated if the attacker knows which page contains the 'truelysell_edit_staff' shortcode.	9.8	More Details
CVE-2025-62586	OPEXUS FOIAXpress allows a remote, unauthenticated attacker to reset the administrator password. Fixed in FOIAXpress version 11.13.2.0.	9.8	More Details
CVE-2025-10850	The Felan Framework plugin for WordPress is vulnerable to improper authentication in versions up to, and including, 1.1.4. This is due to the hardcoded password in the 'fb_ajax_login_or_register' function and in the 'google_ajax_login_or_register' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, if they registered with facebook or google social login and did not change their password.	9.8	More Details
CVE-2025-62583	Whale Browser before 4.33.325.17 allows an attacker to escape the iframe sandbox in a dual-tab environment.	9.8	More Details
CVE-2025-9152	An improper privilege management vulnerability exists in WSO2 API Manager due to missing authentication and authorization checks in the keymanager-operations Dynamic Client Registration (DCR) endpoint. A malicious user can exploit this flaw to generate access tokens with elevated privileges, potentially leading to administrative access and the ability to perform unauthorized operations.	9.8	More Details
CVE-2025-49655	Deserialization of untrusted data can occur in versions of the Keras framework running versions 3.11.0 up to but not including 3.11.3, enabling a maliciously uploaded Keras file containing a TorchModuleWrapper class to run arbitrary code on an end user's system when loaded despite safe mode being enabled. The vulnerability can be triggered through both local and remote files.	9.8	More Details
CVE-2025-54539	A Deserialization of Untrusted Data vulnerability exists in the Apache ActiveMQ NMS AMQP Client. This issue affects all versions of Apache ActiveMQ NMS AMQP up to and including 2.3.0, when establishing connections to untrusted AMQP servers. Malicious servers could exploit unbounded deserialization logic present in the client to craft responses that may lead to arbitrary code execution on the client side. Although version 2.1.0 introduced a mechanism to restrict deserialization via allow/deny lists, the protection was found to be bypassable under certain conditions. In line with Microsoft's deprecation of binary serialization in .NET 9, the project is evaluating the removal of .NET binary serialization support	9.8	More Details

	from the NMS API entirely in future releases. Mitigation and Recommendations: Users are strongly encouraged to upgrade to version 2.4.0 or later, which resolves the issue. Additionally, projects depending on NMS-AMQP should migrate away from .NET binary serialization as part of a long-term hardening strategy.		
CVE-2025-60279	A server-side request forgery (SSRF) vulnerability in Illia Cloud illia-Builder before v4.8.5 allows authenticated users to send arbitrary requests to internal services via the API. An attacker can leverage this to enumerate open ports based on response discrepancies and interact with internal services.	9.6	More Details
CVE-2025-9804	An improper access control vulnerability exists in multiple WSO2 products due to insufficient permission enforcement in certain internal SOAP Admin Services and System REST APIs. A low-privileged user may exploit this flaw to perform unauthorized operations, including accessing server-level information. This vulnerability affects only internal administrative interfaces. APIs exposed through the WSO2 API Manager's API Gateway remain unaffected.	9.6	More Details
CVE-2025-11492	In the ConnectWise Automate Agent, communications could be configured to use HTTP instead of HTTPS. In such cases, an on-path threat actor with a man-in-the-middle network position could intercept, modify, or replay agent-server traffic. Additionally, the encryption method used to obfuscate some communications over the HTTP channel is updated in the Automate 2025.9 patch to enforce HTTPS for all agent communications.	9.6	More Details
CVE-2025-56749	Creativeitem Academy LMS up to and including 6.14 uses a hardcoded default JWT secret for token signing. This predictable secret allows attackers to forge valid JWT tokens, leading to authentication bypass and unauthorized access to any user account.	9.4	More Details
CVE-2025-11849	Versions of the package mammoth from 0.3.25 and before 1.11.0; versions of the package mammoth from 0.3.25 and before 1.11.0; versions of the package mammoth before 1.11.0; versions of the package org.zwobble.mammoth:mammoth before 1.11.0 are vulnerable to Directory Traversal due to the lack of path or file type validation when processing a docx file containing an image with an external link (r:link attribute instead of embedded r:embed). The library resolves the URI to a file path and after reading, the content is encoded as base64 and included in the HTML output as a data URI. An attacker can read arbitrary files on the system where the conversion is performed or cause an excessive resources consumption by crafting a docx file that links to special device files such as /dev/random or /dev/zero.	9.3	More Details
CVE-2025-9574	Missing Authentication for Critical Function vulnerability in ABB ALS-mini-s4 IP, ABB ALS-mini-s8 IP.This issue affects . All firmware versions with the Serial Number from 2000 to 5166	9.1	More Details
CVE-2025-10916	The FormGent WordPress plugin before 1.0.4 is vulnerable to arbitrary file deletion due to insufficient file path validation. This makes it possible for unauthenticated attackers to delete arbitrary files on the server.	9.1	More Details
CVE-2025-61922	PrestaShop Checkout is the PrestaShop official payment module in partnership with PayPal. Starting in version 1.3.0 and prior to versions 4.4.1 and 5.0.5, missing validation on the Express Checkout feature allows silent login, enabling account takeover via email. The vulnerability is fixed in versions 4.4.1 and 5.0.5. No known workarounds exist.	9.1	More Details
CVE-2025-57567	A remote code execution (RCE) vulnerability exists in the PluXml CMS theme editor, specifically in the minify.php file located under the default theme directory (/themes/defaut/css/minify.php). An authenticated administrator user can overwrite this file with arbitrary PHP code via the admin panel, enabling execution of system commands.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-60507	Cross site scripting vulnerability in Moodle GeniAI plugin (local_geniai) 2.3.6. An authenticated user with Teacher role can upload a PDF containing embedded JavaScript. The assistant outputs a direct HTML link to the uploaded file without sanitization. When other users (including Students or Administrators) click the link, the payload executes in their browser.	8.9	More Details
CVE-2025-47410	Apache Geode is vulnerable to CSRF attacks through GET requests to the Management and Monitoring REST API that could allow an attacker who has tricked a user into giving up their Geode session credentials to submit malicious commands on the target system on behalf of the authenticated user. This issue affects Apache Geode: versions 1.10 through 1.15.1 Users are recommended to upgrade to version 1.15.2, which fixes the issue.	8.8	More Details
CVE-2025-10299	The WPBifröst – Instant Passwordless Temporary Login Links plugin for WordPress is vulnerable to Privilege Escalation due to a missing capability check on the ctl_create_link AJAX action in all versions up to, and including, 1.0.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create new administrative user accounts and subsequently log in as those.	8.8	More Details

CVE-2025-11619	Improper certificate validation when connecting to gateways in Devolutions Server 2025.3.2 and earlier allows attackers in MitM position to intercept traffic.	8.8	More Details
CVE-2025-9890	The Theme Editor plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0. This is due to missing or incorrect nonce validation on the 'theme_editor_theme' page. This makes it possible for unauthenticated attackers to achieve remote code execution via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2025-11746	The XStore theme for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 9.5.4 via theet_ajax_required_plugins_popup() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	8.8	More Details
CVE-2025-11493	The ConnectWise Automate Agent does not fully verify the authenticity of files downloaded from the server, such as updates, dependencies, and integrations. This creates a risk where an on-path attacker could perform a man-in-the-middle attack and substitute malicious files for legitimate ones by impersonating a legitimate server. This risk is mitigated when HTTPS is enforced and is related to CVE-2025-11492.	8.8	More Details
CVE-2025-10706	The Classified Pro theme for WordPress is vulnerable to unauthorized plugin installation due to a missing capability check in the 'cwp_addons_update_plugin_cb' function in all versions up to, and including, 1.0.14. This makes it possible for authenticated attackers, with subscriber-level access and above, to install arbitrary plugins on the affected site's server which may make remote code execution possible. Note: The required nonce for the vulnerability is in the CubeWP Framework plugin.	8.8	More Details
CVE-2025-61417	Cross-Site Scripting (XSS) vulnerability exists in TastyIgniter 3.7.7, affecting the /admin/media_manager component. Attackers can upload a malicious SVG file containing JavaScript code. When an administrator previews the file, the code executes in their browser context, allowing the attacker to perform unauthorized actions such as modifying the admin account credentials.	8.8	More Details
CVE-2025-10293	The Keyy Two Factor Authentication (like Clef) plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.2.3. This is due to the plugin not properly validating a user's identity associated with a token generated. This makes it possible for authenticated attackers, with subscriber-level access and above, to generate valid auth tokens and leverage that to auto-login as other accounts, including administrators, as long as the administrator has the 2FA set up.	8.8	More Details
CVE-2025-61955	A vulnerability exists in F5OS-A and F5OS-C systems that may allow an authenticated attacker with local access to escalate their privileges. A successful exploit may allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.8	More Details
CVE-2025-57780	A vulnerability exists in F5OS-A and F5OS-C system that may allow an authenticated attacker with local access to escalate their privileges. A successful exploit may allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.8	More Details
CVE-2025-59481	A vulnerability exists in an undisclosed iControl REST and BIG-IP TMOS Shell (tmsh) command that may allow an authenticated attacker with at least resource administrator role to execute arbitrary system commands with higher privileges. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2025-53868	When running in Appliance mode, a highly privileged authenticated attacker with access to SCP and SFTP may be able to bypass Appliance mode restrictions using undisclosed commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2025-61958	A vulnerability exists in the iHealth command that may allow an authenticated attacker with at least a resource administrator role to bypass tmsh restrictions and gain access to a bash shell. For BIG-IP systems running in Appliance mode, a successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2025-53036	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. While the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	8.6	More Details
	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Administration). Supported versions that are affected are 7.6.0.0.0 and 8.2.0.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle		

CVE-2025-53049	Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 8.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H).	8.4	More Details
CVE-2025-43281	The issue was addressed with improved authentication. This issue is fixed in macOS Sequoia 15.6. A local attacker may be able to elevate their privileges.	8.4	More Details
CVE-2025-62425	MAS (Matrix Authentication Service) is a user management and authentication service for Matrix homeservers, written and maintained by Element. A logic flaw in matrix-authentication-service 0.20.0 through 1.4.0 allows an attacker with access to an authenticated MAS session to perform sensitive operations without entering the current password. These include changing the current password, adding or removing an e-mail address and deactivating the account. The vulnerability only affects instances which have the local password database feature enabled (passwords section in the config). Patched in matrix-authentication-service 1.4.1.	8.3	More Details
CVE-2025-9428	Zohocorp ManageEngine Analytics Plus versions 6171 and prior are vulnerable to authenticated SQL Injection via the key update api.	8.3	More Details
CVE-2025-62650	The Restaurant Brands International (RBI) assistant platform through 2025-09-06 relies on client-side authentication for use of the diagnostic screen.	8.3	More Details
CVE-2024-56143	Strapi is an open-source headless content management system. In versions from 5.0.0 to before 5.5.2, the lookup operator provided by the document service does not properly sanitize query parameters for private fields. An attacker can access private fields, including admin passwords and reset tokens, by crafting queries with the lookup parameter. This vulnerability is fixed in 5.5.2.	8.2	More Details
CVE-2025-61536	FelixRiddle dev-jobs-handlebars 1.0 uses absolute password-reset (magic) links using the untrusted `req.headers.host` header and forces the `http://` scheme. An attacker who can control the `Host` header (or exploit a misconfigured proxy/load-balancer that forwards the header unchanged) can cause reset links to point to attacker-controlled domains or be delivered via insecure HTTP, enabling token theft, phishing, and account takeover.	8.2	More Details
CVE-2025-11151	Exposure of Sensitive Information to an Unauthorized Actor, Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Beyaz Bilgisayar Software Design Industry and Trade Ltd. Co. CityPLus allows Detect Unpublicized Web Pages.This issue affects CityPLus: before V24.29500.1.0.	8.2	More Details
CVE-2025-61553	An out-of-bounds write in VirtIO network device emulation in BitVisor from commit 108df6 (2020-05-20) to commit 480907 (2025-07-06) allows local attackers to cause a denial of service (host hypervisor crash) via a crafted PCI configuration space access. Given it's a heap overflow in a privileged hypervisor context, exploitation may enable arbitrary code execution or guest-to-host privilege escalation.	8.2	More Details
CVE-2025-62587	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.12 and 7.2.2. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2025-62588	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.12 and 7.2.2. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2025-62589	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.12 and 7.2.2. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.12 and 7.2.2. Easily exploitable vulnerability allows high privileged attacker		

CVE-2025-62590	with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2025-62641	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.12 and 7.2.2. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2025-22381	Aggie 2.6.1 has a Host Header injection vulnerability in the forgot password functionality, allowing an attacker to reset a user's password.	8.2	More Details
CVE-2025-9133	A missing authorization vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.40, USG FLEX series firmware versions from V4.50 through V5.40, USG FLEX 50(W) series firmware versions from V4.16 through V5.40, and USG20(W)-VPN series firmware versions from V4.16 through V5.40 could allow a semi-authenticated attacker—who has completed only the first stage of the two-factor authentication (2FA) process—to view and download the system configuration from an affected device.	8.1	More Details
CVE-2025-62506	MinIO is a high-performance object storage system. In all versions prior to RELEASE.2025-10-15T17-29-55Z, a privilege escalation vulnerability allows service accounts and STS (Security Token Service) accounts with restricted session policies to bypass their inline policy restrictions when performing operations on their own account, specifically when creating new service accounts for the same user. The vulnerability exists in the IAM policy validation logic where the code incorrectly relied on the DenyOnly argument when validating session policies for restricted accounts. When a session policy is present, the system should validate that the action is allowed by the session policy, not just that it is not denied. An attacker with valid credentials for a restricted service or STS account can create a new service account for itself without policy restrictions, resulting in a new service account with full parent privileges instead of being restricted by the inline policy. This allows the attacker to access buckets and objects beyond their intended restrictions and modify, delete, or create objects outside their authorized scope. The vulnerability is fixed in version RELEASE.2025-10-15T17-29-55Z.	8.1	More Details
CVE-2025-62510	FileRise is a self-hosted web-based file manager with multi-file upload, editing, and batch operations. In version 1.4.0, a regression allowed folder visibility/ownership to be inferred from folder names. Low-privilege users could see or interact with folders matching their username and, in some cases, other users' content. This issue has been patched in version 1.5.0, where it introduces explicit per-folder ACLs (owners/read/write/share/read_own) and strict server-side checks across list, read, write, share, rename, copy/move, zip, and WebDAV paths.	8.1	More Details
CVE-2025-58073	Mattermost versions 10.11.x <= 10.11.1, 10.10.x <= 10.10.2, 10.5.x <= 10.5.10 fail to verify a user has permission to join a Mattermost team using the original invite token which allows any attacked to join any team on a Mattermost server regardless of restrictions via manipulating the OAuth state.	8.1	More Details
CVE-2025-62509	FileRise is a self-hosted web-based file manager with multi-file upload, editing, and batch operations. Prior to version 1.4.0, a business logic flaw in FileRise's file/folder handling allows low-privilege users to perform unauthorized operations (view/delete/modify) on files created by other users. The root cause was inferring ownership/visibility from folder names (e.g., a folder named after a username) and missing server-side authorization/ownership checks across file operation endpoints. This amounted to an IDOR pattern: an attacker could operate on resources identified only by predictable names. This issue has been patched in version 1.4.0 and further hardened in version 1.5.0. A workaround for this issue involves restricting non-admin users to read-only or disable delete/rename APIs server-side, avoid creating top-level folders named after other usernames, and adding server-side checks that verify ownership before delete/rename/move.	8.1	More Details
CVE-2025-58075	Mattermost versions 10.11.x <= 10.11.1, 10.10.x <= 10.10.2, 10.5.x <= 10.5.10 fail to verify a user has permission to join a Mattermost team using the original invite token which allows any attacked to join any team on a Mattermost server regardless of restrictions via manipulating the RelayState	8.1	More Details
CVE-2025-62518	astral-tokio-tar is a tar archive reading/writing library for async Rust. Versions of astral-tokio-tar prior to 0.5.6 contain a boundary parsing vulnerability that allows attackers to smuggle additional archive entries by exploiting inconsistent PAX/ustar header handling. When processing archives with PAX-extended headers containing size overrides, the parser incorrectly advances stream position based on ustar header size (often zero) instead of the PAX-specified size, causing it to interpret file content as legitimate tar headers. This issue has been patched in version 0.5.6. There are no workarounds.	8.1	More Details
CVE-2025-11899	Agentflow developed by Flowring has an Use of Hard-coded Cryptographic Key vulnerability, allowing unauthenticated remote attackers to exploit the fixed key to generate verification information, thereby logging into the system as any user. Attacker must first obtain an user ID in order to exploit this vulnerability.	8.1	More Details

CVE-2025-53043	Vulnerability in the Oracle Product Hub product of Oracle E-Business Suite (component: Item Catalog). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Product Hub. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Product Hub accessible data as well as unauthorized access to critical data or complete access to all Oracle Product Hub accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2025-56224	A lack of rate limiting in the One-Time Password (OTP) verification endpoint of SigningHub v8.6.8 allows attackers to bypass verification via a bruteforce attack.	8.1	More Details
CVE-2025-61751	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized access to critical data or complete access to all Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2025-61763	Vulnerability in Oracle Essbase (component: Essbase Web Platform). The supported version that is affected is 21.7.3.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Essbase. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Essbase accessible data as well as unauthorized access to critical data or complete access to all Oracle Essbase accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2025-62580	ASDA-Soft Stack-based Buffer Overflow Vulnerability	7.8	More Details
CVE-2025-8486	A potential vulnerability was reported in PC Manager that could allow a local authenticated user to execute code with elevated privileges.	7.8	More Details
CVE-2025-54279	Animate versions 23.0.13, 24.0.10 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-54658	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability [CWE-22] in Fortinet FortiDLP Agent's Outlookproxy plugin for MacOS 11.5.1 and 11.4.2 through 11.4.6 and 11.3.2 through 11.3.4 and 11.2.0 through 11.2.3 and 11.1.1 through 11.1.2 and 11.0.1 and 10.5.1 and 10.4.0, and 10.3.1 may allow an authenticated attacker to escalate their privilege to Root via sending a crafted request to a local listening port.	7.8	More Details
CVE-2025-41390	An arbitrary code execution vulnerability exists in the git functionality of Truffle Security Co. TruffleHog 3.90.2. A specially crafted repository can lead to a arbitrary code execution. An attacker can provide a malicious respository to trigger this vulnerability.	7.8	More Details
CVE-2025-10581	A potential DLL hijacking vulnerability was discovered in the Lenovo PC Manager during an internal security assessment that could allow a local authenticated user to execute code with elevated privileges.	7.8	More Details
CVE-2025-5555	A vulnerability has been found in Nixdorf Wincor PORT IO Driver up to 1.0.0.1. This affects the function sub_11100 in the library wnport.sys of the component IOCTL Handler. Such manipulation leads to stack-based buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. Upgrading to version 3.0.0.1 is able to mitigate this issue. Upgrading the affected component is recommended. The vendor was contacted beforehand and was able to provide a patch very early.	7.8	More Details
CVE-2025-61804	Animate versions 23.0.13, 24.0.10 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-54268	Bridge versions 14.1.8, 15.1.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-	ASDA-Soft Stack-based Buffer Overflow Vulnerability	7.8	More Details

62579			
CVE-2025-62382	Frigate is a network video recorder (NVR) with realtime local object detection for IP cameras. Prior to 0.16.2, Frigate's export workflow allows an authenticated operator to nominate any filesystem location as the thumbnail source for a video export. Because that path is copied verbatim into the publicly served clips directory, the feature can be abused to read arbitrary files that reside on the host running Frigate. In practice, a low-privilege user with API access can pivot from viewing camera footage to exfiltrating sensitive configuration files, secrets, or user data from the appliance itself. This behavior violates the principle of least privilege for the export subsystem and turns a convenience feature into a direct information disclosure vector, with exploitation hinging on a short race window while the background exporter copies the chosen file into place before cleanup runs. This vulnerability is fixed in 0.16.2.	7.7	More Details
CVE-2025-61488	An issue in Senayan Library Management System (SLiMS) 9 Bulian v.9.6.1 allows a remote attacker to execute arbitrary code via the scrap_image.php component and the imageURL parameter	7.6	More Details
CVE-2025-41253	The following versions of Spring Cloud Gateway Server Webflux may be vulnerable to the ability to expose environment variables and system properties to attackers. An application should be considered vulnerable when all the following are true: * The application is using Spring Cloud Gateway Server Webflux (Spring Cloud Gateway Server WebMVC is not vulnerable). * An admin or untrusted third party using Spring Expression Language (SpEL) to access environment variables or system properties via routes. * An untrusted third party could create a route that uses SpEL to access environment variables or system properties if: * The Spring Cloud Gateway Server Webflux actuator web endpoint is enabled via management.endpoints.web.exposure.include=gateway and management.endpoint.gateway.enabled=trueor management.endpoint.gateway.access=unrestricte. * The actuator endpoints are available to attackers. * The actuator endpoints are unsecured.	7.5	More Details
CVE-2025-53474	When an iRule using an ILX::call command is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-48008	When a TCP profile with Multipath TCP (MPTCP) enabled is configured on a virtual server, undisclosed traffic along with conditions beyond the attacker's control can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-53521	When a BIG-IP APM Access Policy is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-46706	When an iRule containing the HTTP::respond command is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-11722	The Woocommerce Category and Products Accordion Panel plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.0 via the 'categoryaccordionpanel' shortcode. This makes it possible for 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 in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	7.5	More Details
CVE-2025-41430	When BIG-IP SSL Orchestrator is enabled, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-26781	An issue was discovered in L2 in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 9110, W920, W930, Modem 5123, and Modem 5300. Incorrect handling of RLC AM PDUs leads to a Denial of Service.	7.5	More Details
CVE-2025-26782	An issue was discovered in L2 in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 9110, W920, W930, Modem 5123, and Modem 5300. Incorrect handling of RLC AM PDUs leads to a Denial of Service.	7.5	More Details
CVE-2025-54479	When a classification profile is configured on a virtual server without an HTTP or HTTP/2 profile, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-36128	IBM MQ 9.1, 9.2, 9.3, 9.4 LTS and 9.3, 9.4 CD is vulnerable to a denial of service, caused by improper enforcement of the timeout on individual read operations. By conducting slowloris-type attacks, a remote attacker could exploit this vulnerability to cause a denial of service.	7.5	More Details
	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.12 and 7.2.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox.		

CVE-2025-61760	Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H).	7.5	More Details
CVE-2025-11177	The External Login plugin for WordPress is vulnerable to SQL Injection via the 'log' parameter in all versions up to, and including, 1.11.2 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 when a PostgreSQL or MSSQL database is configured as the external authentication database.	7.5	More Details
CVE-2025-11691	The PPOM – Product Addons & Custom Fields for WooCommerce plugin for WordPress is vulnerable to SQL Injection via the PPOM_Meta::get_fields_by_id() function in all versions up to, and including, 33.0.15 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This is only exploitable when the Enable Legacy Price Calculations setting is enabled.	7.5	More Details
CVE-2025-53856	When a virtual server, network address translation (NAT) object, or secure network address translation (SNAT) object uses the embedded Packet Velocity Acceleration (ePVA) feature, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. To determine which BIG-IP platforms have an ePVA chip refer to K12837: Overview of the ePVA feature https://my.f5.com/manage/s/article/K12837 . Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-55036	When BIG-IP SSL Orchestrator explicit forward proxy is configured on a virtual server and the proxy connect feature is enabled, undisclosed traffic may cause memory corruption. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2024-55568	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 9110, W920, W930, W1000, Modem 5123, Modem 5300, Modem 5400. The absence of a NULL check leads to a Denial of Service when an attacker sends malformed MM packets to the target.	7.5	More Details
CVE-2025-54854	When a BIG-IP APM OAuth access profile (Resource Server or Resource Client) is configured on a virtual server, undisclosed traffic can cause the apmd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-58071	When IPsec is configured on the BIG-IP system, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-61974	When a client SSL profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-61960	When a per-request policy is configured on a BIG-IP APM portal access virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-61951	Undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. This issue may occur when a Datagram Transport Layer Security (DTLS) 1.2 virtual server is enabled with a Server SSL profile that is configured with a certificate, key, and the SSL Sign Hash set to ANY, and the backend server is enabled with DTLS 1.2 and client authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-61938	When a BIG-IP Advanced WAF or ASM security policy is configured with a URL greater than 1024 characters in length for the Data Guard Protection Enforcement setting, either manually or through the automatic Policy Builder, the bd process can terminate repeatedly. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-60016	When Diffie-Hellman (DH) group Elliptic Curve Cryptography (ECC) Brainpool curves are configured in an SSL profile's Cipher Rule or Cipher Group, and that profile is applied to a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-61935	When a BIG IP Advanced WAF or ASM security policy is configured on a virtual server, undisclosed requests can cause the bd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-	When DNS cache is configured on a BIG-IP or BIG-IP Next CNF virtual server, undisclosed DNS queries can cause an increase in memory resource utilization. Note: Software versions which have reached End of	7.5	More Details

59781	Technical Support (EoTS) are not evaluated.		
CVE-2025-59778	When the Allowed IP Addresses feature is configured on the F5OS-C partition control plane, undisclosed traffic can cause multiple containers to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-61990	When using a multi-bladed platform with more than one blade, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-59478	When a BIG-IP AFM denial-of-service (DoS) protection profile is configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-62370	Alloy Core libraries at the root of the Rust Ethereum ecosystem. Prior to 0.8.26 and 1.4.1, an uncaught panic triggered by malformed input to alloy_dyn_abi::TypedData could lead to a denial-of-service (DoS) via eip712_signing_hash(). Software with high availability requirements such as network services may be particularly impacted. If in use, external auto-restarting mechanisms can partially mitigate the availability issues unless repeated attacks are possible. The vulnerability was patched by adding a check to ensure the element is not empty before accessing its first element; an error is returned if it is empty. The fix is included in version v1.4.1 and backported to v0.8.26.	7.5	More Details
CVE-2025-58120	When HTTP/2 Ingress is configured, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-58096	When the database variable tm.tcpudptxchecksum is configured as non-default value Software-only on a BIG-IP system, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-20350	A vulnerability in the web UI of Cisco Desk Phone 9800 Series, Cisco IP Phone 7800 and 8800 Series, and Cisco Video Phone 8875 running Cisco SIP Software could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to a buffer overflow when an affected device processes HTTP packets. An attacker could exploit this vulnerability by sending crafted HTTP input to the device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To exploit this vulnerability, the phone must be registered to Cisco Unified Communications Manager and have Web Access enabled. Web Access is disabled by default.	7.5	More Details
CVE-2025-55669	When the BIG-IP Advanced WAF and ASM security policy and a server-side HTTP/2 profile are configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-54858	When a BIG-IP Advanced WAF or BIG-IP ASM Security Policy is configured with a JSON content profile that has a malformed JSON schema, and the security policy is applied to a virtual server, undisclosed requests can cause the bd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2025-11517	The Event Tickets and Registration plugin for WordPress is vulnerable to payment bypass in all versions up to, and including, 5.26.5. This is due to the /wp-json/tribe/tickets/v1/commerce/free/order endpoint not verifying that a ticket type should be free allowing the user to bypass the payment. This makes it possible for unauthenticated attackers to obtain access to paid tickets, without paying for them, causing a loss of revenue for the target.	7.5	More Details
CVE-2025-10743	The Outdoor plugin for WordPress is vulnerable to SQL Injection via the 'edit' action in all versions up to, and including, 1.3.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2025-61756	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: System Configuration). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Financial Services Analytical Applications Infrastructure. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2025-62584	Whale browser before 4.33.325.17 allows an attacker to bypass the Same-Origin Policy in a dual-tab environment.	7.5	More Details
CVE-2025-62585	Whale browser before 4.33.325.17 allows an attacker to bypass the Content Security Policy via a specific scheme in a dual-tab environment.	7.5	More Details

CVE-2025-41020	Insecure direct object reference (IDOR) vulnerability in Sergestec's Exito v8.0. This vulnerability allows an attacker to access data belonging to other customers through the 'id' parameter in '/admin/ticket_a4.php'.	7.5	More Details
CVE-2025-53066	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 8u461, 8u461-perf, 11.0.28, 17.0.16, 21.0.8, 25; Oracle GraalVM for JDK: 17.0.16 and 21.0.8; Oracle GraalVM Enterprise Edition: 21.3.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2025-56223	A lack of rate limiting in the component /Home/UploadStreamDocument of SigningHub v8.6.8 allows attackers to cause a Denial of Service (DoS) via uploading an excessive number of files.	7.5	More Details
CVE-2025-60751	GeographicLib 2.5 is vulnerable to Buffer Overflow in GeoConvert DMS::InternalDecode.	7.5	More Details
CVE-2025-61220	The incomplete verification mechanism in the AutoBizLine com.mysecondline.app 1.2.91 allows attackers to log in as other users and gain unauthorized access to their personal information.	7.5	More Details
CVE-2025-61752	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP/2 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2025-61581	** UNSUPPORTED WHEN ASSIGNED ** Inefficient Regular Expression Complexity vulnerability in Apache Traffic Control. This issue affects Apache Traffic Control: all versions. People with access to the management interface of the Traffic Router component could specify malicious patterns and cause unavailability. As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an alternative or restrict access to the instance to trusted users. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	7.5	More Details
CVE-2025-62356	A path traversal vulnerability in all versions of the Qodo Qodo Gen IDE enables a threat actor to read arbitrary local files in and outside of current projects on an end user’s system. The vulnerability can be reached directly and through indirect prompt injection.	7.5	More Details
CVE-2025-61301	Denial-of-analysis in reporting/mongodb.py and reporting/jsondump.py in CAPEv2 (commit 52e4b43, on 2025-05-17) allows attackers who can submit samples to cause incomplete or missing behavioral analysis reports by generating deeply nested or oversized behavior data that trigger MongoDB BSON limits or orjson recursion errors when the sample executes in the sandbox.	7.5	More Details
CVE-2025-59043	OpenBao is an open source identity-based secrets management system. In OpenBao versions prior to 2.4.1, JSON objects after decoding may use significantly more memory than their serialized version. It is possible to craft a JSON payload to maximize the factor between serialized memory usage and deserialized memory usage, similar to a zip bomb, with factors reaching approximately 35. This can be used to circumvent the max_request_size configuration parameter which is intended to protect against denial of service attacks. The request body is parsed into a map very early in the request handling chain before authentication, which means an unauthenticated attacker can send a specifically crafted JSON object and cause an out-of-memory crash. Additionally, for requests with large numbers of strings, the audit subsystem can consume large quantities of CPU. The vulnerability is fixed in version 2.4.1.	7.5	More Details
CVE-2025-11898	Agentflow developed by Flowring has an Arbitrary File Reading vulnerability, allowing unauthenticated remote attackers to exploit Relative Path Traversal to download arbitrary system files.	7.5	More Details
CVE-2025-11501	The Dynamically Display Posts plugin for WordPress is vulnerable to SQL Injection via the 'tax_query' parameter in all versions up to, and including, 1.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details

CVE-2025-53050	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Performance Monitor). Supported versions that are affected are 8.60, 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2025-11949	EasyFlow .NET and EasyFlow AiNet, developed by Digiwin, has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to obtain database administrator credentials via a specific functionality.	7.5	More Details
CVE-2025-62371	OpenSearch Data Prepper as an open source data collector for observability data. In versions prior to 2.12.2, the OpenSearch sink and source plugins in Data Prepper trust all SSL certificates by default when no certificate path is provided. Prior to this fix, the OpenSearch sink and source plugins would automatically use a trust all SSL strategy when connecting to OpenSearch clusters if no certificate path was explicitly configured. This behavior bypasses SSL certificate validation, potentially allowing attackers to intercept and modify data in transit through man-in-the-middle attacks. The vulnerability affects connections to OpenSearch when the cert parameter is not explicitly provided. This issue has been patched in version 2.12.2. As a workaround, users can add the cert parameter to their OpenSearch sink or source configuration with the path to the cluster's CA certificate.	7.4	More Details
CVE-2025-6042	The Lisfinity Core - Lisfinity Core plugin used for pebas® Lisfinity WordPress theme plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.4.0. This is due to the plugin assigning the editor role by default. While limitations with respect to capabilities are put in place, use of the API is not restricted. This vulnerability can be leveraged together with CVE-2025-6038 to obtain admin privileges.	7.3	More Details
CVE-2025-11943	A vulnerability has been found in 70mai X200 up to 20251010. Affected by this vulnerability is an unknown functionality of the component HTTP Web Server. The manipulation leads to use of default credentials. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-11864	A vulnerability was identified in NucleoidAI Nucleoid up to 0.7.10. The impacted element is the function extension.apply of the file /src/cluster.ts of the component Outbound Request Handler. Such manipulation of the argument https/ip/port/path/headers leads to server-side request forgery. The attack may be performed from remote.	7.3	More Details
CVE-2025-11942	A flaw has been found in 70mai X200 up to 20251010. Affected is an unknown function of the component Pairing. Executing manipulation can lead to missing authentication. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-60500	QDocs Smart School Management System 7.1 allows authenticated users with roles such as "accountant" or "admin" to bypass file type restrictions in the media upload feature by abusing the alternate YouTube URL option. This logic flaw permits uploading of arbitrary PHP files, which are stored in a web-accessible directory.	7.2	More Details
CVE-2025-57738	Apache Syncope offers the ability to extend / customize the base behavior on every deployment by allowing to provide custom implementations of a few Java interfaces; such implementations can be provided either as Java or Groovy classes, with the latter being particularly attractive as the machinery is set for runtime reload. Such a feature has been available for a while, but recently it was discovered that a malicious administrator can inject Groovy code that can be executed remotely by a running Apache Syncope Core instance. Users are recommended to upgrade to version 3.0.14 / 4.0.2, which fix this issue by forcing the Groovy code to run in a sandbox.	7.2	More Details
CVE-2025-62290	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Block Storage). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in takeover of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2025-10313	The Find And Replace content for WordPress plugin for WordPress is vulnerable to unauthorized Stored Cross-Site Scripting and Arbitrary Content Replacement due to a missing capability check on the far_admin_ajax_fun() function in all versions up to, and including, 1.1. This makes it possible for unauthenticated attackers to inject arbitrary web scripts into pages that can make privilege escalation and malicious redirects possible.	7.2	More Details
CVE-2025-10754	The DocoDoco Store Locator plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the zip upload functionality in all versions up to, and including, 1.0.1. This makes it possible for authenticated attackers, with Editor-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.40, USG FLEX series firmware versions from V4.50 through V5.40, USG FLEX 50(W) series		

2025-8078	firmware versions from V4.16 through V5.40, and USG20(W)-VPN series firmware versions from V4.16 through V5.40 could allow an authenticated attacker with administrator privileges to execute operating system (OS) commands on the affected device by passing a crafted string as an argument to a CLI command.	7.2	More Details
CVE-2025-10051	The Demo Import Kit plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in all versions up to, and including, 1.1.0 via the import functionality. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2025-62429	ClipBucket v5 is an open source video sharing platform. Prior to version 5.5.2 #147, ClipBucket v5 is vulnerable to arbitrary PHP code execution. In /upload/admin_area/actions/update_launch.php, the "type" parameter from a POST request is embedded into PHP tags and executed. Proper sanitization is not performed, and by injecting malicious code an attacker can execute arbitrary PHP code. This allows an attacker to achieve RCE. This issue has been resolved in version 5.5.2 #147.	7.2	More Details
CVE-2020-36853	The 10WebMapBuilder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Plugin Settings Change in versions up to, and including, 1.0.63 due to insufficient input sanitization and output escaping and a lack of capability checks. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-61541	Webmin 2.510 is vulnerable to a Host Header Injection in the password reset functionality (forgot_send.cgi). The reset link sent to users is constructed using the HTTP Host header via get_webmin_email_url(). An attacker can manipulate the Host header to inject a malicious domain into the reset email. If a victim follows the poisoned link, the attacker can intercept the reset token and gain full control of the target account.	7.1	More Details
CVE-2025-3465	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ABB CoreSense™ HM, ABB CoreSense™ M10.This issue affects CoreSense™ HM: through 2.3.1; CoreSense™ M10: through 1.4.1.12.	7.1	More Details
CVE-2025-56219	Incorrect access control in SigningHub v8.6.8 allows attackers to arbitrarily add user accounts without any rate limiting. This can lead to a resource exhaustion and a Denial of Service (DoS) when an excessively large number of user accounts are created.	7.1	More Details
CVE-2025-62527	Taguette is an open source qualitative research tool. An issue has been discovered in Taguette versions prior to 1.5.0. It was possible for an attacker to request password reset email containing a malicious link, allowing the attacker to set the email if clicked by the victim. This issue has been patched in version 1.5.0.	7.1	More Details
CVE-2025-61543	A Host Header Injection vulnerability exists in the password reset functionality of CraftMyCMS 4.0.2.2. The system uses `$_SERVER['HTTP_HOST']` directly to construct password reset links sent via email. An attacker can manipulate the Host header to send malicious reset links, enabling phishing attacks or account takeover.	7.1	More Details
CVE-2025-11940	A security vulnerability has been detected in LibreWolf up to 143.0.4-1 on Windows. This affects an unknown function of the file assets/setup.nsi of the component Installer. Such manipulation leads to uncontrolled search path. The attack must be carried out locally. Attacks of this nature are highly complex. The exploitability is reported as difficult. Upgrading to version 144.0-1 mitigates this issue. The name of the patch is dd10e31dd873e9cb309fad8aed921d45bf905a55. It is suggested to upgrade the affected component.	7.0	More Details
CVE-2025-62415	Bagisto is an open source laravel eCommerce platform. In Bagisto v2.3.7, the TinyMCE image upload functionality allows an attacker with sufficient privileges (e.g. admin) to upload a crafted HTML file containing embedded JavaScript. When viewed, the malicious code executes in the context of the admin/user’s browser. This vulnerability is fixed in 2.3.8.	6.9	More Details
CVE-2025-62414	Bagisto is an open source laravel eCommerce platform. In Bagisto v2.3.7, the “Create New Customer” feature (in the admin panel) is vulnerable to Cross-Site Scripting (XSS). An attacker with access to the admin create-customer form can inject malicious JavaScript payloads into certain input fields. These payloads may later execute in the context of an admin’s browser or another user viewing the customer data, enabling session theft or admin-level actions. This vulnerability is fixed in 2.3.8.	6.9	More Details
CVE-2025-62418	Bagisto is an open source laravel eCommerce platform. In Bagisto v2.3.7, the TinyMCE image upload functionality allows an attacker with sufficient privileges (e.g. admin) to upload a crafted SVG file containing embedded JavaScript. When viewed, the malicious code executes in the context of the admin/user’s browser. This vulnerability is fixed in 2.3.8.	6.9	More Details
CVE-2025-31702	A vulnerability exists in certain Dahua embedded products. Third-party malicious attacker with obtained normal user credentials could exploit the vulnerability to access certain data which are restricted to admin privileges, such as system-sensitive files through specific HTTP request. This may cause tampering with admin password, leading to privilege escalation. Systems with only admin account are not affected.	6.8	More Details
CVE-2025-6515	The MCP SSE endpoint in oatpp-mcp returns an instance pointer as the session ID, which is not unique nor cryptographically secure. This allows network attackers with access to the oatpp-mcp server to guess future session IDs and hijack legitimate client MCP sessions, returning malicious responses from the oatpp-mcp server.	6.8	More Details

CVE-2025-5517	Heap-based Buffer Overflow vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (MID/ CE) -Terra AC MID, ABB Terra AC wallbox (MID/ CE) -Terra AC Juno CE, ABB Terra AC wallbox (MID/ CE) -Terra AC PTB, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): through 1.8.32; Terra AC wallbox (UL32A): through 1.8.2; Terra AC wallbox (MID/ CE) -Terra AC MID: through 1.8.32; Terra AC wallbox (MID/ CE) -Terra AC Juno CE: through 1.8.32; Terra AC wallbox (MID/ CE) -Terra AC PTB: through 1.8.21; Terra AC wallbox (JP): through 1.8.2.	6.8	More Details
CVE-2025-60856	Reolink Video Doorbell WiFi DB_566128M5MP_W allows root shell access through an unsecured UART/serial console. An attacker with physical access can connect to the exposed interface and execute arbitrary commands with root privileges. NOTE: this is disputed by the Supplier because of "certain restrictions on users privately connecting serial port cables" and because "the root user has a password and it meets the requirements of password security complexity."	6.8	More Details
CVE-2025-62424	ClipBucket is a web-based video-sharing platform. In ClipBucket version 5.5.2 - #146 and earlier, the /admin_area/template_editor.php endpoint is vulnerable to path traversal. The validation of the file-loading path is inadequate, allowing authenticated administrators to read and write arbitrary files outside the intended template directory by inserting path traversal sequences into the folder parameter. An attacker with administrator privileges can exploit this vulnerability to read sensitive files such as /etc/passwd and modify writable files on the system, potentially leading to sensitive information disclosure and compromise of the application or server. This issue is fixed in version 5.5.2 - #147.	6.7	More Details
CVE-2025-62423	ClipBucket V5 provides open source video hosting with PHP. In version5.5.2 - #140 and earlier, a Blind SQL injection vulnerability exists in the Admin Area’s “/admin_area/login_as_user.php” file. Exploiting this vulnerability requires access privileges to the Admin Area.	6.7	More Details
CVE-2025-60344	An unauthenticated Local File Inclusion (LFI) vulnerability in D-Link DSR series routers allows remote attackers to retrieve sensitive configuration files in clear text. The exposed files contain administrative credentials, VPN settings, and other sensitive information, enabling full administrative access to the router. Affected Products include: DSR-150, DSR-150N, and DSR-250N v1.09B32_WW.	6.6	More Details
CVE-2025-61514	An arbitrary file upload vulnerability in SageMath, Inc CoCalc before commit 0d2ff58 allows attackers to execute arbitrary code via uploading a crafted SVG file.	6.5	More Details
CVE-2025-61540	SQL injection vulnerability in Ultimate PHP Board 2.2.7 via the username field in lostpassword.php.	6.5	More Details
CVE-2025-48087	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jason C. Memberlite Shortcodes memberlite-shortcodes allows Stored XSS.This issue affects Memberlite Shortcodes: from n/a through 1.4.1.	6.5	More Details
CVE-2025-61330	A hard-coded weak password vulnerability has been discovered in all Magic-branded devices from Chinese network equipment manufacturer H3C. The vulnerability stems from the use of a hard-coded weak password for the root account in the /etc/shadow configuration or even the absence of any password at all. Some of these devices have the Telnet service enabled by default, or users can choose to enable the Telnet service in other device management interfaces (e.g. /debug.asp or /debug_telnet.asp). In addition, these devices have related interfaces called Virtual Servers, which can map the devices to the public network, posing the risk of remote attacks. Therefore, attackers can obtain the highest root privileges of the devices through the Telnet service using the weak password hardcoded in the firmware (or without a password), and remote attacks are possible.	6.5	More Details
CVE-2025-11372	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to modification of data in all versions up to, and including, 4.2.9.2. This is due to missing capability checks on the Admin Tools REST endpoints which are registered with permission_callback set to __return_true. This makes it possible for unauthenticated attackers to perform destructive database operations including dropping indexes on any table (including WordPress core tables like wp_options), creating duplicate configuration entries, and degrading site performance via the /wp-json/lp/v1/admin/tools/create-indexs endpoint granted they can provide table names.	6.5	More Details
CVE-2025-9559	Pega Platform versions 8.7.5 to Infinity 24.2.2 are affected by a Insecure Direct Object Reference issue in a user interface component that can only be used to read data.	6.5	More Details
CVE-2025-55090	In NetX Duo before 6.4.4, the networking support module for Eclipse Foundation ThreadX, there was a potential out of bound read issue in _nx_ipv4_packet_receive() function when received an Ethernet frame with less than 4 bytes of IP packet.	6.5	More Details
CVE-2025-58051	Nextcloud Tables allows you to create your own tables with individual columns. Prior 0.7.6, 0.8.8, and 0.9.5, when importing a table, a user was able to specify files on the server and when their format is supported by the used PhpSpreadsheet library they would be included and their content leaked to the user. It is recommended that the Nextcloud Tables app is upgraded to 0.7.6, 0.8.8 or 0.9.5.	6.5	More Details

CVE-2025-62504	Envoy is an open source edge and service proxy. Envoy versions earlier than 1.36.2, 1.35.6, 1.34.10, and 1.33.12 contain a use-after-free vulnerability in the Lua filter. When a Lua script executing in the response phase rewrites a response body so that its size exceeds the configured per_connection_buffer_limit_bytes (default 1MB), Envoy generates a local reply whose headers override the original response headers, leaving dangling references and causing a crash. This results in denial of service. Updating to versions 1.36.2, 1.35.6, 1.34.10, or 1.33.12 fixes the issue. Increasing per_connection_buffer_limit_bytes (and for HTTP/2 the initial_stream_window_size) or increasing per_request_buffer_limit_bytes / request_body_buffer_limit can reduce the likelihood of triggering the condition but does not correct the underlying memory safety flaw.	6.5	More Details
CVE-2025-11683	YAML::Syck versions before 1.36 for Perl has missing null-terminators which causes out-of-bounds read and potential information disclosure Missing null terminators in token.c leads to but-of-bounds read which allows adjacent variable to be read The issue is seen with complex YAML files with a hash of all keys and empty values. There is no indication that the issue leads to accessing memory outside that allocated to the module.	6.5	More Details
CVE-2025-57164	Flowise through v3.0.4 is vulnerable to remote code execution via unsanitized evaluation of user input in the "Supabase RPC Filter" field.	6.5	More Details
CVE-2025-62651	The Restaurant Brands International (RBI) assistant platform through 2025-09-06 does not implement access control for the bathroom rating interface.	6.5	More Details
CVE-2025-60514	Tillywork v0.1.3 and below is vulnerable to SQL Injection in app/common/helpers/query.builder.helper.ts.	6.5	More Details
CVE-2025-0277	HCL BigFix Mobile 3.3 and earlier are vulnerable to certain insecure directives within the Content Security Policy (CSP). An attacker could trick users into performing actions by not properly restricting the sources of scripts and other content.	6.5	More Details
CVE-2025-0276	HCL BigFix Modern Client Management (MCM) 3.3 and earlier are vulnerable to certain insecure directives within the Content Security Policy (CSP). An attacker could trick users into performing actions by not properly restricting the sources of scripts and other content.	6.5	More Details
CVE-2025-62508	Citizen is a MediaWiki skin that makes extensions part of the cohesive experience. Citizen from 3.3.0 to 3.9.0 are vulnerable to stored cross-site scripting in the sticky header button message handling. In stickyHeader.js the copyButtonAttributes function assigns innerHTML from a source element’s textContent when copying button labels. This causes escaped HTML in system message content (such as citizen-share, citizen-view-history, citizen-view-edit, and nstab-talk) to be interpreted as HTML in the sticky header, allowing injection of arbitrary script by a user with the ability to edit interface messages. The vulnerability allows a user with the editinterface right but without the editsitejs right (by default the sysop group has editinterface but may not have editsitejs) to execute arbitrary JavaScript in other users’ sessions, enabling unauthorized access to sensitive data or actions. The issue is fixed in 3.9.0.	6.5	More Details
CVE-2025-20359	Multiple Cisco products are affected by a vulnerability in the Snort 3 HTTP Decoder that could allow an unauthenticated, remote attacker to cause the disclosure of possible sensitive data or cause the Snort 3 Detection Engine to crash. This vulnerability is due to an error in the logic of buffer handling when the MIME fields of the HTTP header are parsed. This can result in a buffer under-read. An attacker could exploit this vulnerability by sending crafted HTTP packets through an established connection that is parsed by Snort 3. A successful exploit could allow the attacker to induce one of two possible outcomes: the unexpected restarting of the Snort 3 Detection Engine, which could cause a denial of service (DoS) condition, or information disclosure of sensitive information in the Snort 3 data stream. Due to the under-read condition, it is possible that sensitive information that is not valid connection data could be returned.	6.5	More Details
CVE-2025-53092	Strapi is an open source headless content management system. Strapi versions prior to 5.20.0 contain a CORS misconfiguration vulnerability in default installations. By default, Strapi reflects the value of the Origin header back in the Access-Control-Allow-Origin response header without proper validation or whitelisting. This allows an attacker-controlled site to send credentialed requests to the Strapi backend. An attacker can exploit this by hosting a malicious site on a different origin (e.g., different port) and sending requests with credentials to the Strapi API. The vulnerability is fixed in version 5.20.0. No known workarounds exist.	6.5	More Details
CVE-2025-55091	In NetX Duo before 6.4.4, the networking support module for Eclipse Foundation ThreadX, there was a potential out of bound read issue in _nx_ip_packet_receive() function when received an Ethernet with type set as IP but no IP data.	6.5	More Details
CVE-2025-60641	The file mexcel.php in the Vfront 0.99.52 codebase contains a vulnerable call to unserialize(base64_decode($_POST['mexcel'])), where $_POST['mexcel'] is user-controlled input. This input is decoded from base64 and deserialized without validation or use of the allowed_classes option, allowing an attacker to inject arbitrary PHP objects. This can lead to malicious behavior, such as Remote Code Execution (RCE), SQL Injection, Path Traversal, or Denial of Service, depending on the availability of exploitable classes in the Vfront codebase or its dependencies.	6.5	More Details

CVE-2025-10575	The WP jQuery Pager plugin for WordPress is vulnerable to SQL Injection via the 'ids' shortcode attribute parameter handled by the WPJqueryPaged::get_gallery_page_imgs() function in all versions up to, and including, 1.4.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-61194	daicuocms V1.3.13 contains a SQL injection vulnerability in the file library\think\db\Builder.php.	6.5	More Details
CVE-2025-56450	Log2Space Subscriber Management Software 1.1 is vulnerable to unauthenticated SQL injection via the `lead_id` parameter in the `/l2s/api/selfcareLeadHistory` endpoint. A remote attacker can exploit this by sending a specially crafted POST request, resulting in the execution of arbitrary SQL queries. The backend fails to sanitize the user input, allowing enumeration of database schemas, table names, and potentially leading to full database compromise.	6.5	More Details
CVE-2025-55039	This issue affects Apache Spark versions before 3.4.4, 3.5.2 and 4.0.0. Apache Spark versions before 4.0.0, 3.5.2 and 3.4.4 use an insecure default network encryption cipher for RPC communication between nodes. When spark.network.crypto.enabled is set to true (it is set to false by default), but spark.network.crypto.cipher is not explicitly configured, Spark defaults to AES in CTR mode (AES/CTR/NoPadding), which provides encryption without authentication. This vulnerability allows a man-in-the-middle attacker to modify encrypted RPC traffic undetected by flipping bits in ciphertext, potentially compromising heartbeat messages or application data and affecting the integrity of Spark workflows. To mitigate this issue, users should either configure spark.network.crypto.cipher to AES/GCM/NoPadding to enable authenticated encryption or enable SSL encryption by setting spark.ssl.enabled to true, which provides stronger transport security.	6.5	More Details
CVE-2025-10038	The Binary MLM Plan plugin for WordPress is vulnerable to limited Privilege Escalation in all versions up to, and including, 3.0. This is due to bmp_user role granting all users with the manage_bmp capability by default upon registration through the plugin's form. This makes it possible for unauthenticated attackers to register and manage the plugin's settings.	6.5	More Details
CVE-2025-60783	There is a SQL injection vulnerability in Restaurant Management System DBMS Project v1.0 via login.php. The vulnerability allows attackers to manipulate the application's database through specially crafted SQL query strings.	6.5	More Details
CVE-2025-10660	The WP Dashboard Chat plugin for WordPress is vulnerable to SQL Injection via the ‘id’ parameter in all versions up to, and including, 1.0.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-10682	The TARIFFUXX plugin for WordPress is vulnerable to SQL Injection in versions up to, and including, 1.4. This is due to insufficient neutralization of user-supplied input used directly in SQL queries. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject additional SQL into queries and extract sensitive information from the database via a crafted id attribute in the 'tariffuxx_configurator' shortcode.	6.5	More Details
CVE-2025-10730	The Wp tabber widget plugin for WordPress is vulnerable to SQL Injection via the 'wp-tabber-widget' shortcode in all versions up to, and including, 4.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-11365	The WP Google Map Plugin plugin for WordPress is vulnerable to blind SQL Injection via the 'id' parameter of the 'google_map' shortcode in all versions up to, and including, 1.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-61181	daicuocms V1.3.13 contains an arbitrary file upload vulnerability in the image upload feature.	6.5	More Details
CVE-2025-47148	When the BIG-IP system is configured as both a Security Assertion Markup Language (SAML) service provider (SP) and Identity Provider (IdP), with single logout (SLO) enabled on an access policy, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2025-	When SNMP is configured on F5OS Appliance and Chassis systems, undisclosed requests can cause an increase in SNMP memory resource utilization. Note: Software versions which have reached End of Technical	6.5	More

47150	Support (EoTS) are not evaluated.		Details
CVE-2025-53068	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	6.5	More Details
CVE-2025-6239	Zohocorp ManageEngine Applications Manager versions 176800 and below are vulnerable to information disclosure in File/Directory monitor.	6.5	More Details
CVE-2025-54805	When an iRule is configured on a virtual server via the declarative API, upon re-instantiation, the cleanup process can cause an increase in the Traffic Management Microkernel (TMM) memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2025-55670	On BIG-IP Next CNF, BIG-IP Next SPK, and BIG-IP Next for Kubernetes systems, repeated undisclosed API calls can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2025-61758	Vulnerability in the PeopleSoft Enterprise FIN IT Asset Management product of Oracle PeopleSoft (component: IT Asset Management). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN IT Asset Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise FIN IT Asset Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2025-61759	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.12 and 7.2.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	6.5	More Details
CVE-2025-54957	An issue was discovered in Dolby UDC 4.5 through 4.13. A crash of the DD+ decoder process can occur when a malformed DD+ bitstream is processed. When Evolution data is processed by evo_priv.c from the DD+ bitstream, the decoder writes that data into a buffer. The length calculation for a write can overflow due to an integer wraparound. This can lead to the allocated buffer being too small, and the out-of-bounds check of the subsequent write to be ineffective, leading to an out-of-bounds write.	6.5	More Details
CVE-2025-56799	Reolink desktop application 8.18.12 contains a command injection vulnerability in its scheduled cache-clearing mechanism via a crafted folder name.	6.5	More Details
CVE-2025-53035	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2025-60639	Hardcoded credentials in gsigel14 ATLAS-EPIC commit f29312c (2025-05-26).	6.5	More Details
CVE-2025-59483	A validation vulnerability exists in an undisclosed URL in the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
CVE-2025-50075	Vulnerability in the Oracle Financial Services Revenue Management and Billing product of Oracle Financial Services Applications (component: Security Management System). Supported versions that are affected are 2.9.0.0.0-7.2.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Revenue Management and Billing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financial Services Revenue Management and Billing accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Service API). Supported		

CVE-2025-61754	versions that are affected are 7.6.0.0.0 and 8.2.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2025-10133	The URLYar URL Shortner plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'urlyar_shortlink' shortcode in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11814	The Ultimate Addons for WPBakery plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to 3.21.1 (exclusive) due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-10135	The WP ViewSTL plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'viewstl' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11161	The WPBakery Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the vc_custom_heading shortcode in all versions up to, and including, 8.6.1. This is due to insufficient restriction of allowed HTML tags and improper sanitization of user-supplied attributes in the font_container parameter. This makes it possible for authenticated attackers with contributor-level access or higher to inject arbitrary web scripts in posts that will execute whenever a user accesses an injected page via the vc_custom_heading shortcode with malicious tag and text attributes granted they have access to use WPBakery shortcodes.	6.4	More Details
CVE-2025-8561	The Ova Advent plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes in all versions up to, and including, 1.1.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-62648	The Restaurant Brands International (RBI) assistant platform through 2025-09-06 allows remote attackers to adjust Drive Thru speaker audio volume.	6.4	More Details
CVE-2025-11160	The WPBakery Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Custom JS module in all versions up to, and including, 8.6.1. This is due to insufficient input sanitization and output escaping of user-supplied JavaScript code in the Custom JS module. This makes it possible for authenticated attackers with contributor-level access or higher to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page via the WPBakery Page Builder Custom JS module granted they have access to the WPBakery editor for post types.	6.4	More Details
CVE-2025-10132	The Dhivehi Text plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'dhivehi' shortcode in all versions up to, and including, 0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-10140	The Quick Social Login plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'quick-login' shortcode in all versions up to, and including, 1.4.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-10139	The WP BookWidgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'bw_link' shortcode in all versions up to, and including, 0.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2020-36854	The Async JavaScript plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 2.19.07.14. This is due to missing authorization checks on the aj_steps AJAX aciton along with a lack on sanitization on the settings saved via the function. This makes it possible for authenticated attackers with subscriber level permissions and above to inject malicious web scripts into a page that execute whenever a user accesses that page.	6.4	More Details
CVE-2025-10194	The Shortcode Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'button' shortcode in all versions up to, and including, 1.1.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE-2025-56748	Creativeitem Academy LMS up to and including 5.13 uses predictable password reset tokens based on Base64 encoded templates without rate limiting, allowing brute force attacks to guess valid reset tokens and compromise user accounts.	6.4	More Details
CVE-2025-11361	The Gutenberg Essential Blocks – Page Builder for Gutenberg Blocks & Patterns plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.7.1 via the eb_save_ai_generated_image function. This makes it possible for authenticated attackers, with Author-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	6.4	More Details
CVE-2025-11857	The XX2WP Integration Tools plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mxp_fb2wp_display_embed' shortcode in all versions up to, and including, 1.9.9. This is due to the plugin not properly sanitizing user input and output of the 'post_id' parameter. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-10006	The WPBakery Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'rev_slider_vc' shortcode in all versions up to, and including, 8.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is only exploitable when RevSlider is also installed.	6.4	More Details
CVE-2025-11270	The Gutenberg Essential Blocks – Page Builder for Gutenberg Blocks & Patterns plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'titleTag' attribute in all versions up to, and including, 5.7.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9562	The Redirection for Contact Form 7 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's qs_date shortcode in all versions up to, and including, 3.2.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-10141	The Digiseller plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ds' shortcode in all versions up to, and including, 1.3.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11910	A security vulnerability has been detected in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. This affects the function Query of the file /MemoryState.do?Action=Query. The manipulation of the argument orderField leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-11905	A vulnerability was found in yanyutao0402 ChanCMS up to 3.3.2. This vulnerability affects the function getArticle of the file app\modules\cms\controller\gather.js. The manipulation results in code injection. The attack may be launched 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 way.	6.3	More Details
CVE-2025-11908	A security flaw has been discovered in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. The affected element is the function uploadFile of the file /FileDir.do?Action=Upload. Performing manipulation of the argument File results in unrestricted upload. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-11911	A vulnerability was detected in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. This impacts the function Query of the file /DeviceFault.do?Action=Query. The manipulation of the argument sortField results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-11904	A vulnerability has been found in yanyutao0402 ChanCMS up to 3.3.2. This affects the function hasUse of the file /cms/model/hasUse. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-11909	A weakness has been identified in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. The impacted element is the function queryLast of the file /RepairRecord.do?Action=QueryLast. Executing manipulation of the argument orderField can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE-2025-11912	A flaw has been found in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. Affected is the function Query of the file /DeviceState.do?Action=Query. This manipulation of the argument orderField causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-62511	yt-grabber-tui is a C++ terminal user interface application for downloading YouTube content. yt-grabber-tui version 1.0 contains a Time-of-Check to Time-of-Use (TOCTOU) race condition (CWE-367) in the creation of the default configuration file config.json. In version 1.0, load_json_settings in Settings.hpp checks for the existence of config.json using boost::filesystem::exists and, if the file is missing, calls create_json_settings which writes the JSON configuration with boost::property_tree::write_json. A local attacker with write access to the application's configuration directory (~/.config/yt-grabber-tui on Linux or the current working directory on Windows) can create a symbolic link between the existence check and the subsequent write so that the write operation follows the symlink and overwrites an attacker-chosen file accessible to the running process. This enables arbitrary file overwrite within the privileges of the application process, which can corrupt files and cause loss of application or user data. If the application is executed with elevated privileges, this could extend to system file corruption. The issue is fixed in version 1.0.1.	6.3	More Details
CVE-2025-11853	A vulnerability was determined in Sismics Teedy up to 1.11. This affects an unknown function of the file /api/file of the component API Endpoint. Executing manipulation can lead to improper access controls. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-61762	Vulnerability in the PeopleSoft Enterprise FIN Payables product of Oracle PeopleSoft (component: Payables). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Payables. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise FIN Payables accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise FIN Payables accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise FIN Payables. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	6.3	More Details
CVE-2025-11902	A vulnerability was detected in yanyutao0402 ChanCMS up to 3.3.2. Affected by this vulnerability is the function findField of the file /cms/article/findField. Performing manipulation of the argument cid results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-11903	A flaw has been found in yanyutao0402 ChanCMS up to 3.3.2. Affected by this issue is the function update of the file /cms/article/update. Executing manipulation of the argument cid can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-11842	A security vulnerability has been detected in Shazwazza Smidge up to 4.5.1. The impacted element is an unknown function of the component Bundle Handler. The manipulation of the argument Version leads to path traversal. Remote exploitation of the attack is possible. Upgrading to version 4.6.0 is sufficient to resolve this issue. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2025-54764	Mbed TLS before 3.6.5 allows a local timing attack against certain RSA operations, and direct calls to mbedtls_mpi_mod_inv or mbedtls_mpi_gcd.	6.2	More Details
CVE-2025-55035	Mattermost Desktop App versions <=5.13.0 fail to manage modals in the Mattermost Desktop App that stops a user with a server that uses basic authentication from accessing their server which allows an attacker that provides a malicious server to the user to deny use of the Desktop App via having the user configure the malicious server and forcing a modal popup that cannot be closed.	6.1	More Details
CVE-2025-61539	Cross site scripting (XSS) vulnerability in Ultimate PHP Board 2.2.7 via the u_name parameter in lostpassword.php.	6.1	More Details
CVE-2025-53056	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Object and Environment Tech). Supported versions that are affected are 9.2.0.0-9.2.9.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 8.60, 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise		

CVE-2025-53055	PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2025-61753	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: Miscellaneous). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Scripting, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Scripting accessible data as well as unauthorized read access to a subset of Oracle Scripting accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2025-53052	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Workflow Notification Mailer). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Workflow, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Workflow accessible data as well as unauthorized read access to a subset of Oracle Workflow accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2025-53041	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.2.5-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iStore accessible data as well as unauthorized read access to a subset of Oracle iStore accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2025-53058	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: Application Logging Interfaces). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Manager accessible data as well as unauthorized read access to a subset of Oracle Applications Manager accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2025-62287	Vulnerability in the Oracle Life Sciences InForm product of Oracle Health Sciences Applications (component: Web Server). The supported version that is affected is 7.0.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Life Sciences InForm. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Life Sciences InForm, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Life Sciences InForm accessible data as well as unauthorized read access to a subset of Oracle Life Sciences InForm accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2025-62413	MQTTX is an MQTT 5.0 desktop client and MQTT testing tool. A Cross-Site Scripting (XSS) vulnerability was introduced in MQTTX v1.12.0 due to improper handling of MQTT message payload rendering. Malicious payloads containing HTML or JavaScript could be rendered directly in the MQTTX message viewer. If exploited, this could allow attackers to execute arbitrary scripts in the context of the application UI — for example, attempting to access MQTT connection credentials or trigger unintended actions through script injection. This vulnerability is especially relevant when MQTTX is used with brokers in untrusted or multi-tenant environments, where message content cannot be fully controlled. This vulnerability is fixed in 1.12.1.	6.1	More Details
CVE-2025-62407	Frappe is a full-stack web application framework. Prior to 14.98.0 and 15.83.0, an open redirect was possible through the redirect argument on the login page, if a specific type of URL was passed in. This vulnerability is fixed in 14.98.0 and 15.83.0.	6.1	More Details
CVE-	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are 9.2.0.0-9.2.9.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the		

2025-53060	vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2025-61454	A Cross-Site Scripting (XSS) vulnerability exists in Bhabishya-123 E-commerce 1.0, specifically within the search endpoint. Unsanitized input in the /search parameter is directly reflected back into the response HTML, allowing attackers to execute arbitrary JavaScript in the browser of a user who visits a malicious link or submits a crafted request.	6.1	More Details
CVE-2025-60781	PHP Education Manager v1.0 is vulnerable to Cross Site Scripting (XSS) in the worksheet.php file via the participant_name parameter.	6.1	More Details
CVE-2025-60934	Multiple stored cross-site scripting (XSS) vulnerabilities in the index.php component of HR Performance Solutions Performance Pro v3.19.17 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Employee Notes, title, or description parameters. The patched version is PP-Release-6.3.2.0.	6.1	More Details
CVE-2025-61933	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of BIG-IP APM that allows an attacker to run JavaScript in the context of the targeted logged-out user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.1	More Details
CVE-2025-61456	A Cross-Site Scripting (XSS) vulnerability exists in Bhabishya-123 E-commerce 1.0, specifically within the index endpoint. Unsanitized input in the /index parameter is directly reflected back into the response HTML, allowing attackers to execute arbitrary JavaScript in the browser of a user who visits a malicious link or submits a crafted request.	6.1	More Details
CVE-2025-20351	A vulnerability in the web UI of Cisco Desk Phone 9800 Series, Cisco IP Phone 7800 and 8800 Series, and Cisco Video Phone 8875 running Cisco SIP Software could allow an unauthenticated, remote attacker to conduct XSS attacks against a user of the web UI. This vulnerability exists because the web UI of an affected device does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Note: To exploit this vulnerability, the phone must be registered to Cisco Unified Communications Manager and have Web Access enabled. Web Access is disabled by default.	6.1	More Details
CVE-2025-62378	CommandKit is the discord.js meta-framework for building Discord bots. In versions 1.2.0-rc.1 through 1.2.0-rc.11, a logic flaw exists in the message command handler that affects how the commandName property is exposed to both middleware functions and command execution contexts when handling command aliases. When a message command is invoked using an alias, the ctx.commandName value reflects the alias rather than the canonical command name. This occurs in both middleware functions and within the command's own run function. Although not explicitly documented, CommandKit's examples and guidance around middleware usage implicitly convey that ctx.commandName represents the canonical command identifier. Middleware examples in the documentation consistently use ctx.commandName to reference the command being executed. Developers who assume ctx.commandName is canonical may introduce unintended behavior when relying on it for logic such as permission checks, rate limiting, or audit logging. This could allow unauthorized command execution or inaccurate access control decisions. Slash commands and context menu commands are not affected. This issue has been patched in version 1.2.0-rc.12, where ctx.commandName now consistently returns the actual canonical command name regardless of the alias used to invoke it.	6.1	More Details
CVE-2025-10612	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in giSoft Information Technologies City Guide allows Reflected XSS.This issue affects City Guide: before 1.4.45.	6.1	More Details
CVE-2025-57521	Bambu Studio 2.1.1.52 and earlier is affected by a vulnerability that allows arbitrary code execution during application startup. The application loads a network plugin without validating its digital signature or verifying its authenticity. A local attacker can exploit this behavior by placing a malicious component in the expected location, which is controllable by the attacker (e.g., under %APPDATA%), resulting in code execution within the context of the user. The main application is digitally signed, which may allow a malicious component to inherit trust and evade detection by security solutions that rely on signed parent processes.	6.1	More Details
CVE-2025-60932	Multiple stored cross-site scripting (XSS) vulnerabilities in the Current Goals function of HR Performance Solutions Performance Pro v3.19.17 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Goal Name, Goal Notes, Action Step Name, Action Step Description, Note Name, and Goal Description parameters. The patched version is PP-Release-6.3.2.0.	6.1	More Details
CVE-2025-60933	Multiple stored cross-site scripting (XSS) vulnerabilities in the Future Goals function of HR Performance Solutions Performance Pro v3.19.17 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Goal Name, Goal Notes, Action Step Name, Action Step Description, Note Name, and	6.1	More Details

	Goal Description parameters. The patched version is PP-Release-6.3.2.0.		
CVE-2025-59269	A stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.1	More Details
CVE-2025-60280	Cross-Site Scripting (XSS) vulnerability in Bang Resto v1.0 could allow an attacker to inject malicious JavaScript code into the application's web pages. This vulnerability exists due to insufficient input sanitization or output encoding, allowing attacker-controlled input to be rendered directly in the browser. When exploited, an attacker can steal session cookies, redirect users to malicious sites, perform actions on behalf of the user, or deface the website. This can lead to user data compromise, loss of user trust, and a broader attack surface for more advanced exploitation techniques.	6.1	More Details
CVE-2025-61457	code16 Sharp v9.6.6 is vulnerable to Cross Site Scripting (XSS) src/Form/Fields/SharpFormUploadField.php.	6.1	More Details
CVE-2025-61255	Bank Locker Management System by PHPGurukul is affected by a Cross-Site Scripting (XSS) vulnerability via the /search parameter, where unsanitized input allows arbitrary HTML and JavaScript injection, potentially resulting in information disclosure and user redirection.	6.1	More Details
CVE-2025-62592	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.12 and 7.2.2. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2025-62591	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are 7.1.12 and 7.2.2. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2025-61881	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.28, 21.3-21.19 and 23.4-23.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data. CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	5.9	More Details
CVE-2025-58153	Under undisclosed traffic conditions along with conditions beyond the attacker's control, hardware systems with a High-Speed Bridge (HSB) may experience a lockup of the HSB. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.9	More Details
CVE-2025-62171	ImageMagick is an open source software suite for displaying, converting, and editing raster image files. In ImageMagick versions prior to 7.1.2-7 and 6.9.13-32, an integer overflow vulnerability exists in the BMP decoder on 32-bit systems. The vulnerability occurs in coders/bmp.c when calculating the extent value by multiplying image columns by bits per pixel. On 32-bit systems with size_t of 4 bytes, a malicious BMP file with specific dimensions can cause this multiplication to overflow and wrap to zero. The overflow check added to address CVE-2025-57803 is placed after the overflow occurs, making it ineffective. A specially crafted 58-byte BMP file with width set to 536,870,912 and 32 bits per pixel can trigger this overflow, causing the bytes_per_line calculation to become zero. This vulnerability only affects 32-bit builds of ImageMagick where default resource limits for width, height, and area have been manually increased beyond their defaults. 64-bit systems with size_t of 8 bytes are not vulnerable, and systems using default ImageMagick resource limits are not vulnerable. The vulnerability is fixed in versions 7.1.2-7 and 6.9.13-32.	5.9	More Details
CVE-2025-53057	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u461, 8u461-perf, 11.0.28, 17.0.16, 21.0.8, 25; Oracle GraalVM for JDK: 17.0.16 and 21.0.8; Oracle GraalVM Enterprise Edition: 21.3.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	5.9	More Details

CVE-2025-62649	The Restaurant Brands International (RBI) assistant platform through 2025-09-06 relies on client-side authentication for submission of equipment orders.	5.8	More Details
CVE-2025-62642	The Restaurant Brands International (RBI) assistant platform through 2025-09-06 has an "Anyone Can Join This Party" signup API that does not verify user account creation, allowing a remote unauthenticated attacker to create a user account.	5.8	More Details
CVE-2025-53047	Vulnerability in the Portable Clusterware component of Oracle Database Server. Supported versions that are affected are 19.3-19.28, 21.3-21.19 and 23.4-23.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via Bonjour to compromise Portable Clusterware. While the vulnerability is in Portable Clusterware, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Portable Clusterware accessible data. CVSS 3.1 Base Score 5.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N).	5.8	More Details
CVE-2025-20360	Multiple Cisco products are affected by a vulnerability in the Snort 3 HTTP Decoder that could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to restart. This vulnerability is due to a lack of complete error checking when the MIME fields of the HTTP header are parsed. An attacker could exploit this vulnerability by sending crafted HTTP packets through an established connection to be parsed by Snort 3. A successful exploit could allow the attacker to cause a DoS condition when the Snort 3 Detection Engine unexpectedly restarts.	5.8	More Details
CVE-2025-60015	An out-of-bounds write vulnerability exists in F5OS-A and F5OS-C that could lead to memory corruption. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.7	More Details
CVE-2025-9955	An improper access control vulnerability exists in WSO2 Enterprise Integrator product due to insufficient permission restrictions on internal SOAP admin services related to system logs and user-store configuration. A low-privileged user can access log data and user-store configuration details that are not intended to be exposed at that privilege level. While no credentials or sensitive user information are exposed, this vulnerability may allow unauthorized visibility into internal operational details, which could aid in further exploitation or reconnaissance.	5.7	More Details
CVE-2025-60013	When a user attempts to initialize the rSeries FIPS module using a password with special shell metacharacters, the FIPS hardware security module (HSM) may fail to initialize. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.7	More Details
CVE-2025-54271	Creative Cloud Desktop versions 6.7.0.278 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to arbitrary file system write. A low-privileged attacker could exploit the timing between the check and use of a resource, potentially allowing unauthorized modifications to files. Exploitation of this issue does not require user interaction.	5.6	More Details
CVE-2025-11938	A vulnerability was found in ChurchCRM up to 5.18.0. This vulnerability affects unknown code of the file setup/routes/setup.php. Performing manipulation of the argument DB_PASSWORD/ROOT_PATH/URL results in deserialization. The attack may be initiated remotely. The attack's complexity is rated as high. It is stated that the exploitability is difficult. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-2025-60359	radare2 v5.9.8 and before contains a memory leak in the function r_bin_object_new.	5.5	More Details
CVE-2025-60360	radare2 v5.9.8 and before contains a memory leak in the function r2r_subprocess_init.	5.5	More Details
CVE-2025-62411	LibreNMS is a community-based GPL-licensed network monitoring system. LibreNMS <= 25.8.0 contains a Stored Cross-Site Scripting (XSS) vulnerability in the Alert Transports management functionality. When an administrator creates a new Alert Transport, the value of the Transport name field is stored and later rendered in the Transports column of the Alert Rules page without proper input validation or output encoding. This leads to arbitrary JavaScript execution in the admin’s browser. This vulnerability is fixed in 25.10.0.	5.5	More Details
CVE-2025-53070	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). The supported version that is affected is 11. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:N/I:N/A:H).	5.5	More Details
CVE-	Authorization Bypass Through User-Controlled Key vulnerability in VHS Electronic Software Ltd. Co. ACE		

2025-8884	Center allows Privilege Abuse, Exploitation of Trusted Identifiers.This issue affects ACE Center: from 3.10.100.1768 before 3.10.161.2255.	5.5	More Details
CVE-2025-53054	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.43, 8.4.0-8.4.6 and 9.0.0-9.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2025-53061	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 8.60, 8.61 and 8.62. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N).	5.5	More Details
CVE-2025-60358	radare2 v.5.9.8 and before contains a memory leak in the function _load_relocations.	5.5	More Details
CVE-2025-61554	A divide-by-zero in VirtIO network device emulation in BitVisor from commit 108df6 (2020-05-20) to commit 480907 (2025-07-06) allows local attackers to cause a denial of service (host hypervisor crash) via a crafted PCI configuration space access.	5.5	More Details
CVE-2024-42192	HCL Traveler for Microsoft Outlook (HTMO) is susceptible to a credential leakage which could allow an attacker to access other computers or applications.	5.5	More Details
CVE-2025-53053	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.0-8.0.43, 8.4.0-8.4.6 and 9.0.0-9.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2025-54270	Animate versions 23.0.13, 24.0.10 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive memory information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-54269	Animate versions 23.0.13, 24.0.10 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-43282	A double free issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.6, iOS 18.6 and iPadOS 18.6, watchOS 11.6, tvOS 18.6, visionOS 2.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7, iPadOS 17.7.9. An app may be able to cause unexpected system termination.	5.5	More Details
CVE-2025-53950	An Exposure of Private Personal Information ('Privacy Violation') vulnerability [CWE-359] in Fortinet FortiDLP Agent's Outlookproxy plugin for MacOS and Windows 11.5.1 and 11.4.2 through 11.4.6 and 11.3.2 through 11.3.4 and 11.2.0 through 11.2.3 and 11.1.1. through 11.1.2 and 11.0.1 and 10.5.1 and 10.4.0, and 10.3.1 may allow an authenticated administrator to collect current user's email information.	5.5	More Details
CVE-2025-9548	A potential null pointer dereference vulnerability was reported in the Lenovo Power Management Driver that could allow a local authenticated user to cause a Windows blue screen error.	5.5	More Details
CVE-2025-43313	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.7.7, macOS Sonoma 14.7.7, macOS Sequoia 15.6. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-54278	Bridge versions 14.1.8, 15.1.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-	The BlindMatrix e-Commerce WordPress plugin before 3.1 does not validate some shortcode attributes before		

2025-10406	using them to generate paths passed to include function/s, allowing any authenticated users, such as contributors, to perform LFI attacks.	5.5	More Details
CVE-2025-36002	IBM Sterling B2B Integrator 6.2.0.0 through 6.2.0.5, and 6.2.1.0 and IBM Sterling File Gateway 6.2.0.0 through 6.2.0.5, and 6.2.1.0 stores user credentials in configuration files which can be read by a local user.	5.5	More Details
CVE-2025-53063	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 8.60, 8.61 and 8.62. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2025-56700	Boolean SQL injection vulnerability in the web app of Base Digitale Group spa product Centrax Open PSIM version 6.1 allows a low level priviliged user that has access to the platform, to execute arbitrary SQL commands via the datafine parameter.	5.4	More Details
CVE-2025-41410	Mattermost versions 10.10.x <= 10.10.2, 10.5.x <= 10.5.10, 10.11.x <= 10.11.2 fail to validate email ownership during Slack import process which allows attackers to create verified user accounts with arbitrary email domains via malicious Slack import data to bypass email-based team access restrictions	5.4	More Details
CVE-2025-61761	Vulnerability in the PeopleSoft Enterprise FIN Maintenance Management product of Oracle PeopleSoft (component: Work Order Management). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Maintenance Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise FIN Maintenance Management accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise FIN Maintenance Management accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2025-62528	Taguette is an open source qualitative research tool. An issue has been discovered in Taguette versions prior to 1.5.0. It was possible for a project member to put JavaScript in name or description fields which would run on project load. This issue has been patched in version 1.5.0.	5.4	More Details
CVE-2025-11941	A vulnerability was detected in e107 CMS up to 2.3.3. This impacts an unknown function of the file /e107_admin/image.php?mode=main&action=avatar of the component Avatar Handler. Performing manipulation of the argument multiaction[] results in path traversal. It is possible to initiate the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2025-53065	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 8.60, 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2025-56699	SQL injection vulnerability in the cmd component of Base Digitale Group spa product Centrax Open PSIM version 6.1 allows an unauthenticated user to execute arbitrary SQL commands via the sender parameter.	5.4	More Details
CVE-2025-53034	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).	5.4	More Details
CVE-2025-41021	Stored Cross-Site Scripting (XSS) in Sergestec's Exito v8.0, consisting of a stored XSS due to a lack of proper validation of user input by sending a POST request using the 'obs' parameter in '/admin/index.php?action=product_update'. This vulnerability could allow a remote user to send a specially crafted query to an authenticated user and steal their cookie session details.	5.4	More Details

CVE-2025-56320	Enterprise Contract Management Portal v.22.4.0 is vulnerable to Stored Cross-Site Scripting (XSS) in its chat box component. This allows a remote attacker to execute arbitrary code	5.4	More Details
CVE-2025-62430	ClipBucket v5 is an open source video sharing platform. ClipBucket v5 through build 5.5.2 #145 allows stored cross-site scripting (XSS) in multiple video and photo metadata fields. For videos the Tags field and the Genre, Actors, Producer, Executive Producer, and Director fields in Movieinfos accept user supplied values without adequate sanitization. For photos the Photo Title and Photo Tags fields accept user supplied values without adequate sanitization. A regular user who can edit a video or photo can inject script (for example by supplying a value such as a closing delimiter followed by a script element). The injected script executes when any user, including an unauthenticated visitor or an administrator, views the affected video or photo page. Although cookies are set with the HttpOnly attribute and cannot be read directly, the injected script can issue fetch requests to endpoints such as admin_area pages and exfiltrate their contents or trigger unintended actions. Version 5.5.2 build #146 and later contain a fix. Update to build 5.5.2 #146 or later. No known workarounds exist.	5.4	More Details
CVE-2025-53048	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Rich Text Editor). Supported versions that are affected are 8.60, 8.61 and 8.62. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2025-11378	The ShortPixel Image Optimizer – Optimize Images, Convert WebP & AVIF plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'shortpixel_ajaxRequest' AJAX action in all versions up to, and including, 6.3.4. This makes it possible for authenticated attackers, with Contributor-level access and above, to export and import site options.	5.4	More Details
CVE-2025-26392	SolarWinds Observability Self-Hosted is susceptible to SQL injection vulnerability that may display sensitive data using a low-level account. This vulnerability requires authentication from a low-privilege account.	5.4	More Details
CVE-2025-55083	In NetX Duo version before 6.4.4, the component of Eclipse Foundation ThreadX, there was an incorrect bound check resulting it out by two out of bound read.	5.3	More Details
CVE-2025-0274	HCL BigFix Modern Client Management (MCM) 3.3 and earlier is affected by improper access control. Unauthorized users can access a small subset of endpoint actions, potentially allowing access to select internal functions.	5.3	More Details
CVE-2025-53951	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability [CWE-22] in Fortinet FortiDLP Agent's Outlookproxy plugin for Windows 11.5.1 and 11.4.2 through 11.4.6 and 11.3.2 through 11.3.4 and 11.2.0 through 11.2.3 and 11.1.1 through 11.1.2 and 11.0.1 and 10.5.1 and 10.4.0, and 10.3.1 may allow an authenticated attacker to escalate their privilege to LocalService via sending a crafted request to a local listening port.	5.3	More Details
CVE-2025-11701	The Zip Attachments plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check as well as missing post status validation in the za_create_zip_callback function in all versions up to, and including, 1.6. This makes it possible for unauthenticated attackers to download attachments from private and password-protected posts.	5.3	More Details
CVE-2025-0275	HCL BigFix Mobile 3.3 and earlier is affected by improper access control. Unauthorized users can access a small subset of endpoint actions, potentially allowing access to select internal functions.	5.3	More Details
CVE-2025-58133	Authentication bypass in some Zoom Rooms Clients before version 6.5.1 may allow an unauthenticated user to conduct a disclosure of information via network access.	5.3	More Details
CVE-2025-11256	The Kognetiks Chatbot plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several functions in all versions up to, and including, 2.3.5. This makes it possible for unauthenticated attackers to upload limited safe files and erase conversations.	5.3	More Details
CVE-2025-10648	The YourMembership Single Sign On – YM SSO Login plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'moym_display_test_attributes' function in all versions up to, and including, 1.1.7. This makes it possible for unauthenticated attackers to read the profile data of the latest SSO login.	5.3	More Details
CVE-			

2025-10699	A vulnerability was reported in the Lenovo LeCloud client application that, under certain conditions, could allow information disclosure.	5.3	More Details
CVE-2025-10849	The Felan Framework plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'process_plugin_actions' function called via an AJAX action in versions up to, and including, 1.1.4. This makes it possible for unauthenticated attackers to activate or deactivate arbitrary plugins.	5.3	More Details
CVE-2025-55084	In NetX Duo version before 6.4.4, the component of Eclipse Foundation ThreadX, there was an incorrect bound check in_nx_secure_tls_proc_clienthello_supported_versions_extension() in the extension version field.	5.3	More Details
CVE-2025-10486	The Content Writer plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.6.8 through publicly exposed log files. This makes it possible for unauthenticated attackers to view potentially sensitive information contained in the exposed log files.	5.3	More Details
CVE-2025-11692	The Zip Attachments plugin for WordPress is vulnerable to unauthorized loss of data due to a missing authorization and capability checks on the download.php file in all versions up to, and including, 1.6. This makes it possible for unauthenticated attackers to delete arbitrary files from the current wp_upload_dir directory.	5.3	More Details
CVE-2025-11728	The Oceanpayment CreditCard Gateway plugin for WordPress is vulnerable to unauthenticated and unauthorized modification of data due to missing authentication and capability checks on the 'return_payment' and 'notice_payment' functions in all versions up to, and including, 6.0. This makes it possible for unauthenticated attackers to update WooCommerce orders to 'failed' status, and update transaction IDs.	5.3	More Details
CVE-2025-58474	When BIG-IP Advanced WAF is configured on a virtual server with Server-Side Request Forgery (SSRF) protection or when an NGINX server is configured with App Protect Bot Defense, undisclosed requests can disrupt new client requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.3	More Details
CVE-2025-62672	rplay through 3.3.2 allows attackers to cause a denial of service (SIGSEGV and daemon crash) or possibly have unspecified other impact. This occurs in memcpy in the RPLAY_DATA case in rplay_unpack in librplay/rplay.c, potentially reachable via packet data with no authentication.	5.3	More Details
CVE-2025-59268	On the BIG-IP system, undisclosed endpoints that contain static non-sensitive information are accessible to an unauthenticated remote attacker through the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.3	More Details
CVE-2025-11979	An authorized user may crash the MongoDB server by causing buffer over-read. This can be done by issuing a DDL operation while queries are being issued, under some conditions. This issue affects MongoDB Server v7.0 versions prior to 7.0.25, MongoDB Server v8.0 versions prior to 8.0.15, and MongoDB Server version 8.2.0.	5.3	More Details
CVE-2025-55082	In NetX Duo version before 6.4.4, the component of Eclipse Foundation ThreadX, there was a potential out of bound read in _nx_secure_tls_process_clienthello() because of a missing validation of PSK length provided in the user message.	5.3	More Details
CVE-2025-11738	The Media Library Assistant plugin for WordPress is vulnerable to limited file reading in all versions up to, and including, 3.29 via the mla-stream-image.php file. This makes it possible for unauthenticated attackers to read the contents of arbitrary ai/eps/pdf/ps files on the server, which can contain sensitive information.	5.3	More Details
CVE-2025-11852	A vulnerability was found in Apeman ID71 218.53.203.117. The impacted element is an unknown function of the file /onvif/device_service of the component ONVIF Service. Performing manipulation results in missing authentication. The attack is possible to be carried out 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 way.	5.3	More Details
CVE-2025-59438	Mbed TLS through 3.6.4 has an Observable Timing Discrepancy.	5.3	More Details
CVE-2025-11741	The WPC Smart Quick View for WooCommerce plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 4.2.5 via the 'woosq_quickview' AJAX endpoint due to insufficient restrictions on which posts can be included. This makes it possible for unauthenticated attackers to extract data from password protected, private, or draft products that they should not have access to.	5.3	More Details
CVE-2025-52079	The administrator password setting of the D-Link DIR-820L 1.06B02 is has Improper Access Control and is vulnerable to Unverified Password Change via crafted POST request to /get_set.ccp.	5.3	More Details
CVE-	The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to Cache Poisoning in all		

2025-11703	versions up to, and including, 9.0.48. This is due to the plugin not serving cached data from server-side responses and instead relying on user-input. This makes it possible for unauthenticated attackers to poison the cache location for location search results.	5.3	More Details
CVE-2020-36855	A security vulnerability has been detected in DCMTK up to 3.6.5. The affected element is the function parseQuota of the component dcmqrscp. The manipulation of the argument StorageQuota leads to stack-based buffer overflow. Local access is required to approach this attack. The exploit has been disclosed publicly and may be used. Upgrading to version 3.6.6 is sufficient to fix this issue. The identifier of the patch is 0fef9f02e. It is recommended to upgrade the affected component.	5.3	More Details
CVE-2025-61789	Icinga DB Web provides a graphical interface for Icinga monitoring. Before 1.1.4 and 1.2.3, an authorized user with access to Icinga DB Web, can use a custom variable in a filter that is either protected by icingadb/protect/variables or hidden by icingadb/denylist/variables, to guess values assigned to it. Versions 1.1.4 and 1.2.3 respond with an error if such a custom variable is used.	5.3	More Details
CVE-2025-61764	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2025-10750	The PowerBI Embed Reports plugin for WordPress is vulnerable to Sensitive Information Disclosure in all versions up to, and including, 1.2.0. This is due to missing capability checks and authentication verification on the 'testUser' endpoint accessible via the mo_epbr_admin_observer() function hooked on 'init'. This makes it possible for unauthenticated attackers to access sensitive Azure AD user information including personal identifiable information (PII) such as displayName, mail, phones, department, or detailed OAuth error data including Azure AD Application/Client IDs, error codes, trace IDs, and correlation IDs.	5.3	More Details
CVE-2025-10186	The WhyDonate – FREE Donate button – Crowdfunding – Fundraising plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the remove_row function in all versions up to, and including, 4.0.14. This makes it possible for unauthenticated attackers to delete rows from the wp_wdplugin_style table.	5.3	More Details
CVE-2025-7473	Zohocorp ManageEngine EndPoint Central versions 11.4.2516.1 and prior are vulnerable to XML Injection.	5.2	More Details
CVE-2025-56802	The Reolink desktop application uses a hard-coded and predictable AES encryption key to encrypt user configuration files allowing attackers with local access to decrypt sensitive application data stored in %APPDATA%. A different vulnerability than CVE-2025-56802.	5.1	More Details
CVE-2025-56800	Reolink desktop application 8.18.12 contains a vulnerability in its local authentication mechanism. The application implements lock screen password logic entirely on the client side using JavaScript within an Electron resource file. Because the password is stored and returned via a modifiable JavaScript property(a.settingsManager.lockScreenPassword), an attacker can patch the return value to bypass authentication.	5.1	More Details
CVE-2025-60855	Reolink Video Doorbell WiFi DB_566128M5MP_W performs insufficient validation of firmware update signatures. This allows attackers to load malicious firmware images, resulting in arbitrary code execution with root privileges. NOTE: this is disputed by the Supplier because the integrity of updates is instead assured via a "private encryption algorithm" and other "tamper-proof verification."	5.1	More Details
CVE-2025-62416	Bagisto is an open source laravel eCommerce platform. Bagisto v2.3.7 is vulnerable to Server-Side Template Injection (SSTI) due to unsanitized user input being processed by the server-side templating engine when rendering product descriptions. This allows an attacker with product creation privileges to inject arbitrary template expressions that are evaluated by the backend — potentially leading to Remote Code Execution (RCE) on the server. This vulnerability is fixed in 2.3.8.	5.1	More Details
CVE-2025-56801	The Reolink Desktop Application 8.18.12 contains hardcoded credentials as the Initialization Vector (IV) in its AES-CFB encryption implementation allowing attackers with access to the application environment to reliably decrypt encrypted configuration data.	5.1	More Details
CVE-2025-62644	The Restaurant Brands International (RBI) assistant platform through 2025-09-06 has a Global Store Directory that shares personal information among authenticated users.	5.0	More Details
CVE-2025-62646	The Restaurant Brands International (RBI) assistant platform through 2025-09-06 allows remote attackers to review the stored audio of conversations between associates and Drive Thru customers.	5.0	More Details
CVE-	The Restaurant Brands International (RBI) assistant platform through 2025-09-06 provides the functionality of		More

2025-62647	returning a JWT that can be used to call an API to return a signed AWS upload URL, for any store's path.	5.0	Details
CVE-2025-11536	The Element Pack Addons for Elementor plugin for WordPress is vulnerable to Blind Server-Side Request Forgery in all versions up to, and including, 8.2.5 via the wp_ajax_import_elementor_template action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	5.0	More Details
CVE-2025-62763	Zimbra Collaboration (ZCS) before 10.1.12 allows SSRF because of the configuration of the chat proxy.	5.0	More Details
CVE-2025-53045	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.43, 8.4.0-8.4.6 and 9.0.0-9.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-10045	The onOffice for WP-Websites plugin for WordPress is vulnerable to SQL Injection via the 'order' parameter in all versions up to, and including, 5.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Editor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2025-20329	A vulnerability in the logging component of Cisco TelePresence Collaboration Endpoint (CE) and Cisco RoomOS Software could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system. To exploit this vulnerability, the attacker must have valid administrative credentials. This vulnerability exists because certain unencrypted credentials are stored when SIP media component logging is enabled. An attacker could exploit this vulnerability by accessing the audit logs on an affected system and obtaining credentials to which they may not normally have access. A successful exploit could allow the attacker to use those credentials to access confidential information, some of which may contain personally identifiable information (PII). Note: To access the logs that are stored in the Webex Cloud or stored on the device itself, an attacker must have valid administrative credentials.	4.9	More Details
CVE-2025-10187	The GSpeech TTS – WordPress Text To Speech Plugin plugin for WordPress is vulnerable to SQL Injection via the 'field' parameter in all versions up to, and including, 3.17.13 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2025-53046	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Analytics). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-62477	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Remote Replication). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-53059	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: OpenSearch Dashboards). Supported versions that are affected are 8.60, 8.61 and 8.62. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.9	More Details
CVE-2025-53044	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.43, 8.4.0-8.4.6 and 9.0.0-9.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.43, 8.4.0-8.4.6 and 9.0.0-9.4.0. Easily exploitable vulnerability allows high		

2025-53062	privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-62478	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Object Store). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-62476	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Remote Replication). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-53042	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.43, 8.4.0-8.4.6 and 9.0.0-9.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-62475	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-53067	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 9.0.0-9.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-53069	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.0-8.0.43, 8.4.0-8.4.6 and 9.0.0-9.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-62289	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Filesystems). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-62288	Vulnerability in the Oracle Health Sciences Data Management Workbench product of Oracle Health Sciences Applications (component: Logger). Supported versions that are affected are 3.4.0.1.3 and 3.4.1.0.10. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Health Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences Data Management Workbench accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.9	More Details
CVE-2025-10310	The Rich Snippet Site Report plugin for WordPress is vulnerable to SQL Injection via the 'last' parameter in all versions up to, and including, 2.0.0105 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This can also be exploited via CSRF.	4.9	More Details
CVE-2025-54755	A directory traversal vulnerability exists in TMUI that allows an authenticated attacker to access files which are not limited to the intended files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.9	More Details

CVE-2025-50074	Vulnerability in the Oracle Financial Services Revenue Management and Billing product of Oracle Financial Services Applications (component: Security Management System). Supported versions that are affected are 2.9.0.0.0-7.2.0.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Financial Services Revenue Management and Billing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financial Services Revenue Management and Billing accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.9	More Details
CVE-2025-53040	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.43, 8.4.0-8.4.6 and 9.0.0-9.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2025-43280	The issue was resolved by not loading remote images This issue is fixed in iOS 18.6 and iPadOS 18.6. Forwarding an email could display remote images in Mail in Lockdown Mode.	4.7	More Details
CVE-2025-11944	A vulnerability was determined in givanz Vvveb up to 1.0.7.3. This affects the function Import of the file admin/controller/tools/import.php of the component Raw SQL Handler. This manipulation causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. Patch name: 52204b4a106b2fb02d16eee06a88a1f2697f9b35. It is recommended to apply a patch to fix this issue.	4.7	More Details
CVE-2025-11939	A vulnerability was determined in ChurchCRM up to 5.18.0. This issue affects some unknown processing of the file src/ChurchCRM/Backup/RestoreJob.php of the component Backup Restore Handler. Executing manipulation of the argument restoreFile can lead to path traversal. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-11947	A weakness has been identified in bftpd up to 6.2. Impacted is the function expand_groups of the file options.c of the component Configuration File Handler. Executing manipulation can lead to heap-based buffer overflow. It is possible to launch the attack on the local host. Attacks of this nature are highly complex. The exploitability is considered difficult. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	4.5	More Details
CVE-2025-11926	The Related Posts Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-11568	A data corruption vulnerability has been identified in the luksmeta utility when used with the LUKS1 disk encryption format. An attacker with the necessary permissions can exploit this flaw by writing a large amount of metadata to an encrypted device. The utility fails to correctly validate the available space, causing the metadata to overwrite and corrupt the user's encrypted data. This action leads to a permanent loss of the stored information. Devices using the LUKS formats other than LUKS1 are not affected by this issue.	4.4	More Details
CVE-2025-10056	The Task Scheduler plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.6.3 via the “Check Website” task. This makes it possible for authenticated attackers, with Administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	4.4	More Details
CVE-2025-46752	A insertion of sensitive information into log file in Fortinet FortiDLP 12.0.0 through 12.0.5, 11.5.1, 11.4.6, 11.4.5 allows attacker to information disclosure via re-using the enrollment code.	4.4	More Details
CVE-2025-62605	Mastodon is a free, open-source social network server based on ActivityPub. In Mastodon version 4.4, support for verifiable quote posts with quote controls was added, but it is possible for an attacker to bypass these controls in Mastodon versions prior to 4.4.8 and 4.5.0-beta.2. Mastodon internally treats reblogs as statuses. Since they were not special-treated, an attacker could reblog any post, then quote their reblog, technically quoting themselves, but having the quote feature a preview of the post they did not get authorization for with all of the affordances that would be otherwise denied by the quote controls. This issue has been patched in versions 4.4.8 and 4.5.0-beta.2.	4.3	More Details
CVE-2025-41254	STOMP over WebSocket applications may be vulnerable to a security bypass that allows an attacker to send unauthorized messages. Affected Spring Products and VersionsSpring Framework: * 6.2.0 - 6.2.11 * 6.1.0 - 6.1.23 * 6.0.x - 6.0.29 * 5.3.0 - 5.3.45 * Older, unsupported versions are also affected. MitigationUsers of affected versions should upgrade to the corresponding fixed version. Affected version(s)Fix versionAvailability6.2.x6.2.12OSS6.1.x6.1.24 Commercial https://enterprise.spring.io/ 6.0.xN/A Out of support https://spring.io/projects/spring-framework#support 5.3.x5.3.46 Commercial https://enterprise.spring.io/ No further mitigation steps are necessary. CreditThis vulnerability was discovered and responsibly reported by	4.3	More Details

	Jannis Kaiser.		
CVE-2025-48025	In Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1280, 1330, 1380, 1480, 1580, W920, W930, and W1000, there is an improper access control vulnerability related to a log file.	4.3	More Details
CVE-2025-11510	The FileBird – WordPress Media Library Folders & File Manager plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the /filebird/v1/fb-wipe-clear-all-data function in all versions up to, and including, 6.4.9. This makes it possible for authenticated attackers, with author-level access and above, to reset all of the plugin's configuration data.	4.3	More Details
CVE-2025-9640	A flaw was found in Samba, in the vfs_streams_xattr module, where uninitialized heap memory could be written into alternate data streams. This allows an authenticated user to read residual memory content that may include sensitive data, resulting in an information disclosure vulnerability.	4.3	More Details
CVE-2025-61750	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Query). Supported versions that are affected are 8.61 and 8.62. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2025-11519	The Optimole – Optimize Images | Convert WebP & AVIF | CDN & Lazy Load | Image Optimization plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.1.0 via the /wp-json/optml/v1/move_image REST API endpoint due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Author-level access and above, to offload media that doesn't belong to them.	4.3	More Details
CVE-2025-60511	Moodle OpenAI Chat Block plugin 3.0.1 (2025021700) suffers from an Insecure Direct Object Reference (IDOR) vulnerability due to insufficient validation of the blockId parameter in /blocks/openai_chat/api/completion.php. An authenticated student can impersonate another user's block (e.g., administrator) and send queries that are executed with that block's configuration. This can expose administrator-only Source of Truth entries, alter model behavior, and potentially misuse API resources.	4.3	More Details
CVE-2025-61885	Vulnerability in the Oracle Life Sciences InForm product of Oracle Health Sciences Applications (component: Web Server). The supported version that is affected is 7.0.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Life Sciences InForm. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Life Sciences InForm accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2025-10303	The Library Management System plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the owt7_library_management_ajax_handler() function in all versions up to, and including, 3.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update and manipulate several of the plugin's settings and features.	4.3	More Details
CVE-2025-10312	The Theme Importer plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing nonce validation when processing form submissions in the theme-importer.php file. This makes it possible for unauthenticated attackers to trigger arbitrary file downloads and potentially execute malicious operations via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-10700	The Ally – Web Accessibility & Usability plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.8.0. This is due to missing or incorrect nonce validation on the enable_unfiltered_files_upload function. This makes it possible for unauthenticated attackers to enable unfiltered file upload and add svg files to the upload list via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-10301	The FunKItools 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 or incorrect nonce validation on the saveFields() function. This makes it possible for unauthenticated attackers to update plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-53071	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Upload Attachments). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	4.3	More Details
CVE-2025-	The Quick Featured Images plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 13.7.2 via the qfi_set_thumbnail and qfi_delete_thumbnail AJAX actions due to	4.3	More

11176	missing validation on a user controlled key. This makes it possible for authenticated attackers, with Author-level access and above, to change or remove featured images of other user's posts.		Details
CVE-2025-11895	The Binary MLM Plan plugin for WordPress is vulnerable to insecure direct object reference in versions up to, and including, 3.0. This is due to the bmp_user_payout_detail_of_current_user() function selecting payout records solely by id without verifying ownership. This makes it possible for authenticated attackers with the bmp_user role (often subscribers) to view other members' payout summaries via direct requests to the /bmp-account-detail/ endpoint with a crafted payout-id parameter granted they can access the shortcode output.	4.3	More Details
CVE-2025-11742	The WPC Smart Wishlist for WooCommerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'wishlist_quickview' AJAX action in all versions up to, and including, 5.0.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to view other user's wishlist data and information.	4.3	More Details
CVE-2025-11914	A vulnerability was found in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. Affected by this issue is the function Download of the file /DeviceFileReport.do?Action=Download. Performing manipulation of the argument FilePath results in path traversal. The attack may be initiated 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 way.	4.3	More Details
CVE-2025-53064	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Personalization). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	4.3	More Details
CVE-2025-10300	The TopBar plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.0. This is due to missing or incorrect nonce validation on the fme_nb_topbar_save_settings() function. This makes it possible for unauthenticated attackers to update the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-11913	A vulnerability has been found in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. Affected by this vulnerability is the function Download of the file /Service.do?Action=Download. Such manipulation of the argument Path leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-41443	Mattermost versions 10.5.x <= 10.5.10, 10.11.x <= 10.11.2 fail to properly validate guest user permissions when accessing channel information which allows guest users to discover active public channels and their metadata via the `/api/v4/teams/{team_id}/channels/ids` endpoint	4.3	More Details
CVE-2025-62595	Koa is expressive middleware for Node.js using ES2017 async functions. In versions 2.16.2 to before 2.16.3 and 3.0.1 to before 3.0.3, a bypass to CVE-2025-8129 was discovered in the Koa.js framework affecting its back redirect functionality. In certain circumstances, an attacker can manipulate the Referer header to force a user’s browser to navigate to an external, potentially malicious website. This occurs because the implementation incorrectly treats some specially crafted URLs as safe relative paths. Exploiting this vulnerability could allow attackers to perform phishing, social engineering, or other redirect-based attacks on users of affected applications. This issue has been patched in version 3.0.3.	4.3	More Details
CVE-2025-11196	The External Login plugin for WordPress is vulnerable to sensitive information exposure in all versions up to, and including, 1.11.2 due to the 'exlog_test_connection' AJAX action lacking capability checks or nonce validation. This makes it possible for authenticated attackers, with subscriber-level access and above, to query the configured external database and retrieve truncated usernames, email addresses, and password hashes via the diagnostic test results view.	4.3	More Details
CVE-2025-58132	Command injection in some Zoom Clients for Windows may allow an authenticated user to conduct a disclosure of information via network access.	4.1	More Details
CVE-2025-61923	PrestaShop Checkout is the PrestaShop official payment module in partnership with PayPal. In versions prior to 4.4.1 and 5.0.5, the backoffice is missing validation on input resulting in a directory traversal and arbitrary file disclosure. The vulnerability is fixed in versions 4.4.1 and 5.0.5. No known workarounds exist.	4.1	More Details
CVE-2025-53860	A vulnerability exists in F5OS-A software that allows a highly privileged authenticated attacker to access sensitive FIPS hardware security module (HSM) information on F5 rSeries systems. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.1	More Details
CVE-2025-57839	Photo module is affected by information leak vulnerability, successful exploitation of this vulnerability may affect service confidentiality.	4.0	More Details
CVE-			

2024-31573	XMLUnit for Java before 2.10.0, in the default configuration, might allow code execution via an untrusted stylesheet (used for an XSLT transformation), because XSLT extension functions are enabled.	4.0	More Details
CVE-2025-57838	Some Honor products are affected by information leak vulnerability, successful exploitation of this vulnerability may affect service confidentiality.	4.0	More Details
CVE-2025-62412	LibreNMS is a community-based GPL-licensed network monitoring system. The alert rule name in the Alerts > Alert Rules page is not properly sanitized, and can be used to inject HTML code. This vulnerability is fixed in 25.10.0.	3.8	More Details
CVE-2025-61924	PrestaShop Checkout is the PrestaShop official payment module in partnership with PayPal. In versions prior to 4.4.1 and 5.0.5, the Target PayPal merchant account hijacking from backoffice due to wrong usage of the PHP array_search(). The vulnerability is fixed in versions 4.4.1 and 5.0.5. No known workarounds exist.	3.8	More Details
CVE-2025-58424	On BIG-IP systems, undisclosed traffic can cause data corruption and unauthorized data modification in protocols which do not have message integrity protection. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	3.7	More Details
CVE-2025-61755	Vulnerability in the Oracle GraalVM for JDK product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.16 and 21.0.8. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	3.7	More Details
CVE-2025-61748	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 21.0.8 and 25; Oracle GraalVM for JDK: 21.0.8; Oracle GraalVM Enterprise Edition: 21.3.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	3.7	More Details
CVE-2025-11946	A security flaw has been discovered in LogicalDOC Community Edition up to 9.2.1. This issue affects some unknown processing of the file /frontend.jsp of the component Add Contact Page. Performing manipulation of the argument First Name/Last Name/Company/Address/Phone/Mobile results in cross site scripting. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-11945	A vulnerability was identified in toeverything AFFiNE up to 0.24.1. This vulnerability affects unknown code of the component Avatar Upload Image Endpoint. Such manipulation leads to cross site scripting. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-11851	A vulnerability has been found in Apeman ID71 EN75.8.53.20. The affected element is an unknown function of the file /set_alias.cgi. Such manipulation of the argument alias 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.	3.5	More Details
CVE-2025-62643	The Restaurant Brands International (RBI) assistant platform through 2025-09-06 transmits passwords of user accounts in cleartext e-mail messages.	3.4	More Details
CVE-2025-60361	radare2 v5.9.8 and before contains a memory leak in the function bochs_open.	3.3	More Details
CVE-2025-11839	A security flaw has been discovered in GNU Binutils 2.45. Impacted is the function tg_tag_type of the file prdbg.c. Performing manipulation results in unchecked return value. The attack needs to be approached locally. The exploit has been released to the public and may be exploited.	3.3	More Details
CVE-2025-5496	ZohoCorp ManageEngine Endpoint Central versions earlier than 11.4.2508.14, 11.4.2516.06, and 11.4.2518.01 are affected by an arbitrary file deletion vulnerability in the agent setup component.	3.3	More Details
	A vulnerability was detected in DCMTK up to 3.6.7. The impacted element is the function		

CVE-2022-4981	DcmQueryRetrieveConfig::readPeerList of the file /dcmqrcnf.cc of the component dcmqrscp. The manipulation results in null pointer dereference. The attack needs to be approached locally. The exploit is now public and may be used. Upgrading to version 3.6.8 is sufficient to resolve this issue. The patch is identified as 957fb31e5. Upgrading the affected component is advised.	3.3	More Details
CVE-2025-11840	A weakness has been identified in GNU Binutils 2.45. The affected element is the function vfinfo of the file ldmisc.c. Executing manipulation can lead to out-of-bounds read. The attack can only be executed locally. The exploit has been made available to the public and could be exploited. This patch is called 16357. It is best practice to apply a patch to resolve this issue.	3.3	More Details
CVE-2025-6026	An improper certificate validation vulnerability was reported in the Lenovo Universal Device Client (UDC) that could allow a user capable of intercepting network traffic to obtain application metadata, including device information, geolocation, and telemetry data.	3.1	More Details
CVE-2025-62379	Reflex is a library to build full-stack web apps in pure Python. In versions 0.5.4 through 0.8.14, the /auth-codespace endpoint automatically assigns the redirect_to query parameter value directly to client-side links without any validation and triggers automatic clicks when the page loads in a GitHub Codespaces environment. This allows attackers to redirect users to arbitrary external URLs. The vulnerable route is only registered when a Codespaces environment is detected, and the detection is controlled by environment variables. The same behavior can be activated in production if the GITHUB_CODESPACES_PORT_FORWARDING_DOMAIN environment variable is set. The vulnerability occurs because the code assigns the redirect_to query parameter directly to a.href without any validation and immediately triggers a click (automatic navigation), allowing users to be sent to arbitrary external domains. The execution condition is based on the presence of a sessionStorage flag, meaning it triggers immediately on first visits or in incognito/private browsing windows, with no server-side origin/scheme whitelist or internal path enforcement defenses in place. This issue has been patched in version 0.8.15. As a workaround, users can ensure that GITHUB_CODESPACES_PORT_FORWARDING_DOMAIN is not set in a production environment.	3.1	More Details
CVE-2025-10545	Mattermost versions 10.5.x <= 10.5.10, 10.11.x <= 10.11.2 fail to properly validate guest user permissions when adding channel members which allows guest users to add any team members to their private channels via the `/api/v4/channels/{channel_id}/members` endpoint	3.1	More Details
CVE-2025-54499	Mattermost versions 10.5.x <= 10.5.10, 10.11.x <= 10.11.2 fail to use constant-time comparison for sensitive string comparisons which allows attackers to exploit timing oracles to perform byte-by-byte brute force attacks via response time analysis on Cloud API keys and OAuth client secrets	3.1	More Details
CVE-2025-62505	LobeChat is an open source chat application platform. The web-crawler package in LobeChat version 1.136.1 allows server-side request forgery (SSRF) in the tools.search.crawlPages tRPC endpoint. A client can supply an arbitrary urls array together with impls containing the value naive. The service passes the user URLs to Crawler.crawl and the naive implementation performs a server-side fetch of each supplied URL without validating or restricting internal network addresses (such as localhost, 127.0.0.1, private IP ranges, or cloud instance metadata endpoints). This allows an attacker with a valid user token (or in development mode using a bypass header) to make the server disclose responses from internal HTTP services, potentially exposing internal API data or cloud metadata credentials. Version 1.136.2 fixes the issue. Update to version 1.136.2. No known workarounds exist.	3.0	More Details
CVE-2025-57837	Tileservice module is affected by information leak vulnerability, successful exploitation of this vulnerability may affect service confidentiality.	2.9	More Details
CVE-2025-2529	Applications using affected versions of Ehcache 3.x can experience degraded cache-write performance if the application using Ehcache utilizes keys sourced from (malicious) external parties in an unfiltered/unsalted way.	2.9	More Details
CVE-2025-61749	Vulnerability in the Unified Audit component of Oracle Database Server. Supported versions that are affected are 23.4-23.9. Easily exploitable vulnerability allows high privileged attacker having DBA privilege with network access via Oracle Net to compromise Unified Audit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Unified Audit accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2.7	More Details
CVE-2025-62479	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Block Storage). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.7	More Details
CVE-2025-53051	Vulnerability in the RDBMS Functional Index component of Oracle Database Server. Supported versions that are affected are 23.4-23.9. Easily exploitable vulnerability allows high privileged attacker having SYSDBA privilege with network access via Oracle Net to compromise RDBMS Functional Index. Successful attacks of this vulnerability can result in unauthorized read access to a subset of RDBMS Functional Index accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector:	2.7	More Details

	(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).		
CVE-2025-62480	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Naming Subsystem). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.7	More Details
CVE-2025-56746	Creativeitem Academy LMS up to and including 5.13 does not regenerate session IDs upon successful authentication, enabling session fixation attacks where attackers can hijack user sessions by predetermining session identifiers.	2.2	More Details
CVE-2025-39995	In the Linux kernel, the following vulnerability has been resolved: media: i2c: tc358743: Fix use-after-free bugs caused by orphan timer in probe The state->timer is a cyclic timer that schedules work_i2c_poll and delayed_work_enable_hotplug, while rearming itself. Using timer_delete() fails to guarantee the timer isn't still running when destroyed, similarly cancel_delayed_work() cannot ensure delayed_work_enable_hotplug has terminated if already executing. During probe failure after timer initialization, these may continue running as orphans and reference the already-freed tc358743_state object through tc358743_irq_poll_timer. The following is the trace captured by KASAN. BUG: KASAN: slab-use-after-free in __run_timer_base.part.0+0x7d7/0x8c0 Write of size 8 at addr ffff88800ded83c8 by task swapper/1/0 ... Call Trace: <IRQ> dump_stack_lvl+0x55/0x70 print_report+0xcf/0x610 ? __pfx_sched_balance_find_src_group+0x10/0x10 ? __run_timer_base.part.0+0x7d7/0x8c0 kasan_report+0xb8/0xf0 ? __run_timer_base.part.0+0x7d7/0x8c0 __run_timer_base.part.0+0x7d7/0x8c0 ? rcu_sched_clock_irq+0xb06/0x27d0 ? __pfx___run_timer_base.part.0+0x10/0x10 ? try_to_wake_up+0xb15/0x1960 ? tmigr_update_events+0x280/0x740 ? _raw_spin_lock_irq+0x80/0xe0 ? __pfx__raw_spin_lock_irq+0x10/0x10 tmigr_handle_remote_up+0x603/0x7e0 ? __pfx_tmigr_handle_remote_up+0x10/0x10 ? sched_balance_trigger+0x98/0x9f0 ? sched_tick+0x221/0x5a0 ? _raw_spin_lock_irq+0x80/0xe0 ? __pfx__raw_spin_lock_irq+0x10/0x10 ? tick_nohz_handler+0x339/0x440 ? __pfx_tmigr_handle_remote_up+0x10/0x10 __walk_groups.isra.0+0x42/0x150 tmigr_handle_remote+0x1f4/0x2e0 ? __pfx_tmigr_handle_remote+0x10/0x10 ? ktime_get+0x60/0x140 ? lapic_next_event+0x11/0x20 ? clockevents_program_event+0x1d4/0x2a0 ? hrtimer_interrupt+0x322/0x780 handle_softirqs+0x16a/0x550 irq_exit_rcu+0xaf/0xe0 sysvec_apic_timer_interrupt+0x70/0x80 </IRQ> ... Allocated by task 141: kasan_save_stack+0x24/0x50 kasan_save_track+0x14/0x30 __kasan_kmalloc+0x7f/0x90 __kmalloc_node_track_caller_noprof+0x198/0x430 devm_kmalloc+0x7b/0x1e0 tc358743_probe+0xb7/0x610 i2c_device_probe+0x51d/0x880 really_probe+0x1ca/0x5c0 __driver_probe_device+0x248/0x310 driver_probe_device+0x44/0x120 __device_attach_driver+0x174/0x220 bus_for_each_drv+0x100/0x190 __device_attach+0x206/0x370 bus_probe_device+0x123/0x170 device_add+0xd25/0x1470 i2c_new_client_device+0x7a0/0xcd0 do_one_initcall+0x89/0x300 do_init_module+0x29d/0x7f0 load_module+0x4f48/0x69e0 init_module_from_file+0xe4/0x150 idempotent_init_module+0x320/0x670 __x64_sys_finit_module+0xbd/0x120 do_syscall_64+0xac/0x280 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 141: kasan_save_stack+0x24/0x50 kasan_save_track+0x14/0x30 kasan_save_free_info+0x3a/0x60 __kasan_slab_free+0x3f/0x50 kfree+0x137/0x370 release_nodes+0xa4/0x100 devres_release_group+0x1b2/0x380 i2c_device_probe+0x694/0x880 really_probe+0x1ca/0x5c0 __driver_probe_device+0x248/0x310 driver_probe_device+0x44/0x120 __device_attach_driver+0x174/0x220 bus_for_each_drv+0x100/0x190 __device_attach+0x206/0x370 bus_probe_device+0x123/0x170 device_add+0xd25/0x1470 i2c_new_client_device+0x7a0/0xcd0 do_one_initcall+0x89/0x300 do_init_module+0x29d/0x7f0 load_module+0x4f48/0x69e0 init_module_from_file+0xe4/0x150 idempotent_init_module+0x320/0x670 __x64_sys_finit_module+0xbd/0x120 do_syscall_64+0xac/0x280 entry_SYSCALL_64_after_hwframe+0x77/0x7f ... Replace timer_delete() with timer_delete_sync() and cancel_delayed_work() with cancel_delayed_work_sync() to ensure proper termination of timer and work items before resource cleanup. This bug was initially identified through static analysis. For reproduction and testing, I created a functional emulation of the tc358743 device via a kernel module and introduced faults through the debugfs interface.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: media: b2c2: Fix use-after-free causing by irq_check_work in flexcop_pci_remove The original code uses cancel_delayed_work() in flexcop_pci_remove(), which does not guarantee that the delayed work item irq_check_work has fully completed if it was already running. This leads to use-after-free scenarios where flexcop_pci_remove() may free the flexcop_device while irq_check_work is still active and attempts to dereference the device. A typical race condition is illustrated below: CPU 0 (remove) | CPU 1 (delayed work callback) flexcop_pci_remove() | flexcop_pci_irq_check_work() cancel_delayed_work() | flexcop_device_kfree(fc_pci->fc_dev) | | fc = fc_pci->fc_dev; // UAF This is confirmed by a KASAN report: == BUG: KASAN: slab-use-after-free in __run_timer_base.part.0+0x7d7/0x8c0 Write of size 8 at addr ffff8880093aa8c8 by task bash/135 ... Call Trace: <IRQ> dump_stack_lvl+0x55/0x70 print_report+0xcf/0x610 ? __run_timer_base.part.0+0x7d7/0x8c0 kasan_report+0xb8/0xf0 ? __run_timer_base.part.0+0x7d7/0x8c0 __run_timer_base.part.0+0x7d7/0x8c0 ? __pfx___run_timer_base.part.0+0x10/0x10 ? __pfx_read_tsc+0x10/0x10 ? ktime_get+0x60/0x140 ? lapic_next_event+0x11/0x20 ? clockevents_program_event+0x1d4/0x2a0 run_timer_softirq+0xd1/0x190		

CVE-2025-39996	handle_softirqs+0x16a/0x550 irq_exit_rcu+0xaf/0xe0 sysvec_apic_timer_interrupt+0x70/0x80 </IRQ> ... Allocated by task 1: kasan_save_stack+0x24/0x50 kasan_save_track+0x14/0x30 __kasan_kmalloc+0x7f/0x90 __kmalloc_noprof+0x1be/0x460 flexcop_device_kmalloc+0x54/0xe0 flexcop_pci_probe+0x1f/0x9d0 local_pci_probe+0xdc/0x190 pci_device_probe+0x2fe/0x470 really_probe+0x1ca/0x5c0 __driver_probe_device+0x248/0x310 driver_probe_device+0x44/0x120 __driver_attach+0xd2/0x310 bus_for_each_dev+0xed/0x170 bus_add_driver+0x208/0x500 driver_register+0x132/0x460 do_one_initcall+0x89/0x300 kernel_init_freeable+0x40d/0x720 kernel_init+0x1a/0x150 ret_from_fork+0x10c/0x1a0 ret_from_fork_asm+0x1a/0x30 Freed by task 135: kasan_save_stack+0x24/0x50 kasan_save_track+0x14/0x30 kasan_save_free_info+0x3a/0x60 __kasan_slab_free+0x3f/0x50 kfree+0x137/0x370 flexcop_device_kfree+0x32/0x50 pci_device_remove+0xa6/0x1d0 device_release_driver_internal+0xf8/0x210 pci_stop_bus_device+0x105/0x150 pci_stop_and_remove_bus_device_locked+0x15/0x30 remove_store+0xcc/0xe0 kernfs_fop_write_iter+0x2c3/0x440 vfs_write+0x871/0xd70 ksys_write+0xee/0x1c0 do_syscall_64+0xac/0x280 entry_SYSCALL_64_after_hwframe+0x77/0x7f ... Replace cancel_delayed_work() with cancel_delayed_work_sync() to ensure that the delayed work item is properly canceled and any executing delayed work has finished before the device memory is deallocated. This bug was initially identified through static analysis. To reproduce and test it, I simulated the B2C2 FlexCop PCI device in QEMU and introduced artificial delays within the flexcop_pci_irq_check_work() function to increase the likelihood of triggering the bug.	N/A	More Details
CVE-2025-62695	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - WikiLambda Extension allows Stored XSS.This issue affects Mediawiki - WikiLambda Extension: master.	N/A	More Details
CVE-2025-62679	Rejected reason: Not used	N/A	More Details
CVE-2025-39994	In the Linux kernel, the following vulnerability has been resolved: media: tuner: xc5000: Fix use-after-free in xc5000_release The original code uses cancel_delayed_work() in xc5000_release(), which does not guarantee that the delayed work item timer_sleep has fully completed if it was already running. This leads to use-after-free scenarios where xc5000_release() may free the xc5000_priv while timer_sleep is still active and attempts to dereference the xc5000_priv. A typical race condition is illustrated below: CPU 0 (release thread) | CPU 1 (delayed work callback) xc5000_release() | xc5000_do_timer_sleep() cancel_delayed_work() | hybrid_tuner_release_state(priv) | kfree(priv) | | priv = container_of() // UAF Replace cancel_delayed_work() with cancel_delayed_work_sync() to ensure that the timer_sleep is properly canceled before the xc5000_priv memory is deallocated. A deadlock concern was considered: xc5000_release() is called in a process context and is not holding any locks that the timer_sleep work item might also need. Therefore, the use of the _sync() variant is safe here. This bug was initially identified through static analysis. [hverkuil: fix typo in Subject: tunner -> tuner]	N/A	More Details
CVE-2025-62678	Rejected reason: Not used	N/A	More Details
CVE-2025-62680	Rejected reason: Not used	N/A	More Details
CVE-2025-62677	Rejected reason: Not used	N/A	More Details
CVE-2025-62681	Rejected reason: Not used	N/A	More Details
CVE-2025-62682	Rejected reason: Not used	N/A	More Details
CVE-2025-62683	Rejected reason: Not used	N/A	More Details
CVE-2025-62684	Rejected reason: Not used	N/A	More Details
CVE-2025-	SQL injection vulnerability in the fields of warehouse document filtering form in SIMPLE.ERP software allows logged-in user to send a payload of up to 20 characters. Identified use case allows to delete tables with a name of maximum 6 characters. We weren't able to identify a way to exfiltrate data within query character	N/A	More Details

9339	limit. This issue affects SIMPLE.ERP in versions before 6.30@a04.3.		
CVE-2025-62694	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - WikiLove Extension allows Stored XSS.This issue affects Mediawiki - WikiLove Extension: 1.39.	N/A	More Details
CVE-2025-62696	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in The Wikimedia Foundation Mediawiki Foundation - Springboard Extension allows Command Injection.This issue affects Mediawiki Foundation - Springboard Extension: master.	N/A	More Details
CVE-2025-62699	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in The Wikimedia Foundation Mediawiki - Translate Extension allows Footprinting. Translate extension appears to use jobs to make edits to translation pages. This causes the CheckUser tool to log the wrong IP and User-Agent making these edits un-auditable via the CheckUser tool.This issue affects Mediawiki - Translate Extension: from master before 1.39.	N/A	More Details
CVE-2025-11625	Improper host authentication vulnerability in wolfSSH version 1.4.20 and earlier clients that allows authentication bypass and leaking of clients credentials.	N/A	More Details
CVE-2025-62701	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - Wikistories allows Stored XSS.This issue affects Mediawiki - Wikistories: from master before 1.44.	N/A	More Details
CVE-2025-62702	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - PageTriage Extension allows Stored XSS.This issue affects Mediawiki - PageTriage Extension: from master before 1.44.	N/A	More Details
CVE-2025-12004	Incorrect Permission Assignment for Critical Resource vulnerability in The Wikimedia Foundation Mediawiki - Lockdown Extension allows Privilege Abuse. Fixed in Mediawiki Core Action APIThis issue affects Mediawiki - Lockdown Extension: from master before 1.42.	N/A	More Details
CVE-2025-61941	A path traversal issue exists in WXR9300BE6P series firmware versions prior to Ver.1.10. Arbitrary file may be altered by an administrative user who logs in to the affected product. Moreover, arbitrary OS command may be executed via some file alteration.	N/A	More Details
CVE-2025-10639	The WorkExaminer Professional server installation comes with an FTP server that is used to receive the client logs on TCP port 12304. An attacker with network access to this port can use weak hardcoded credentials to login to the FTP server and modify or read data, log files and gain remote code execution as NT Authority\SYSTEM on the server by exchanging accessible service binaries in the WorkExaminer installation directory (e.g. "C:\Program File (x86)\Work Examiner Professional Server").	N/A	More Details
CVE-2025-10640	An unauthenticated attacker with access to TCP port 12306 of the WorkExaminer server can exploit missing server-side authentication checks to bypass the login prompt in the WorkExaminer Professional console to gain administrative access to the WorkExaminer server and therefore all sensitive monitoring data. This includes monitored screenshots and keystrokes of all users. The WorkExaminer Professional console is used for administrative access to the server. Before access to the console is granted administrators must login. Internally, a custom protocol is used to call a respective stored procedure on the MSSQL database. The return value of the call is not validated on the server-side. Instead it is only validated client-side which allows to bypass authentication.	N/A	More Details
CVE-2025-10641	All WorkExaminer Professional traffic between monitoring client, console and server is transmitted as plain text. This allows an attacker with access to the network to read the transmitted sensitive data. An attacker can also freely modify the data on the wire. The monitoring clients transmit their data to the server using the unencrypted FTP. Clients connect to the FTP server on port 12304 and transmit the data unencrypted. In addition, all traffic between the console client and the server at port 12306 is unencrypted.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: fix use-after-free in rtw89_core_tx_kick_off_and_wait() There is a bug observed when rtw89_core_tx_kick_off_and_wait() tries to access already freed skb_data: BUG: KFENCE: use-after-free write in rtw89_core_tx_kick_off_and_wait drivers/net/wireless/realtek/rtw89/core.c:1110 CPU: 6 UID: 0 PID: 41377 Comm: kworker/u64:24 Not tainted 6.17.0-rc1+ #1 PREEMPT(lazy) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS edk2-20250523-14.fc42 05/23/2025 Workqueue: events_unbound cfg80211_wiphy_work [cfg80211] Use-after-free write at 0x0000000020309d9d (in kfence-#251): rtw89_core_tx_kick_off_and_wait drivers/net/wireless/realtek/rtw89/core.c:1110 rtw89_core_scan_complete drivers/net/wireless/realtek/rtw89/core.c:5338 rtw89_hw_scan_complete_cb drivers/net/wireless/realtek/rtw89/fw.c:7979 rtw89_chanctx_proceed_cb drivers/net/wireless/realtek/rtw89/chan.c:3165 rtw89_chanctx_proceed drivers/net/wireless/realtek/rtw89/chan.h:141 rtw89_hw_scan_complete drivers/net/wireless/realtek/rtw89/fw.c:8012 rtw89_mac_c2h_scanofld_rsp drivers/net/wireless/realtek/rtw89/mac.c:5059 rtw89_fw_c2h_work drivers/net/wireless/realtek/rtw89/fw.c:6758 process_one_work kernel/workqueue.c:3241 worker_thread kernel/workqueue.c:3400 kthread kernel/kthread.c:463 ret_from_fork arch/x86/kernel/process.c:154		

CVE-2025-40000	ret_from_fork_asm arch/x86/entry/entry_64.S:258 kfence-#251: 0x0000000056e2393d-0x000000009943cb62, size=232, cache=skbuff_head_cache allocated by task 41377 on cpu 6 at 77869.159548s (0.009551s ago): __alloc_skb net/core/skbuff.c:659 __netdev_alloc_skb net/core/skbuff.c:734 ieee80211_nullfunc_get net/mac80211/tx.c:5844 rtw89_core_send_nullfunc drivers/net/wireless/realtek/rtw89/core.c:3431 rtw89_core_scan_complete drivers/net/wireless/realtek/rtw89/core.c:5338 rtw89_hw_scan_complete_cb drivers/net/wireless/realtek/rtw89/fw.c:7979 rtw89_chanctx_proceed_cb drivers/net/wireless/realtek/rtw89/chan.c:3165 rtw89_chanctx_proceed drivers/net/wireless/realtek/rtw89/chan.c:3194 rtw89_hw_scan_complete drivers/net/wireless/realtek/rtw89/fw.c:8012 rtw89_mac_c2h_scanofld_rsp drivers/net/wireless/realtek/rtw89/mac.c:5059 rtw89_fw_c2h_work drivers/net/wireless/realtek/rtw89/fw.c:6758 process_one_work kernel/workqueue.c:3241 worker_thread kernel/workqueue.c:3400 kthread kernel/kthread.c:463 ret_from_fork arch/x86/kernel/process.c:154 ret_from_fork_asm arch/x86/entry/entry_64.S:258 freed by task 1045 on cpu 9 at 77869.168393s (0.001557s ago): ieee80211_tx_status_skb net/mac80211/status.c:1117 rtw89_pci_release_txwd_skb drivers/net/wireless/realtek/rtw89/pci.c:564 rtw89_pci_release_tx_skbs.isra.0 drivers/net/wireless/realtek/rtw89/pci.c:651 rtw89_pci_release_tx drivers/net/wireless/realtek/rtw89/pci.c:676 rtw89_pci_napi_poll drivers/net/wireless/realtek/rtw89/pci.c:4238 __napi_poll net/core/dev.c:7495 net_rx_action net/core/dev.c:7557 net/core/dev.c:7684 handle_softirqs kernel/softirq.c:580 do_softirq.part.0 kernel/softirq.c:480 __local_bh_enable_ip kernel/softirq.c:407 rtw89_pci_interrupt_threadfn drivers/net/wireless/realtek/rtw89/pci.c:927 irq_thread_fn kernel/irq/manage.c:1133 irq_thread kernel/irq/manage.c:1257 kthread kernel/kthread.c:463 ret_from_fork arch/x86/kernel/process.c:154 ret_from_fork_asm arch/x86/entry/entry_64.S:258 It is a consequence of a race between the waiting and the signaling side of the completion: Waiting thread Completing thread rtw89_core_tx_kick_off_and_wait() rcu_assign_pointer(skb_data->wait, wait) /* start waiting */ wait_for_completion_timeout() rtw89_pci_tx_status() rtw89_core_tx_wait_complete() rcu_read_lock() /* signals completion and ---truncated---	N/A	More Details
CVE-2025-39999	In the Linux kernel, the following vulnerability has been resolved: blk-mq: fix blk_mq_tags double free while nr_requests grown In the case user trigger tags grow by queue sysfs attribute nr_requests, hctx->sched_tags will be freed directly and replaced with a new allocated tags, see blk_mq_tag_update_depth(). The problem is that hctx->sched_tags is from elevator->et->tags, while et->tags is still the freed tags, hence later elevator exit will try to free the tags again, causing kernel panic. Fix this problem by replacing et->tags with new allocated tags as well. Noted there are still some long term problems that will require some refactor to be fixed thoroughly[1]. [1] https://lore.kernel.org/all/20250815080216.410665-1-yukuai1@huaweicloud.com/	N/A	More Details
CVE-2025-39998	In the Linux kernel, the following vulnerability has been resolved: scsi: target: target_core_configfs: Add length check to avoid buffer overflow A buffer overflow arises from the usage of snprintf to write into the buffer "buf" in target_lu_gp_members_show function located in /drivers/target/target_core_configfs.c. This buffer is allocated with size LU_GROUP_NAME_BUF (256 bytes). snprintf(...) formats multiple strings into buf with the HBA name (hba->hba_group.cg_item), a slash character, a devicename (dev-> dev_group.cg_item) and a newline character, the total formatted string length may exceed the buffer size of 256 bytes. Since snprintf() returns the total number of bytes that would have been written (the length of %s/%sn), this value may exceed the buffer length (256 bytes) passed to memcpy(), this will ultimately cause function memcpy reporting a buffer overflow error. An additional check of the return value of snprintf() can avoid this buffer overflow.	N/A	More Details
CVE-2025-39997	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: fix race condition to UAF in snd_usbmidi_free The previous commit 0718a78f6a9f ("ALSA: usb-audio: Kill timer properly at removal") patched a UAF issue caused by the error timer. However, because the error timer kill added in this patch occurs after the endpoint delete, a race condition to UAF still occurs, albeit rarely. Additionally, since kill-cleanup for urb is also missing, freed memory can be accessed in interrupt context related to urb, which can cause UAF. Therefore, to prevent this, error timer and urb must be killed before freeing the heap memory.	N/A	More Details
CVE-2025-11624	Potential stack buffer overwrite on the SFTP server side when receiving a malicious packet that has a handle size larger than the system handle or file descriptor size, but smaller than max handle size allowed.	N/A	More Details
CVE-2025-34517	Ilevia EVE X1 Server firmware versions ≤ 4.7.18.0.eden contain an absolute path traversal vulnerability in get_file_content.php that allows an attacker to read arbitrary files. Ilevia has declined to service this vulnerability, and recommends that customers not expose port 8080 to the internet.	N/A	More Details
CVE-2025-8050	External Control of File Name or Path vulnerability in opentext Flipper allows Path Traversal. The vulnerability could allow a user to access files hosted on the server. This issue affects Flipper: 3.1.2.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: media: rc: fix races with imon_disconnect() Syzbot reports a KASAN issue as below: BUG: KASAN: use-after-free in __create_pipe include/linux/usb.h:1945 [inline] BUG: KASAN: use-after-free in send_packet+0xa2d/0xbc0 drivers/media/rc/imon.c:627 Read of size 4 at addr ffff8880256fb000 by task syz-executor314/4465 CPU: 2 PID: 4465 Comm: syz-executor314 Not tainted 6.0.0-rc1-syzkaller #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134		

CVE-2025-39993	lib/dump_stack.c:106 print_address_description mm/kasan/report.c:317 [inline] print_report.cold+0x2ba/0x6e9 mm/kasan/report.c:433 kasan_report+0xb1/0x1e0 mm/kasan/report.c:495 __create_pipe include/linux/usb.h:1945 [inline] send_packet+0xa2d/0xbc0 drivers/media/rc/imon.c:627 vfd_write+0x2d9/0x550 drivers/media/rc/imon.c:991 vfs_write+0x2d7/0xdd0 fs/read_write.c:576 ksys_write+0x127/0x250 fs/read_write.c:631 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd The iMON driver improperly releases the usb_device reference in imon_disconnect without coordinating with active users of the device. Specifically, the fields usbdev_intf0 and usbdev_intf1 are not protected by the users counter (ictx->users). During probe, imon_init_intf0 or imon_init_intf1 increments the usb_device reference count depending on the interface. However, during disconnect, usb_put_dev is called unconditionally, regardless of actual usage. As a result, if vfd_write or other operations are still in progress after disconnect, this can lead to a use-after-free of the usb_device pointer. Thread 1 vfd_write Thread 2 imon_disconnect ... if usb_put_dev(ictx->usbdev_intf0) else usb_put_dev(ictx->usbdev_intf1) ... while send_packet if pipe = usb_sndintpipe(ictx->usbdev_intf0) UAF else pipe = usb_sndctrlpipe(ictx->usbdev_intf0, 0) UAF Guard access to usbdev_intf0 and usbdev_intf1 after disconnect by checking ictx->disconnected in all writer paths. Add early return with -ENODEV in send_packet(), vfd_write(), lcd_write() and display_open() if the device is no longer present. Set and read ictx->disconnected under ictx->lock to ensure memory synchronization. Acquire the lock in imon_disconnect() before setting the flag to synchronize with any ongoing operations. Ensure writers exit early and safely after disconnect before the USB core proceeds with cleanup. Found by Linux Verification Center (linuxtesting.org) with Syzkaller.	N/A	More Details
CVE-2025-39973	In the Linux kernel, the following vulnerability has been resolved: i40e: add validation for ring_len param The `ring_len` parameter provided by the virtual function (VF) is assigned directly to the hardware memory context (HMC) without any validation. To address this, introduce an upper boundary check for both Tx and Rx queue lengths. The maximum number of descriptors supported by the hardware is 8k-32. Additionally, enforce alignment constraints: Tx rings must be a multiple of 8, and Rx rings must be a multiple of 32.	N/A	More Details
CVE-2025-39971	In the Linux kernel, the following vulnerability has been resolved: i40e: fix idx validation in config queues msg Ensure idx is within range of active/initialized TCs when iterating over vf->ch[idx] in i40e_vc_config_queues_msg().	N/A	More Details
CVE-2025-39970	In the Linux kernel, the following vulnerability has been resolved: i40e: fix input validation logic for action_meta Fix condition to check 'greater or equal' to prevent OOB dereference.	N/A	More Details
CVE-2025-39969	In the Linux kernel, the following vulnerability has been resolved: i40e: fix validation of VF state in get resources VF state I40E_VF_STATE_ACTIVE is not the only state in which VF is actually active so it should not be used to determine if a VF is allowed to obtain resources. Use I40E_VF_STATE_RESOURCES_LOADED that is set only in i40e_vc_get_vf_resources_msg() and cleared during reset.	N/A	More Details
CVE-2025-39968	In the Linux kernel, the following vulnerability has been resolved: i40e: add max boundary check for VF filters There is no check for max filters that VF can request. Add it.	N/A	More Details
CVE-2025-39967	In the Linux kernel, the following vulnerability has been resolved: fbcon: fix integer overflow in fbcon_do_set_font Fix integer overflow vulnerabilities in fbcon_do_set_font() where font size calculations could overflow when handling user-controlled font parameters. The vulnerabilities occur when: 1. CALC_FONTSZ(h, pitch, charcount) performs h * pith * charcount multiplication with user-controlled values that can overflow. 2. FONT_EXTRA_WORDS * sizeof(int) + size addition can also overflow 3. This results in smaller allocations than expected, leading to buffer overflows during font data copying. Add explicit overflow checking using check_mul_overflow() and check_add_overflow() kernel helpers to safety validate all size calculations before allocation.	N/A	More Details
CVE-2025-39966	In the Linux kernel, the following vulnerability has been resolved: iommufd: Fix race during abort for file descriptors fput() doesn't actually call file_operations release() synchronously, it puts the file on a work queue and it will be released eventually. This is normally fine, except for iommufd the file and the iommufd_object are tied to gether. The file has the object as it's private_data and holds a users refcount, while the object is expected to remain alive as long as the file is. When the allocation of a new object aborts before installing the file it will fput() the file and then go on to immediately kfree() the obj. This causes a UAF once the workqueue completes the fput() and tries to decrement the users refcount. Fix this by putting the core code in charge of the file lifetime, and call __fput_sync() during abort to ensure that release() is called before kfree. __fput_sync() is a bit too tricky to open code in all the object implementations. Instead the objects tell the core code where the file pointer is and the core will take care of the life cycle. If the object is successfully allocated then the file will hold a users refcount and the iommufd_object cannot be destroyed. It is worth noting that close(); ioctl(IOMMU_DESTROY); doesn't have an issue because close() is already using a synchronous version of fput(). The UAF looks like this: BUG: KASAN: slab-use-after-free in iommufd_eventq_fops_release+0x45/0xc0 drivers/iommu/iommufd/eventq.c:376 Write of size 4 at addr ffff888059c97804 by task syz.0.46/6164 CPU: 0 UID: 0 PID: 6164 Comm: syz.0.46 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/18/2025 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x116/0x1f0 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xcd/0x630	N/A	More Details

	mm/kasan/report.c:482 kasan_report+0xe0/0x110 mm/kasan/report.c:595 check_region_inline mm/kasan/generic.c:183 [inline] kasan_check_range+0x100/0x1b0 mm/kasan/generic.c:189 instrument_atomic_read_write include/linux/instrumented.h:96 [inline] atomic_fetch_sub_release include/linux/atomic/atomic-instrumented.h:400 [inline] __refcount_dec include/linux/refcount.h:455 [inline] refcount_dec include/linux/refcount.h:476 [inline] iommufd_eventq_fops_release+0x45/0xc0 drivers/iommu/iommufd/eventq.c:376 __fput+0x402/0xb70 fs/file_table.c:468 task_work_run+0x14d/0x240 kernel/task_work.c:227 resume_user_mode_work include/linux/resume_user_mode.h:50 [inline] exit_to_user_mode_loop+0xeb/0x110 kernel/entry/common.c:43 exit_to_user_mode_prepare include/linux/irq-entry-common.h:225 [inline] syscall_exit_to_user_mode_work include/linux/entry-common.h:175 [inline] syscall_exit_to_user_mode include/linux/entry-common.h:210 [inline] do_syscall_64+0x41c/0x4c0 arch/x86/entry/syscall_64.c:100 entry_SYSCALL_64_after_hwframe+0x77/0x7f		
CVE-2025-55080	In Eclipse ThreadX before 6.4.3, when memory protection is enabled, syscall parameters verification wasn't enough, allowing an attacker to obtain an arbitrary memory read/write.	N/A	More Details
CVE-2025-26861	RemoteCall Remote Support Program (for Operator) versions prior to 5.3.0 contain an uncontrolled search path element vulnerability. If a crafted DLL is placed in the same folder with the affected product, it may cause an arbitrary code execution.	N/A	More Details
CVE-2025-26860	RemoteCall Remote Support Program (for Operator) versions prior to 5.1.0 contain an uncontrolled search path element vulnerability. If a crafted DLL is placed in the same folder with the affected product, it may cause an arbitrary code execution.	N/A	More Details
CVE-2025-26859	RemoteView PC Application Console versions prior to 6.0.2 contain an uncontrolled search path element vulnerability. If a crafted DLL is placed in the same folder with the affected product, it may cause an arbitrary code execution.	N/A	More Details
CVE-2025-55079	In Eclipse ThreadX before version 6.4.3, the thread module has a setting of maximum priority. In some cases the check of that maximum priority wasn't performed, allowing, as a result, to obtain a thread with higher priority than expected and causing a possible denial of service.	N/A	More Details
CVE-2025-62448	Rejected reason: Not used	N/A	More Details
CVE-2025-62447	Rejected reason: Not used	N/A	More Details
CVE-2025-62446	Rejected reason: Not used	N/A	More Details
CVE-2025-62445	Rejected reason: Not used	N/A	More Details
CVE-2025-62444	Rejected reason: Not used	N/A	More Details
CVE-2025-62443	Rejected reason: Not used	N/A	More Details
CVE-2025-62442	Rejected reason: Not used	N/A	More Details
CVE-2025-62441	Rejected reason: Not used	N/A	More Details
CVE-2025-62440	Rejected reason: Not used	N/A	More Details
CVE-2024-13991	Huijietong Cloud Video Platform contains a path traversal vulnerability that allows an unauthenticated attacker can supply arbitrary file paths to the `fullPath` parameter of the `/fileDownload?action=downloadBackupFile` endpoint and retrieve files from the server filesystem. VulnCheck has observed this vulnerability being targeted by the RondoDox botnet campaign.	N/A	More Details

CVE-2023-7311	BYTEVALUE Intelligent Flow Control Router contains a command injection vulnerability via the /goform/webRead/open endpoint. The `path` parameter is not properly validated and is echoed into a shell context, allowing an attacker to inject and execute arbitrary shell commands on the device. Successful exploitation can lead to writing backdoors, privilege escalation on the host, and full compromise of the router and its management functions. VulnCheck has observed this vulnerability being targeted by the RondoDox botnet campaign.	N/A	More Details
CVE-2023-7305	SmartBI V8, V9, and V10 contain an unrestricted file upload vulnerability via the RMIServlet request handling logic. Under certain configurations or usage patterns, attackers can send specially crafted requests that cause the application to perform sensitive operations or execute arbitrary code on the host. The vendor released a fix in July 2023 to address the underlying flaw. VulnCheck has observed this vulnerability being targeted by the RondoDox botnet campaign.	N/A	More Details
CVE-2023-7304	Ruijie RG-UAC Application Management Gateway contains a command injection vulnerability via the 'nmc_sync.php' interface. An unauthenticated attacker able to reach the affected endpoint can inject shell commands via crafted request data, causing the application to execute arbitrary commands on the host. Successful exploitation can yield full control of the application process and may lead to system-level access depending on the service privileges. VulnCheck has observed this vulnerability being targeted by the RondoDox botnet campaign.	N/A	More Details
CVE-2018-25117	VestaCP commit a3f0fa1 (2018-05-31) up to commit ee03eff (2018-06-13) contain embedded malicious code that resulted in a supply-chain compromise. New installations created from the compromised installer since at least May 2018 were subject to installation of Linux/ChachaDDoS, a multi-stage DDoS bot that uses Lua for second- and third-stage components. The compromise leaked administrative credentials (base64-encoded admin password and server domain) to an external URL during installation and/or resulted in the installer dropping and executing a DDoS malware payload under local system privileges. Compromised servers were subsequently observed participating in large-scale DDoS activity. Vesta acknowledged exploitation in the wild in October 2018.	N/A	More Details
CVE-2017-20205	Valve's Source SDK (source-sdk-2013)'s ragdoll model parsing logic contains a stack-based buffer overflow vulnerability.The tokenizer function `nexttoken` copies characters from an input string into a fixed-size stack buffer without performing bounds checks. When `ParseKeyValue` processes a collisionpair rule longer than the destination buffer (256 bytes), an overflow of the stack buffer `szToken` can occur and overwrite the function return address. A remote attacker can trigger the vulnerable code by supplying a specially crafted ragdoll model which causes the oversized collisionpair rule to be parsed, resulting in remote code execution on affected clients or servers. Valve has addressed this issue in many of their Source games, but independently-developed games must manually apply patch.	N/A	More Details
CVE-2017-20204	DBLTek GoIP devices (models GoIP 1, 4, 8, 16, and 32) contain an undocumented vendor backdoor in the Telnet administrative interface that allows remote authentication as an undocumented user via a proprietary challenge–response scheme which is fundamentally flawed. Because the challenge response can be computed from the challenge itself, a remote attacker can authenticate without knowledge of a secret and obtain a root shell on the device. This can lead to persistent remote code execution, full device compromise, and arbitrary control of the device and any managed services. The firmware used within these devices was updated in December 2016 to make this vulnerability more complex to exploit. However, it is unknown if DBLTek has taken steps to fully mitigate.	N/A	More Details
CVE-2011-10033	The WordPress plugin is-human <= v1.4.2 contains an eval injection vulnerability in /is-human/engine.php that can be triggered via the 'type' parameter when the 'action' parameter is set to 'log-reset'. The root cause is unsafe use of eval() on user-controlled input, which can lead to execution of attacker-supplied PHP and OS commands. This may result in arbitrary code execution as the webserver user, site compromise, or data exfiltration. The is-human plugin was made defunct in June 2008 and is no longer available for download. This vulnerability was exploited in the wild in March 2012.	N/A	More Details
CVE-2025-62661	Incorrect Default Permissions vulnerability in The Wikimedia Foundation Mediawiki - Thanks Extension, Mediawiki - Growth Experiments Extension allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Mediawiki - Thanks Extension, Mediawiki - Growth Experiments Extension: from 1.43 before 1.44.	N/A	More Details
CVE-2025-39972	In the Linux kernel, the following vulnerability has been resolved: i40e: fix idx validation in i40e_validate_queue_map Ensure idx is within range of active/initialized TCs when iterating over vf->ch[idx] in i40e_validate_queue_map().	N/A	More Details
CVE-2025-39974	In the Linux kernel, the following vulnerability has been resolved: tracing/osnoise: Fix slab-out-of-bounds in _parse_integer_limit() When config osnoise cpus by write() syscall, the following KASAN splat may be observed: BUG: KASAN: slab-out-of-bounds in _parse_integer_limit+0x103/0x130 Read of size 1 at addr ffff88810121e3a1 by task test/447 CPU: 1 UID: 0 PID: 447 Comm: test Not tainted 6.17.0-rc6-dirty #288 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x55/0x70 print_report+0xcb/0x610 kasan_report+0xb8/0xf0 _parse_integer_limit+0x103/0x130 bitmap_parselist+0x16d/0x6f0 osnoise_cpus_write+0x116/0x2d0 vfs_write+0x21e/0xcc0 ksys_write+0xee/0x1c0 do_syscall_64+0xa8/0x2a0 entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> This issue can be reproduced by below code: const	N/A	More Details

	char *cpulist = "1"; int fd=open("/sys/kernel/debug/tracing/osnoise/cpus", O_WRONLY); write(fd, cpulist, strlen(cpulist)); Function bitmap_parselist() was called to parse cpulist, it require that the parameter 'buf' must be terminated with a '\0' or '\n'. Fix this issue by adding a '\0' to 'buf' in osnoise_cpus_write().		
CVE-2025-39992	In the Linux kernel, the following vulnerability has been resolved: mm: swap: check for stable address space before operating on the VMA It is possible to hit a zero entry while traversing the vmas in unuse_mm() called from swapoff path and accessing it causes the OOPS: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000446--> Loading the memory from offset 0x40 on the XA_ZERO_ENTRY as address. Mem abort info: ESR = 0x0000000096000005 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x05: level 1 translation fault The issue is manifested from the below race between the fork() on a process and swapoff: fork(dup_mmap()) swapoff(unuse_mm) ---------- ---------- 1) Identical mtree is built using __mt_dup(). 2) copy_pte_range()--> copy_nonpresent_pte(): The dst mm is added into the mmlist to be visible to the swapoff operation. 3) Fatal signal is sent to the parent process(which is the current during the fork) thus skip the duplication of the vmas and mark the vma range with XA_ZERO_ENTRY as a marker for this process that helps during exit_mmap(). 4) swapoff is tried on the 'mm' added to the 'mmlist' as part of the 2. 5) unuse_mm(), that iterates through the vma's of this 'mm' will hit the non-NULL zero entry and operating on this zero entry as a vma is resulting into the oops. The proper fix would be around not exposing this partially-valid tree to others when droping the mmap lock, which is being solved with [1]. A simpler solution would be checking for MMF_UNSTABLE, as it is set if mm_struct is not fully initialized in dup_mmap(). Thanks to Liam/Lorenzo/David for all the suggestions in fixing this issue.	N/A	More Details
CVE-2025-39975	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix wrong index reference in smb2_compound_op() In smb2_compound_op(), the loop that processes each command's response uses wrong indices when accessing response bufferes. This incorrect indexing leads to improper handling of command results. Also, if incorrectly computed index is greather than or equal to MAX_COMPOUND, it can cause out-of-bounds accesses.	N/A	More Details
CVE-2025-12024	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-22166	This High severity DoS (Denial of Service) vulnerability was introduced in version 2.0 of Confluence Data Center. This DoS (Denial of Service) vulnerability, with a CVSS Score of 8.3, allows an attacker to cause a resource to be unavailable for its intended users by temporarily or indefinitely disrupting services of a host connected to a network. Atlassian recommends that Confluence Data Center customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Confluence Data Center and Server 8.5: Upgrade to a release greater than or equal to 8.5.25 Confluence Data Center and Server 9.2: Upgrade to a release greater than or equal to 9.2.7 Confluence Data Center and Server 10.0: Upgrade to a release greater than or equal to 10.0.2 See the release notes ([https://confluence.atlassian.com/doc/confluence-release-notes-327.html]). You can download the latest version of Confluence Data Center from the download center ([https://www.atlassian.com/software/confluence/download-archives]). This vulnerability was reported via our Atlassian (Internal) program.	N/A	More Details
CVE-2025-39991	In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: fix NULL dereference in ath11k_qmi_m3_load() If ab->fw.m3_data points to data, then fw pointer remains null. Further, if m3_mem is not allocated, then fw is dereferenced to be passed to ath11k_err function. Replace fw->size by m3_len. Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2025-39990	In the Linux kernel, the following vulnerability has been resolved: bpf: Check the helper function is valid in get_helper_proto kernel test robot reported verifier bug [1] where the helper func pointer could be NULL due to disabled config option. As Alexei suggested we could check on that in get_helper_proto directly. Marking tail_call helper func with BPF_PTR_POISON, because it is unused by design. [1] https://lore.kernel.org/oe-lkp/202507160818.68358831-lkp@intel.com	N/A	More Details
CVE-2025-39988	In the Linux kernel, the following vulnerability has been resolved: can: etas_es58x: populate ndo_change_mtu() to prevent buffer overflow Sending an PF_PACKET allows to bypass the CAN framework logic and to directly reach the xmit() function of a CAN driver. The only check which is performed by the PF_PACKET framework is to make sure that skb->len fits the interface's MTU. Unfortunately, because the etas_es58x driver does not populate its net_device_ops->ndo_change_mtu(), it is possible for an attacker to configure an invalid MTU by doing, for example: $ ip link set can0 mtu 9999 After doing so, the attacker could open a PF_PACKET socket using the ETH_P_CANXL protocol: socket(PF_PACKET, SOCK_RAW, htons(ETH_P_CANXL)); to inject a malicious CAN XL frames. For example: struct canxl_frame frame = { .flags = 0xff, .len = 2048, }; The CAN drivers' xmit() function are calling can_dev_dropped_skb() to check that the skb is valid, unfortunately under above conditions, the malicious packet is able to go through can_dev_dropped_skb() checks: 1. the skb->protocol is set to ETH_P_CANXL which is valid (the function does not check the actual device capabilities). 2. the length is a valid CAN XL length. And so, es58x_start_xmit() receives a CAN XL frame which it is not able to correctly handle and will thus misinterpret it as a CAN(FD) frame. This can result in a buffer overflow. For example, using the es581.4 variant, the frame will be dispatched to es581_4_tx_can_msg(), go through the last check at the beginning of this function: if (can_is_canfd_skb(skb)) return -EMSGSIZE; and reach this line: memcpy(tx_can_msg->data, cf->data, cf-	N/A	More Details

	>len); Here, cf->len corresponds to the flags field of the CAN XL frame. In our previous example, we set canxl_frame->flags to 0xff. Because the maximum expected length is 8, a buffer overflow of 247 bytes occurs! Populate net_device_ops->ndo_change_mtu() to ensure that the interface's MTU can not be set to anything bigger than CAN_MTU or CANFD_MTU (depending on the device capabilities). By fixing the root cause, this prevents the buffer overflow.		
CVE-2025-39987	In the Linux kernel, the following vulnerability has been resolved: can: hi311x: populate ndo_change_mtu() to prevent buffer overflow Sending an PF_PACKET allows to bypass the CAN framework logic and to directly reach the xmit() function of a CAN driver. The only check which is performed by the PF_PACKET framework is to make sure that skb->len fits the interface's MTU. Unfortunately, because the sun4i_can driver does not populate its net_device_ops->ndo_change_mtu(), it is possible for an attacker to configure an invalid MTU by doing, for example: $ ip link set can0 mtu 9999 After doing so, the attacker could open a PF_PACKET socket using the ETH_P_CANXL protocol: socket(PF_PACKET, SOCK_RAW, htons(ETH_P_CANXL)) to inject a malicious CAN XL frames. For example: struct canxl_frame frame = { .flags = 0xff, .len = 2048, }; The CAN drivers' xmit() function are calling can_dev_dropped_skb() to check that the skb is valid, unfortunately under above conditions, the malicious packet is able to go through can_dev_dropped_skb() checks: 1. the skb->protocol is set to ETH_P_CANXL which is valid (the function does not check the actual device capabilities). 2. the length is a valid CAN XL length. And so, hi3110_hard_start_xmit() receives a CAN XL frame which it is not able to correctly handle and will thus misinterpret it as a CAN frame. The driver will consume frame->len as-is with no further checks. This can result in a buffer overflow later on in hi3110_hw_tx() on this line: memcpy(buf + HI3110_FIFO_EXT_DATA_OFF, frame->data, frame->len); Here, frame->len corresponds to the flags field of the CAN XL frame. In our previous example, we set canxl_frame->flags to 0xff. Because the maximum expected length is 8, a buffer overflow of 247 bytes occurs! Populate net_device_ops->ndo_change_mtu() to ensure that the interface's MTU can not be set to anything bigger than CAN_MTU. By fixing the root cause, this prevents the buffer overflow.	N/A	More Details
CVE-2025-39986	In the Linux kernel, the following vulnerability has been resolved: can: sun4i_can: populate ndo_change_mtu() to prevent buffer overflow Sending an PF_PACKET allows to bypass the CAN framework logic and to directly reach the xmit() function of a CAN driver. The only check which is performed by the PF_PACKET framework is to make sure that skb->len fits the interface's MTU. Unfortunately, because the sun4i_can driver does not populate its net_device_ops->ndo_change_mtu(), it is possible for an attacker to configure an invalid MTU by doing, for example: $ ip link set can0 mtu 9999 After doing so, the attacker could open a PF_PACKET socket using the ETH_P_CANXL protocol: socket(PF_PACKET, SOCK_RAW, htons(ETH_P_CANXL)) to inject a malicious CAN XL frames. For example: struct canxl_frame frame = { .flags = 0xff, .len = 2048, }; The CAN drivers' xmit() function are calling can_dev_dropped_skb() to check that the skb is valid, unfortunately under above conditions, the malicious packet is able to go through can_dev_dropped_skb() checks: 1. the skb->protocol is set to ETH_P_CANXL which is valid (the function does not check the actual device capabilities). 2. the length is a valid CAN XL length. And so, sun4ican_start_xmit() receives a CAN XL frame which it is not able to correctly handle and will thus misinterpret it as a CAN frame. This can result in a buffer overflow. The driver will consume cf->len as-is with no further checks on this line: dlc = cf->len; Here, cf->len corresponds to the flags field of the CAN XL frame. In our previous example, we set canxl_frame->flags to 0xff. Because the maximum expected length is 8, a buffer overflow of 247 bytes occurs a couple line below when doing: for (i = 0; i < dlc; i++) writel(cf->data[i], priv->base + (dreg + i * 4)); Populate net_device_ops->ndo_change_mtu() to ensure that the interface's MTU can not be set to anything bigger than CAN_MTU. By fixing the root cause, this prevents the buffer overflow.	N/A	More Details
CVE-2025-62250	Improper Authentication in Liferay Portal 7.4.0 through 7.4.3.132, and older unsupported versions, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions allows remote attackers to send malicious data to the Liferay Portal 7.4.0 through 7.4.3.132, and older unsupported versions, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions that will treat it as trusted data via unauthenticated cluster messages.	N/A	More Details
CVE-2025-11534	The affected Raisecom devices allow SSH sessions to be established without completing user authentication. This could allow attackers to gain shell access without valid credentials.	N/A	More Details
CVE-2025-39985	In the Linux kernel, the following vulnerability has been resolved: can: mcba_usb: populate ndo_change_mtu() to prevent buffer overflow Sending an PF_PACKET allows to bypass the CAN framework logic and to directly reach the xmit() function of a CAN driver. The only check which is performed by the PF_PACKET framework is to make sure that skb->len fits the interface's MTU. Unfortunately, because the mcba_usb driver does not populate its net_device_ops->ndo_change_mtu(), it is possible for an attacker to configure an invalid MTU by doing, for example: $ ip link set can0 mtu 9999 After doing so, the attacker could open a PF_PACKET socket using the ETH_P_CANXL protocol: socket(PF_PACKET, SOCK_RAW, htons(ETH_P_CANXL)) to inject a malicious CAN XL frames. For example: struct canxl_frame frame = { .flags = 0xff, .len = 2048, }; The CAN drivers' xmit() function are calling can_dev_dropped_skb() to check that the skb is valid, unfortunately under above conditions, the malicious packet is able to go through can_dev_dropped_skb() checks: 1. the skb->protocol is set to ETH_P_CANXL which is valid (the function does not check the actual device capabilities). 2. the length is a valid CAN XL length. And so, mcba_usb_start_xmit() receives a CAN XL frame which it is not able to correctly handle and will thus	N/A	More Details

	misinterpret it as a CAN frame. This can result in a buffer overflow. The driver will consume cf->len as-is with no further checks on these lines: usb_msg.dlc = cf->len; memcpy(usb_msg.data, cf->data, usb_msg.dlc); Here, cf->len corresponds to the flags field of the CAN XL frame. In our previous example, we set canxl_frame->flags to 0xff. Because the maximum expected length is 8, a buffer overflow of 247 bytes occurs! Populate net_device_ops->ndo_change_mtu() to ensure that the interface's MTU can not be set to anything bigger than CAN_MTU. By fixing the root cause, this prevents the buffer overflow.		
CVE-2025-60506	Moodle PDF Annotator plugin v1.5 release 9 allows stored cross-site scripting (XSS) via the Public Comments feature. An attacker with a low-privileged account (e.g., Student) can inject arbitrary JavaScript payloads into a comment. When any other user (Student, Teacher, or Admin) views the annotated PDF, the payload is executed in their browser, leading to session hijacking, credential theft, or other attacker-controlled actions.	N/A	More Details
CVE-2025-60772	Improper authentication in the web-based management interface of NETLINK HG322G V1.0.00-231017, allows a remote unauthenticated attacker to escalate privileges and lock out the legitimate administrator via crafted HTTP requests.	N/A	More Details
CVE-2025-39984	In the Linux kernel, the following vulnerability has been resolved: net: tun: Update napi->skb after XDP process The syzbot report a UAF issue: BUG: KASAN: slab-use-after-free in skb_reset_mac_header include/linux/skbuff.h:3150 [inline] BUG: KASAN: slab-use-after-free in napi_frags_skb net/core/gro.c:723 [inline] BUG: KASAN: slab-use-after-free in napi_gro_frags+0x6e/0x1030 net/core/gro.c:758 Read of size 8 at addr ffff88802ef22c18 by task syz.0.17/6079 CPU: 0 UID: 0 PID: 6079 Comm: syz.0.17 Not tainted syzkaller #0 PREEMPT(full) Call Trace: <TASK> dump_stack_lvl+0x189/0x250 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xca/0x240 mm/kasan/report.c:482 kasan_report+0x118/0x150 mm/kasan/report.c:595 skb_reset_mac_header include/linux/skbuff.h:3150 [inline] napi_frags_skb net/core/gro.c:723 [inline] napi_gro_frags+0x6e/0x1030 net/core/gro.c:758 tun_get_user+0x28cb/0x3e20 drivers/net/tun.c:1920 tun_chr_write_iter+0x113/0x200 drivers/net/tun.c:1996 new_sync_write fs/read_write.c:593 [inline] vfs_write+0x5c9/0xb30 fs/read_write.c:686 ksys_write+0x145/0x250 fs/read_write.c:738 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0x3b0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> Allocated by task 6079: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:68 unpoison_slab_object mm/kasan/common.c:330 [inline] __kasan_mempool_unpoison_object+0xa0/0x170 mm/kasan/common.c:558 kasan_mempool_unpoison_object include/linux/kasan.h:388 [inline] napi_skb_cache_get+0x37b/0x6d0 net/core/skbuff.c:295 __alloc_skb+0x11e/0x2d0 net/core/skbuff.c:657 napi_alloc_skb+0x84/0x7d0 net/core/skbuff.c:811 napi_get_frags+0x69/0x140 net/core/gro.c:673 tun_napi_alloc_frags drivers/net/tun.c:1404 [inline] tun_get_user+0x77c/0x3e20 drivers/net/tun.c:1784 tun_chr_write_iter+0x113/0x200 drivers/net/tun.c:1996 new_sync_write fs/read_write.c:593 [inline] vfs_write+0x5c9/0xb30 fs/read_write.c:686 ksys_write+0x145/0x250 fs/read_write.c:738 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0x3b0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 6079: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x46/0x50 mm/kasan/generic.c:576 poison_slab_object mm/kasan/common.c:243 [inline] __kasan_slab_free+0x5b/0x80 mm/kasan/common.c:275 kasan_slab_free include/linux/kasan.h:233 [inline] slab_free_hook mm/slub.c:2422 [inline] slab_free mm/slub.c:4695 [inline] kmem_cache_free+0x18f/0x400 mm/slub.c:4797 skb_pp_cow_data+0xdd8/0x13e0 net/core/skbuff.c:969 netif_skb_check_for_xdp net/core/dev.c:5390 [inline] netif_receive_generic_xdp net/core/dev.c:5431 [inline] do_xdp_generic+0x699/0x11a0 net/core/dev.c:5499 tun_get_user+0x2523/0x3e20 drivers/net/tun.c:1872 tun_chr_write_iter+0x113/0x200 drivers/net/tun.c:1996 new_sync_write fs/read_write.c:593 [inline] vfs_write+0x5c9/0xb30 fs/read_write.c:686 ksys_write+0x145/0x250 fs/read_write.c:738 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0x3b0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f After commit e6d5dbdd20aa ("xdp: add multi-buff support for xdp running in generic mode"), the original skb may be freed in skb_pp_cow_data() when XDP program was attached, which was allocated in tun_napi_alloc_frags(). However, the napi->skb still point to the original skb, update it after XDP process.	N/A	More Details
CVE-2025-62597	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. Prior to version 3.5.1, a reflected cross-site scripting (XSS) vulnerability was identified in the editar_info_pessoal.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the sql parameter. The vulnerable endpoint is GET /WeGIA/html/pessoa/editar_info_pessoal.php?sql=1. This issue has been patched in version 3.5.1.	N/A	More Details
CVE-2025-62598	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. Prior to version 3.5.1, a reflected cross-site scripting (XSS) vulnerability was identified in the editar_info_pessoal.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the action parameter. The vulnerable endpoint is GET /WeGIA/html/pessoa/editar_info_pessoal.php?action=1. This issue has been patched in version 3.5.1.	N/A	More Details
CVE-2025-11757	The CloudEdge Cloud does not sanitize the MQTT topic input, which could allow an attacker to leverage the MQTT wildcard to receive all the messages that should be delivered to other users by subscribing to the a MQTT topic. In these messages, the attacker can obtain the credentials and key information to connect to the cameras from peer to peer.	N/A	More Details

CVE-2025-12031	HTTP Security Misconfiguration - Lacking Secure and HTTPOnly Attribute may allow reading the sensitive cookies from the javascript contextThis issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-60427	LibreTime 3.0.0-alpha.10 and possibly earlier is vulnerable to Broken Access Control, where a user with the DJ role can access analytics data via the Web UI and direct API calls. The backend does not verify role-based permissions for analytics endpoints, allowing unauthorized retrieval of station-wide metrics. This results in information disclosure to less privileged users.	N/A	More Details
CVE-2025-39983	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_event: Fix UAF in hci_conn_tx_dequeue This fixes the following UAF caused by not properly locking hdev when processing HCI_EV_NUM_COMP_PKTS: BUG: KASAN: slab-use-after-free in hci_conn_tx_dequeue+0x1be/0x220 net/bluetooth/hci_conn.c:3036 Read of size 4 at addr ffff8880740f0940 by task kworker/u11:0/54 CPU: 1 UID: 0 PID: 54 Comm: kworker/u11:0 Not tainted 6.16.0-rc7 #3 PREEMPT(full) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.10.2-1ubuntu1 04/01/2014 Workqueue: hci1 hci_rx_work Call Trace: <TASK> dump_stack_lvl+0x189/0x250 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xca/0x230 mm/kasan/report.c:480 kasan_report+0x118/0x150 mm/kasan/report.c:593 hci_conn_tx_dequeue+0x1be/0x220 net/bluetooth/hci_conn.c:3036 hci_num_comp_pkts_evt+0x1c8/0xa50 net/bluetooth/hci_event.c:4404 hci_event_func net/bluetooth/hci_event.c:7477 [inline] hci_event_packet+0x7e0/0x1200 net/bluetooth/hci_event.c:7531 hci_rx_work+0x46a/0xe80 net/bluetooth/hci_core.c:4070 process_one_work kernel/workqueue.c:3238 [inline] process_scheduled_works+0xae1/0x17b0 kernel/workqueue.c:3321 worker_thread+0x8a0/0xda0 kernel/workqueue.c:3402 kthread+0x70e/0x8a0 kernel/kthread.c:464 ret_from_fork+0x3fc/0x770 arch/x86/kernel/process.c:148 ret_from_fork_asm+0x1a/0x30 home/kwqcheii/source/fuzzing/kernel/kasan/linux-6.16-rc7/arch/x86/entry/entry_64.S:245 </TASK> Allocated by task 54: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:68 poison_kmalloc_redzone mm/kasan/common.c:377 [inline] __kasan_kmalloc+0x93/0xb0 mm/kasan/common.c:394 kasan_kmalloc include/linux/kasan.h:260 [inline] __kmalloc_cache_noprof+0x230/0x3d0 mm/slub.c:4359 kmalloc_noprof include/linux/slab.h:905 [inline] kzalloc_noprof include/linux/slab.h:1039 [inline] __hci_conn_add+0x233/0x1b30 net/bluetooth/hci_conn.c:939 le_conn_complete_evt+0x3d6/0x1220 net/bluetooth/hci_event.c:5628 hci_le_enh_conn_complete_evt+0x189/0x470 net/bluetooth/hci_event.c:5794 hci_event_func net/bluetooth/hci_event.c:7474 [inline] hci_event_packet+0x78c/0x1200 net/bluetooth/hci_event.c:7531 hci_rx_work+0x46a/0xe80 net/bluetooth/hci_core.c:4070 process_one_work kernel/workqueue.c:3238 [inline] process_scheduled_works+0xae1/0x17b0 kernel/workqueue.c:3321 worker_thread+0x8a0/0xda0 kernel/workqueue.c:3402 kthread+0x70e/0x8a0 kernel/kthread.c:464 ret_from_fork+0x3fc/0x770 arch/x86/kernel/process.c:148 ret_from_fork_asm+0x1a/0x30 home/kwqcheii/source/fuzzing/kernel/kasan/linux-6.16-rc7/arch/x86/entry/entry_64.S:245 Freed by task 9572: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x46/0x50 mm/kasan/generic.c:576 poison_slab_object mm/kasan/common.c:247 [inline] __kasan_slab_free+0x62/0x70 mm/kasan/common.c:264 kasan_slab_free include/linux/kasan.h:233 [inline] slab_free_hook mm/slub.c:2381 [inline] slab_free mm/slub.c:4643 [inline] kfree+0x18e/0x440 mm/slub.c:4842 device_release+0x9c/0x1c0 kobject_cleanup lib/kobject.c:689 [inline] kobject_release lib/kobject.c:720 [inline] kref_put include/linux/kref.h:65 [inline] kobject_put+0x22b/0x480 lib/kobject.c:737 hci_conn_cleanup net/bluetooth/hci_conn.c:175 [inline] hci_conn_del+0x8ff/0xcb0 net/bluetooth/hci_conn.c:1173 hci_abort_conn_sync+0x5d1/0xdf0 net/bluetooth/hci_sync.c:5689 hci_cmd_sync_work+0x210/0x3a0 net/bluetooth/hci_sync.c:332 process_one_work kernel/workqueue.c:3238 [inline] process_scheduled_works+0xae1/0x17b0 kernel/workqueue.c:3321 worker_thread+0x8a0/0xda0 kernel/workqueue.c:3402 kthread+0x70e/0x8a0 kernel/kthread.c:464 ret_from_fork+0x3fc/0x770 arch/x86/kernel/process.c:148 ret_from_fork_asm+0x1a/0x30 home/kwqcheii/source/fuzzing/kernel/kasan/linux-6.16-rc7/arch/x86/entry/entry_64.S:245	N/A	More Details
CVE-2025-60790	ProcessWire CMS 3.0.246 allows a low-privileged user with lang-edit to upload a crafted ZIP to Language Support that is auto-extracted without limits prior to validation, enabling resource-exhaustion Denial of Service.	N/A	More Details
CVE-2025-7850	A command injection vulnerability may be exploited after the admin's authentication on the web portal on Omada gateways.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_event: Fix UAF in hci_acl_create_conn_sync This fixes the following UFA in hci_acl_create_conn_sync where a connection still pending is command submission (conn->state == BT_OPEN) maybe freed, also since this also can happen with the likes of hci_le_create_conn_sync fix it as well: BUG: KASAN: slab-use-after-free in hci_acl_create_conn_sync+0x5ef/0x790 net/bluetooth/hci_sync.c:6861 Write of size 2 at addr ffff88805ffcc038 by task kworker/u11:2/9541 CPU: 1 UID: 0 PID: 9541 Comm: kworker/u11:2 Not tainted 6.16.0-rc7 #3 PREEMPT(full) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.10.2-1ubuntu1 04/01/2014 Workqueue: hci3 hci_cmd_sync_work Call Trace: <TASK> dump_stack_lvl+0x189/0x250 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xca/0x230 mm/kasan/report.c:480 kasan_report+0x118/0x150 mm/kasan/report.c:593		

CVE-2025-39982	hci_acl_create_conn_sync+0x5ef/0x790 net/bluetooth/hci_sync.c:6861 hci_cmd_sync_work+0x210/0x3a0 net/bluetooth/hci_sync.c:332 process_one_work kernel/workqueue.c:3238 [inline] process_scheduled_works+0xae1/0x17b0 kernel/workqueue.c:3321 worker_thread+0x8a0/0xda0 kernel/workqueue.c:3402 kthread+0x70e/0x8a0 kernel/kthread.c:464 ret_from_fork+0x3fc/0x770 arch/x86/kernel/process.c:148 ret_from_fork_asm+0x1a/0x30 home/kwqcheii/source/fuzzing/kernel/kasan/linux-6.16-rc7/arch/x86/entry/entry_64.S:245 </TASK> Allocated by task 123736: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:68 poison_kmalloc_redzone mm/kasan/common.c:377 [inline] __kasan_kmalloc+0x93/0xb0 mm/kasan/common.c:394 kasan_kmalloc include/linux/kasan.h:260 [inline] __kmalloc_cache_noprof+0x230/0x3d0 mm/slub.c:4359 kmalloc_noprof include/linux/slab.h:905 [inline] kzalloc_noprof include/linux/slab.h:1039 [inline] __hci_conn_add+0x233/0x1b30 net/bluetooth/hci_conn.c:939 hci_conn_add_unset net/bluetooth/hci_conn.c:1051 [inline] hci_connect_acl+0x16c/0x4e0 net/bluetooth/hci_conn.c:1634 pair_device+0x418/0xa70 net/bluetooth/mgmt.c:3556 hci_mgmt_cmd+0x9c9/0xef0 net/bluetooth/hci_sock.c:1719 hci_sock_sendmsg+0x6ca/0xef0 net/bluetooth/hci_sock.c:1839 sock_sendmsg_nosec net/socket.c:712 [inline] __sock_sendmsg+0x219/0x270 net/socket.c:727 sock_write_iter+0x258/0x330 net/socket.c:1131 new_sync_write fs/read_write.c:593 [inline] vfs_write+0x54b/0xa90 fs/read_write.c:686 ksys_write+0x145/0x250 fs/read_write.c:738 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0x3b0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 103680: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x46/0x50 mm/kasan/generic.c:576 poison_slab_object mm/kasan/common.c:247 [inline] __kasan_slab_free+0x62/0x70 mm/kasan/common.c:264 kasan_slab_free include/linux/kasan.h:233 [inline] slab_free_hook mm/slub.c:2381 [inline] slab_free mm/slub.c:4643 [inline] kfree+0x18e/0x440 mm/slub.c:4842 device_release+0x9c/0x1c0 kobject_cleanup lib/kobject.c:689 [inline] kobject_release lib/kobject.c:720 [inline] kref_put include/linux/kref.h:65 [inline] kobject_put+0x22b/0x480 lib/kobject.c:737 hci_conn_cleanup net/bluetooth/hci_conn.c:175 [inline] hci_conn_del+0x8ff/0xcb0 net/bluetooth/hci_conn.c:1173 hci_conn_complete_evt+0x3c7/0x1040 net/bluetooth/hci_event.c:3199 hci_event_func net/bluetooth/hci_event.c:7477 [inline] hci_event_packet+0x7e0/0x1200 net/bluetooth/hci_event.c:7531 hci_rx_work+0x46a/0xe80 net/bluetooth/hci_core.c:4070 process_one_work kernel/workqueue.c:3238 [inline] process_scheduled_works+0xae1/0x17b0 kernel/workqueue.c:3321 worker_thread+0x8a0/0xda0 kernel/workqueue.c:3402 kthread+0x70e/0x8a0 kernel/kthread.c:464 ret_from_fork+0x3fc/0x770 arch/x86/kernel/process.c:148 ret_from_fork_asm+0x1a/0x30 home/kwqcheii/sour ---truncated---	N/A	More Details
CVE-2025-39981	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: Fix possible UAFs This attemps to fix possible UAFs caused by struct mgmt_pending being freed while still being processed like in the following trace, in order to fix mgmt_pending_valid is introduce and use to check if the mgmt_pending hasn't been removed from the pending list, on the complete callbacks it is used to check and in addtion remove the cmd from the list while holding mgmt_pending_lock to avoid TOCTOU problems since if the cmd is left on the list it can still be accessed and freed. BUG: KASAN: slab-use-after-free in mgmt_add_adv_patterns_monitor_sync+0x35/0x50 net/bluetooth/mgmt.c:5223 Read of size 8 at addr ffff8880709d4dc0 by task kworker/u11:0/55 CPU: 0 UID: 0 PID: 55 Comm: kworker/u11:0 Not tainted 6.16.4 #2 PREEMPT(full) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.10.2-1ubuntu1 04/01/2014 Workqueue: hci0 hci_cmd_sync_work Call Trace: <TASK> dump_stack_lvl+0x189/0x250 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xca/0x240 mm/kasan/report.c:482 kasan_report+0x118/0x150 mm/kasan/report.c:595 mgmt_add_adv_patterns_monitor_sync+0x35/0x50 net/bluetooth/mgmt.c:5223 hci_cmd_sync_work+0x210/0x3a0 net/bluetooth/hci_sync.c:332 process_one_work kernel/workqueue.c:3238 [inline] process_scheduled_works+0xade/0x17b0 kernel/workqueue.c:3321 worker_thread+0x8a0/0xda0 kernel/workqueue.c:3402 kthread+0x711/0x8a0 kernel/kthread.c:464 ret_from_fork+0x3fc/0x770 arch/x86/kernel/process.c:148 ret_from_fork_asm+0x1a/0x30 home/kwqcheii/source/fuzzing/kernel/kasan/linux-6.16.4/arch/x86/entry/entry_64.S:245 </TASK> Allocated by task 12210: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:68 poison_kmalloc_redzone mm/kasan/common.c:377 [inline] __kasan_kmalloc+0x93/0xb0 mm/kasan/common.c:394 kasan_kmalloc include/linux/kasan.h:260 [inline] __kmalloc_cache_noprof+0x230/0x3d0 mm/slub.c:4364 kmalloc_noprof include/linux/slab.h:905 [inline] kzalloc_noprof include/linux/slab.h:1039 [inline] mgmt_pending_new+0x65/0x1e0 net/bluetooth/mgmt_util.c:269 mgmt_pending_add+0x35/0x140 net/bluetooth/mgmt_util.c:296 __add_adv_patterns_monitor+0x130/0x200 net/bluetooth/mgmt.c:5247 add_adv_patterns_monitor+0x214/0x360 net/bluetooth/mgmt.c:5364 hci_mgmt_cmd+0x9c9/0xef0 net/bluetooth/hci_sock.c:1719 hci_sock_sendmsg+0x6ca/0xef0 net/bluetooth/hci_sock.c:1839 sock_sendmsg_nosec net/socket.c:714 [inline] __sock_sendmsg+0x219/0x270 net/socket.c:729 sock_write_iter+0x258/0x330 net/socket.c:1133 new_sync_write fs/read_write.c:593 [inline] vfs_write+0x5c9/0xb30 fs/read_write.c:686 ksys_write+0x145/0x250 fs/read_write.c:738 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0x3b0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 12221: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x46/0x50 mm/kasan/generic.c:576 poison_slab_object mm/kasan/common.c:247 [inline] __kasan_slab_free+0x62/0x70 mm/kasan/common.c:264 kasan_slab_free include/linux/kasan.h:233 [inline] slab_free_hook mm/slub.c:2381 [inline] slab_free mm/slub.c:4648 [inline] kfree+0x18e/0x440	N/A	More Details

	mm/slub.c:4847 mgmt_pending_free net/bluetooth/mgmt_util.c:311 [inline] mgmt_pending_foreach+0x30d/0x380 net/bluetooth/mgmt_util.c:257 __mgmt_power_off+0x169/0x350 net/bluetooth/mgmt.c:9444 hci_dev_close_sync+0x754/0x1330 net/bluetooth/hci_sync.c:5290 hci_dev_do_close net/bluetooth/hci_core.c:501 [inline] hci_dev_close+0x108/0x200 net/bluetooth/hci_core.c:526 sock_do_ioctl+0xd9/0x300 net/socket.c:1192 sock_ioctl+0x576/0x790 net/socket.c:1313 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:907 [inline] __se_sys_ioctl+0xf9/0x170 fs/ioctl.c:893 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xf ---truncated---		
CVE-2025-39980	In the Linux kernel, the following vulnerability has been resolved: nexthop: Forbid FDB status change while nexthop is in a group The kernel forbids the creation of non-FDB nexthop groups with FDB nexthops: # ip nexthop add id 1 via 192.0.2.1 fdb # ip nexthop add id 2 group 1 Error: Non FDB nexthop group cannot have fdb nexthops. And vice versa: # ip nexthop add id 3 via 192.0.2.2 dev dummy1 # ip nexthop add id 4 group 3 fdb Error: FDB nexthop group can only have fdb nexthops. However, as long as no routes are pointing to a non-FDB nexthop group, the kernel allows changing the type of a nexthop from FDB to non-FDB and vice versa: # ip nexthop add id 5 via 192.0.2.2 dev dummy1 # ip nexthop add id 6 group 5 # ip nexthop replace id 5 via 192.0.2.2 fdb # echo $? 0 This configuration is invalid and can result in a NPD [1] since FDB nexthops are not associated with a nexthop device: # ip route add 198.51.100.1/32 nhid 6 # ping 198.51.100.1 Fix by preventing nexthop FDB status change while the nexthop is in a group: # ip nexthop add id 7 via 192.0.2.2 dev dummy1 # ip nexthop add id 8 group 7 # ip nexthop replace id 7 via 192.0.2.2 fdb Error: Cannot change nexthop FDB status while in a group. [1] BUG: kernel NULL pointer dereference, address: 00000000000003c0 [...] Oops: Oops: 0000 [#1] SMP CPU: 6 UID: 0 PID: 367 Comm: ping Not tainted 6.17.0-rc6-virtme-gb65678cacc03 #1 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.17.0-4.fc41 04/01/2014 RIP: 0010:fib_lookup_good_nhc+0x1e/0x80 [...] Call Trace: <TASK> fib_table_lookup+0x541/0x650 ip_route_output_key_hash_rcu+0x2ea/0x970 ip_route_output_key_hash+0x55/0x80 __ip4_datagram_connect+0x250/0x330 udp_connect+0x2b/0x60 __sys_connect+0x9c/0xd0 __x64_sys_connect+0x18/0x20 do_syscall_64+0xa4/0x2a0 entry_SYSCALL_64_after_hwframe+0x4b/0x53	N/A	More Details
CVE-2025-62249	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q3.0 through 2025.Q3.2, 2025.Q2.0 through 2025.Q2.12, 2025.Q1.0 through 2025.Q1.17, 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.Q1.20, and 2023.Q4.0 through 2023.Q4.10 allows an remote non-authenticated attacker to inject JavaScript into the google_gadget.	N/A	More Details
CVE-2025-39979	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: fs, fix UAF in flow counter release Fix a kernel trace [1] caused by releasing an HWS action of a local flow counter in mlx5_cmd_hws_delete_fte(), where the HWS action refcount and mutex were not initialized and the counter struct could already be freed when deleting the rule. Fix it by adding the missing initializations and adding refcount for the local flow counter struct. [1] Kernel log: Call Trace: <TASK> dump_stack_lvl+0x34/0x48 mlx5_fs_put_hws_action.part.0.cold+0x21/0x94 [mlx5_core] mlx5_fc_put_hws_action+0x96/0xad [mlx5_core] mlx5_fs_destroy_fs_actions+0x8b/0x152 [mlx5_core] mlx5_cmd_hws_delete_fte+0x5a/0xa0 [mlx5_core] del_hw_fte+0x1ce/0x260 [mlx5_core] mlx5_del_flow_rules+0x12d/0x240 [mlx5_core] ? ttwu_queue_wakelist+0xf4/0x110 mlx5_ib_destroy_flow+0x103/0x1b0 [mlx5_ib] uverbs_free_flow+0x20/0x50 [ib_uverbs] destroy_hw_idr_uobject+0x1b/0x50 [ib_uverbs] uverbs_destroy_uobject+0x34/0x1a0 [ib_uverbs] uobj_destroy+0x3c/0x80 [ib_uverbs] ib_uverbs_run_method+0x23e/0x360 [ib_uverbs] ? uverbs_finalize_object+0x60/0x60 [ib_uverbs] ib_uverbs_cmd_verbs+0x14f/0x2c0 [ib_uverbs] ? do_tty_write+0x1a9/0x270 ? file_tty_write.constprop.0+0x98/0xc0 ? new_sync_write+0xfc/0x190 ib_uverbs_ioctl+0xd7/0x160 [ib_uverbs] __x64_sys_ioctl+0x87/0xc0 do_syscall_64+0x59/0x90	N/A	More Details
CVE-2025-39978	In the Linux kernel, the following vulnerability has been resolved: octeontx2-pf: Fix potential use after free in otx2_tc_add_flow() This code calls kfree_rcu(new_node, rcu) and then dereferences "new_node" and then dereferences it on the next line. Two lines later, we take a mutex so I don't think this is an RCU safe region. Re-order it to do the dereferences before queuing up the free.	N/A	More Details
CVE-2025-39977	In the Linux kernel, the following vulnerability has been resolved: futex: Prevent use-after-free during requeue-PI syzbot managed to trigger the following race: T1 T2 futex_wait_requeue_pi() futex_do_wait() schedule() futex_requeue() futex_proxy_trylock_atomic() futex_requeue_pi_prepare() requeue_pi_wake_futex() futex_requeue_pi_complete() /* preempt */ * timeout/ signal wakes T1 * futex_requeue_pi_wakeup_sync() // Q_REQUEUE_PI_LOCKED futex_hash_put() // back to userland, on stack futex_q is garbage /* back */ wake_up_state(q->task, TASK_NORMAL); In this scenario futex_wait_requeue_pi() is able to leave without using futex_q::lock_ptr for synchronization. This can be prevented by reading futex_q::task before updating the futex_q::requeue_state. A reference on the task_struct is not needed because requeue_pi_wake_futex() is invoked with a spinlock_t held which implies a RCU read section. Even if T1 terminates immediately after, the task_struct will remain valid during T2's wake_up_state(). A READ_ONCE on futex_q::task before futex_requeue_pi_complete() is enough because it ensures that the variable is read before the state is updated. Read futex_q::task before updating the requeue state, use it for the following wakeup.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: futex: Use correct exit on failure from futex_hash_allocate_default() copy_process() uses the wrong error exit path from		

CVE-2025-39976	futex_hash_allocate_default(). After exiting from futex_hash_allocate_default(), neither tasklist_lock nor siglock has been acquired. The exit label bad_fork_core_free unlocks both of these locks which is wrong. The next exit label, bad_fork_cancel_cgroup, is the correct exit. sched_cgroup_fork() did not allocate any resources that need to freed. Use bad_fork_cancel_cgroup on error exit from futex_hash_allocate_default().	N/A	More Details
CVE-2025-7851	An attacker may obtain the root shell on the underlying OS system with the restricted conditions on Omada gateways.	N/A	More Details
CVE-2025-40006	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: fix folio is still mapped when deleted Migration may be raced with fallocating hole. remove_inode_single_folio will unmap the folio if the folio is still mapped. However, it's called without folio lock. If the folio is migrated and the mapped pte has been converted to migration entry, folio_mapped() returns false, and won't unmap it. Due to extra refcount held by remove_inode_single_folio, migration fails, restores migration entry to normal pte, and the folio is mapped again. As a result, we triggered BUG in filemap_unaccount_folio. The log is as follows: BUG: Bad page cache in process hugetlb pfn:156c00 page: refcount:515 mapcount:0 mapping:0000000099fef6e1 index:0x0 pfn:0x156c00 head: order:9 mapcount:1 entire_mapcount:1 nr_pages_mapped:0 pincount:0 aops:hugetlbfs_aops ino:dcc dentry name(?):"my_hugepage_file" flags: 0x17ffffc00000c1(locked|waiters|head|node=0|zone=2|lastcpupid=0x1fffff) page_type: f4(hugetlb) page dumped because: still mapped when deleted CPU: 1 UID: 0 PID: 395 Comm: hugetlb Not tainted 6.17.0-rc5-00044-g7aac71907bde-dirty #484 NONE Hardware name: QEMU Ubuntu 24.04 PC (i440FX + PIIX, 1996), BIOS 0.0.0 02/06/2015 Call Trace: <TASK> dump_stack_lvl+0x4f/0x70 filemap_unaccount_folio+0xc4/0x1c0 __filemap_remove_folio+0x38/0x1c0 filemap_remove_folio+0x41/0xd0 remove_inode_hugepages+0x142/0x250 hugetlbfs_fallocate+0x471/0x5a0 vfs_fallocate+0x149/0x380 Hold folio lock before checking if the folio is mapped to avold race with migration.	N/A	More Details
CVE-2025-6542	An arbitrary OS command may be executed on the product by a remote unauthenticated attacker.	N/A	More Details
CVE-2025-58115	ChatLuck contains a cross-site scripting vulnerability in Guest User Sign-up. If exploited, an arbitrary script may be executed on the web browser of the user who is accessing the product.	N/A	More Details
CVE-2025-8414	Due to improper input validation, a buffer overflow vulnerability is present in Zigbee EZSP Host Applications. If the buffer overflows, stack corruption is possible. In certain conditions, this could lead to arbitrary code execution. Access to a network key is required to exploit this vulnerability.	N/A	More Details
CVE-2025-52583	Reflected cross-site scripting (XSS) vulnerability in desknet's Web Server allows execution of arbitrary JavaScript in a user’s web browser.	N/A	More Details
CVE-2025-54760	Stored cross-site scripting (XSS) vulnerability in desknet's NEO V9.0R2.0 and earlier allow execution of arbitrary JavaScript in a user’s web browser.	N/A	More Details
CVE-2025-58747	Dify is an LLM application development platform. In Dify versions through 1.9.1, the MCP OAuth component is vulnerable to cross-site scripting when a victim connects to an attacker-controlled remote MCP server. The vulnerability exists in the OAuth flow implementation where the authorization_url provided by a remote MCP server is directly passed to window.open without validation or sanitization. An attacker can craft a malicious MCP server that returns a JavaScript URI (such as javascript:alert(1)) in the authorization_url field, which is then executed when the victim attempts to connect to the MCP server. This allows the attacker to execute arbitrary JavaScript in the context of the Dify application.	N/A	More Details
CVE-2025-26625	Git LFS is a Git extension for versioning large files. In Git LFS versions 0.5.2 through 3.7.0, when populating a Git repository's working tree with the contents of Git LFS objects, certain Git LFS commands may write to files visible outside the current Git working tree if symbolic or hard links exist which collide with the paths of files tracked by Git LFS. The git lfs checkout and git lfs pull commands do not check for symbolic links before writing to files in the working tree, allowing an attacker to craft a repository containing symbolic or hard links that cause Git LFS to write to arbitrary file system locations accessible to the user running these commands. As well, when the git lfs checkout and git lfs pull commands are run in a bare repository, they could write to files visible outside the repository. The vulnerability is fixed in version 3.7.1. As a workaround, support for symlinks in Git may be disabled by setting the core.symlinks configuration option to false, after which further clones and fetches will not create symbolic links. However, any symbolic or hard links in existing repositories will still provide the opportunity for Git LFS to write to their targets.	N/A	More Details
CVE-2025-54859	Stored cross-site scripting (XSS) vulnerability in desknet's NEO V9.0R2.0 and earlier allow execution of arbitrary JavaScript in a user’s web browser.	N/A	More Details
CVE-	In NextX Duo before 6.4.4, in the HTTP client module, the network support code for Eclipse Foundation		More

2025-55085	ThreadX, the parsing of HTTP header fields was missing bounds verification. A crafted server response could cause undefined behavior.	N/A	Details
CVE-2025-55072	Stored cross-site scripting (XSS) vulnerability in desknet's NEO V2.0R1.0 to V9.0R2.0 allow execution of arbitrary JavaScript in a user’s web browser.	N/A	More Details
CVE-2025-58079	Improper Protection of Alternate Path (CWE-424) in the AppSuite of desknet's NEO V4.0R1.0 to V9.0R2.0 allows an attacker to create malicious AppSuite applications.	N/A	More Details
CVE-2025-58426	desknet's NEO V4.0R1.0 to V9.0R2.0 contains a hard-coded cryptographic key, which allows an attacker to create malicious AppSuite applications.	N/A	More Details
CVE-2025-6338	There is an incomplete cleanup vulnerability in Qt Network's Schannel support on Windows which can lead to a Denial of Service over a long period.This issue affects Qt from 5.15.0 through 6.8.3, from 6.9.0 before 6.9.2.	N/A	More Details
CVE-2025-3930	Strapi uses JSON Web Tokens (JWT) for authentication. After logout or account deactivation, the JWT is not invalidated, which allows an attacker who has stolen or intercepted the token to freely reuse it until its expiration date (which is set to 30 days by default, but can be changed). The existence of /admin/renew-token endpoint allows anyone to renew near-expiration tokens indefinitely, further increasing the impact of this attack. This issue has been fixed in version 5.24.1.	N/A	More Details
CVE-2025-55100	In USBX before 6.4.3, the USB support module for Eclipse Foundation ThreadX, there was a potential out of bound read issue in _ux_host_class_audio10_sam_parse_func() when parsing a list of sampling frequencies.	N/A	More Details
CVE-2025-55099	In USBX before 6.4.3, the USB support module for Eclipse Foundation ThreadX, there was a potential out of bound read issue in _ux_host_class_audio_alternate_setting_locate() when parsing a descriptor with attacker-controlled frequency fields.	N/A	More Details
CVE-2025-55098	In USBX before 6.4.3, the USB support module for Eclipse Foundation ThreadX, there was a potential out of bound read issue in _ux_host_class_audio_device_type_get() when parsing a descriptor of an USB audio device.	N/A	More Details
CVE-2025-24833	Stored cross-site scripting (XSS) vulnerability in desknet's NEO versions V4.0R1.0–V9.0R2.0 allow execution of arbitrary JavaScript in a user’s web browser.	N/A	More Details
CVE-2025-62419	DataEase is a data visualization and analytics platform. In DataEase versions through 2.10.13, a JDBC URL injection vulnerability exists in the DB2 and MongoDB data source configuration handlers. In the DB2 data source handler, when the extraParams field is empty, the HOSTNAME, PORT, and DATABASE values are directly concatenated into the JDBC URL without filtering illegal parameters. This allows an attacker to inject a malicious JDBC string into the HOSTNAME field to bypass previously patched vulnerabilities CVE-2025-57773 and CVE-2025-58045. The vulnerability is fixed in version 2.10.14. No known workarounds exist.	N/A	More Details
CVE-2025-6541	An arbitrary OS command may be executed on the product by the user who can log in to the web management interface.	N/A	More Details
CVE-2025-62420	DataEase is a data visualization and analytics platform. In DataEase versions through 2.10.13, a JDBC driver bypass vulnerability exists in the H2 database connection handler. The getJdbc function in H2.java checks if the jdbcUrl starts with jdbc:h2 but returns a separate jdbc field as the actual connection URL. An attacker can provide a jdbcUrl that starts with jdbc:h2 while supplying a different jdbc field with an arbitrary JDBC driver and connection string. This allows an authenticated attacker to trigger arbitrary JDBC connections with malicious drivers, potentially leading to remote code execution. The vulnerability is fixed in version 2.10.14. No known workarounds exist.	N/A	More Details
CVE-2025-62632	Rejected reason: Not used	N/A	More Details
CVE-2025-62655	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in The Wikimedia Foundation MediaWiki Cargo extension allows SQL Injection.This issue affects MediaWiki Cargo extension: 1.39, 1.43, 1.44.	N/A	More Details
CVE-2025-62654	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation MediaWiki QuizGame extension allows Stored XSS.This issue affects MediaWiki QuizGame extension: 1.39, 1.43, 1.44.	N/A	More Details
CVE-	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in		

2025-62653	The Wikimedia Foundation MediaWiki PollNY extension allows Stored XSS.This issue affects MediaWiki PollNY extension: 1.39, 1.43, 1.44.	N/A	More Details
CVE-2025-62652	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation MediaWiki WebAuthn extension allows Stored XSS.This issue affects MediaWiki WebAuthn extension: 1.39, 1.43, 1.44.	N/A	More Details
CVE-2025-58778	Multiple versions of RG-EST300 provided by Ruijie Networks provide SSH server functionality. It is not documented in the manual, and enabled in the initial configuration. Anyone with the knowledge of the related credentials can log in to the affected device, leading to information disclosure, altering the system configurations, or causing a denial of service (DoS) condition.	N/A	More Details
CVE-2025-55089	In FileX before 6.4.2, the file support module for Eclipse Foundation ThreadX, there was a possible buffer overflow in the FileX RAM disk driver. It could cause a remote execurtion after receiving a crafted sequence of packets	N/A	More Details
CVE-2025-41019	SQL injection in Sergestec's SISTICK v7.2. This vulnerability allows an attacker to retrieve, create, update, and delete databases through the 'id' parameter in '/index.php?view=ticket_detail'.	N/A	More Details
CVE-2025-11925	Incorrect Content-Type header in one of the APIs (`text/html` instead of `application/json`) replies may potentially allow injection of HTML/JavaScript into reply.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-34282	ThingsBoard versions < 4.2.1 contain a server-side request forgery (SSRF) vulnerability in the dashboard's Image Upload Gallery feature. An attacker can upload a malicious SVG file that references a remote URL. If the server processes the SVG file in a way that parses external references, it may initiate unintended outbound requests. This can be used to access internal services or resources.	N/A	More Details
CVE-2025-34281	ThingsBoard versions < 4.2.1 contain a stored cross-site scripting (XSS) vulnerability in the dashboard's Image Upload Gallery feature. An attacker can upload an SVG file containing malicious JavaScript, which may be executed when the file is rendered in the UI. This issue results from insufficient sanitization and improper content-type validation of uploaded SVG files.	N/A	More Details
CVE-2025-53858	ChatLuck contains a cross-site scripting vulnerability in Chat Rooms. If exploited, an arbitrary script may be executed on the web browser of the user who is accessing the product.	N/A	More Details
CVE-2025-54461	ChatLuck contains an insufficient granularity of access control vulnerability in Invitation of Guest Users. If exploited, an uninvited guest user may register itself as a guest user.	N/A	More Details
CVE-2025-62422	DataEase is an open source data visualization and analytics platform. In versions 2.10.13 and earlier, the /de2api/datasetData/tableField interface is vulnerable to SQL injection. An attacker can construct a malicious tableName parameter to execute arbitrary SQL commands. This issue is fixed in version 2.10.14. No known workarounds exist.	N/A	More Details
CVE-2025-62421	DataEase is a data visualization and analytics platform. In DataEase versions through 2.10.13, a stored cross-site scripting vulnerability exists due to improper file upload validation and authentication bypass. The StaticResourceApi interface defines a route upload/{fileId} that uses a URL path parameter where both the filename and extension of uploaded files are controllable by users. During permission validation, the TokenFilter invokes the WhitelistUtils#match method to determine if the URL path is in the allowlist. If the requestURI ends with .js or similar extensions, it is directly deemed safe and bypasses permission checks. This allows an attacker to access "upload/1.js" while specifying arbitrary file extensions, enabling the upload of HTML files containing malicious JavaScript. The vulnerability is fixed in version 2.10.14. No known workarounds exist.	N/A	More Details
CVE-2025-55097	In USBX before 6.4.3, the USB support module for Eclipse Foundation ThreadX, there was a potential out of bound read issue in _ux_host_class_audio_streaming_sampling_get() when parsing a descriptor of an USB streaming device.	N/A	More Details
CVE-2025-55096	In USBX before 6.4.3, the USB support module for Eclipse Foundation ThreadX, there was a potential out of bound read issue in _ux_host_class_hid_report_descriptor_get() when parsing a descriptor of an USB HID device.	N/A	More Details
CVE-2025-55094	In NetX Duo before 6.4.4, the networking support module for Eclipse Foundation ThreadX, there was a potential out of bound read issue in _nx_icmpv6_validate_options() when handling a packet with ICMP6 options.	N/A	More Details
CVE-2025-55087	In NextX Duo's snmp addon versions before 6.4.4, a part of the Eclipse Foundation ThreadX, an attacker could cause an out-of-bound read by a crafted SNMPv3 security parameters.	N/A	More Details

CVE-2025-11854	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2025-22381. Reason: This candidate is a reservation duplicate of CVE-2025-22381. Notes: All CVE users should reference CVE-2025-22381 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-25298	Strapi is an open source headless CMS. The @strapi/core package before version 5.10.3 does not enforce a maximum password length when using bcryptjs for password hashing. Bcryptjs ignores any bytes beyond 72, so passwords longer than 72 bytes are silently truncated. A user can create an account with a password exceeding 72 bytes and later authenticate with only the first 72 bytes. This reduces the effective entropy of overlong passwords and may mislead users who believe characters beyond 72 bytes are required, creating a low likelihood of unintended authentication if an attacker can obtain or guess the truncated portion. Long over-length inputs can also impose unnecessary processing overhead. The issue is fixed in version 5.10.3. No known workarounds exist.	N/A	More Details
CVE-2025-34255	D-Link Nuclias Connect firmware versions <= 1.3.1.4 contain an observable response discrepancy vulnerability. The application's 'Forgot Password' endpoint returns distinct JSON responses depending on whether the supplied email address is associated with an existing account. Because the responses differ in the `data.exist` boolean value, an unauthenticated remote attacker can enumerate valid email addresses/accounts on the server. NOTE: D-Link states that a fix is under development.	N/A	More Details
CVE-2025-34254	D-Link Nuclias Connect firmware versions <= 1.3.1.4 contain an observable response discrepancy vulnerability. The application's 'Login' endpoint returns distinct JSON responses depending on whether the supplied username is associated with an existing account. Because the responses differ in the `error.message`string value, an unauthenticated remote attacker can enumerate valid usernames/accounts on the server. NOTE: D-Link states that a fix is under development.	N/A	More Details
CVE-2025-34253	D-Link Nuclias Connect firmware versions <= 1.3.1.4 contain a stored cross-site scripting (XSS) vulnerability due to improper sanitization of the 'Network' field when editing the configuration, creating a profile, and adding a network. An authenticated attacker can inject arbitrary JavaScript to be executed in the context of other users viewing the profile entry. NOTE: D-Link states that a fix is under development.	N/A	More Details
CVE-2025-34512	Ilevia EVE X1 Server firmware versions ≤ 4.7.18.0.eden contain a reflected cross-site scripting (XSS) vulnerability in index.php that allows an unauthenticated attacker to execute arbitrary code. Ilevia has declined to service this vulnerability, and recommends that customers not expose port 8080 to the internet.	N/A	More Details
CVE-2025-62409	Envoy is a cloud-native, open source edge and service proxy. Prior to 1.36.1, 1.35.5, 1.34.9, and 1.33.10, large requests and responses can potentially trigger TCP connection pool crashes due to flow control management in Envoy. It will happen when the connection is closing but upstream data is still coming, resulting in a buffer watermark callback nullptr reference. The vulnerability impacts TCP proxy and HTTP 1 & 2 mixed use cases based on ALPN. This vulnerability is fixed in 1.36.1, 1.35.5, 1.34.9, and 1.33.10.	N/A	More Details
CVE-2025-34513	Ilevia EVE X1 Server firmware versions ≤ 4.7.18.0.eden contain an OS command injection vulnerability in mbus_build_from_csv.php that allows an unauthenticated attacker to execute arbitrary code. Ilevia has declined to service this vulnerability, and recommends that customers not expose port 8080 to the internet.	N/A	More Details
CVE-2025-61909	Icinga 2 is an open source monitoring system. From 2.10.0 to before 2.15.1, 2.14.7, and 2.13.13, the safe-reload script (also used during systemctl reload icinga2) and logrotate configuration shipped with Icinga 2 read the PID of the main Icinga 2 process from a PID file writable by the daemon user, but send the signal as the root user. This can allow the Icinga user to send signals to processes it would otherwise not permitted to. A fix is included in the following Icinga 2 versions: 2.15.1, 2.14.7, and 2.13.13.	N/A	More Details
CVE-2025-61908	Icinga 2 is an open source monitoring system. From 2.10.0 to before 2.15.1, 2.14.7, and 2.13.13, when creating an invalid reference, such as a reference to null, dereferencing results in a segmentation fault. This can be used by any API user with access to an API endpoint that allows specifying a filter expression to crash the Icinga 2 daemon. A fix is included in the following Icinga 2 versions: 2.15.1, 2.14.7, and 2.13.13.	N/A	More Details
CVE-2025-61907	Icinga 2 is an open source monitoring system. In Icinga 2 versions 2.4 through 2.15.0, filter expressions provided to the various /v1/objects endpoints could access variables or objects that would otherwise be inaccessible for the user. This allows authenticated API users to learn information that should be hidden from them, including global variables not permitted by the variables permission and objects not permitted by the corresponding objects/query permissions. The vulnerability is fixed in versions 2.15.1, 2.14.7, and 2.13.13.	N/A	More Details
CVE-2025-34514	Ilevia EVE X1 Server firmware versions ≤ 4.7.18.0.eden contain authenticated OS command injection vulnerabilities in multiple web-accessible PHP scripts that call exec() and allow an authenticated attacker to execute arbitrary commands. Ilevia has declined to service this vulnerability, and recommends that customers not expose port 8080 to the internet.	N/A	More Details
CVE-2025-34515	Ilevia EVE X1 Server firmware versions ≤ 4.7.18.0.eden contain an execution with unnecessary privileges vulnerability in sync_project.sh that allows an attacker to escalate privileges to root. Ilevia has declined to service this vulnerability, and recommends that customers not expose port 8080 to the internet.	N/A	More Details
CVE-	Ilevia EVE X1 Server firmware versions ≤ 4.7.18.0.eden contain a use of default credentials vulnerability that		

2025-34516	allows an unauthenticated attacker to obtain remote access. Ilevia has declined to service this vulnerability, and recommends that customers not expose port 8080 to the internet.	N/A	More Details
CVE-2025-34519	Ilevia EVE X1 Server firmware versions ≤ 4.7.18.0.eden contain an insecure hashing algorithm vulnerability. The product stores passwords using the MD5 hash function without applying a per-password salt. Because MD5 is a fast, unsalted hash, an attacker who obtains the password database can efficiently perform offline dictionary, rainbow-table, or brute-force attacks to recover the original passwords. Ilevia has declined to service this vulnerability, and recommends that customers not expose port 8080 to the internet.	N/A	More Details
CVE-2025-62496	A vulnerability exists in the QuickJS engine's BigInt string parsing logic (js_bigint_from_string) when attempting to create a BigInt from a string with an excessively large number of digits. The function calculates the necessary number of bits (n_bits) required to store the BigInt using the formula: $$\text{n\_bits} = (\text{n\_digits} \times 27 + 7) / 8 \quad (\text{for radix 10})$$ * For large input strings (e.g., $79,536,432$ digits or more for base 10), the intermediate calculation $(\text{n\_digits} \times 27 + 7)$ exceeds the maximum value of a standard signed 32-bit integer, resulting in an Integer Overflow. * The resulting n_bits value becomes unexpectedly small or even negative due to this wrap-around. * This flawed n_bits is then used to compute n_limbs, the number of memory "limbs" needed for the BigInt object. Since n_bits is too small, the calculated n_limbs is also significantly underestimated. * The function proceeds to allocate a JSBigInt object using this underestimated n_limbs. * When the function later attempts to write the actual BigInt data into the allocated object, the small buffer size is quickly exceeded, leading to a Heap Out-of-Bounds Write as data is written past the end of the allocated r->tab array.	N/A	More Details
CVE-2025-62495	An integer overflow vulnerability exists in the QuickJS regular expression engine (libregexp) due to an inconsistent representation of the bytecode buffer size. * The regular expression bytecode is stored in a DynBuf structure, which correctly uses a size_t (an unsigned type, typically 64-bit) for its size member. * However, several functions, such as re_emit_op_u32 and other internal parsing routines, incorrectly cast or store this DynBuf size_t value into a signed int (typically 32-bit). * When a large or complex regular expression (such as those generated by a recursive pattern in a Proof-of-Concept) causes the bytecode size to exceed 2^{31} bytes (the maximum positive value for a signed 32-bit integer), the size value wraps around, resulting in a negative integer when stored in the int variable (Integer Overflow). * This negative value is subsequently used in offset calculations. For example, within functions like re_parse_disjunction, the negative size is used to compute an offset (pos) for patching a jump instruction. * This negative offset is then incorrectly added to the buffer pointer (s->byte_code.buf + pos), leading to an out-of-bounds write on the first line of the snippet below: put_u32(s->byte_code.buf + pos, len);	N/A	More Details
CVE-2025-62417	Bagisto is an open source laravel eCommerce platform. When product data that begins with a spreadsheet formula character (for example =, +, -, or @) is accepted and later exported or saved into a CSV and opened in spreadsheet software, the spreadsheet will interpret that cell as a formula. This allows an attacker to supply a CSV field (e.g., product name) that contains a formula which may be evaluated by a victim’s spreadsheet application — potentially leading to data exfiltration and remote command execution (via older Excel exploits / OLE/cmd constructs or Excel macros). This vulnerability is fixed in 2.3.8.	N/A	More Details
CVE-2025-6892	An Incorrect Authorization vulnerability has been identified in Moxa’s network security appliances and routers. A flaw in the API authentication mechanism allows unauthorized access to protected API endpoints, including those intended for administrative functions. This vulnerability can be exploited after a legitimate user has logged in, as the system fails to properly validate session context or privilege boundaries. An attacker may leverage this flaw to perform unauthorized privileged operations. While successful exploitation can severely impact the confidentiality, integrity, and availability of the affected device itself, there is no loss of confidentiality or integrity within any subsequent systems.	N/A	More Details
CVE-2025-55093	In NetX Duo before 6.4.4, the networking support module for Eclipse Foundation ThreadX, there was a potential out of bound read issue in _nx_ipv4_packet_receive() when handling unicast DHCP messages that could cause corruption of 4 bytes of memory.	N/A	More Details
CVE-2025-55092	In Eclipse Foundation NetX Duo before 6.4.4, the networking support module for Eclipse Foundation ThreadX, there was a potential out of bound read issue in _nx_ipv4_option_process() when processing an IPv4 packet with the timestamp option.	N/A	More Details
CVE-2025-6950	An Use of Hard-coded Credentials vulnerability has been identified in Moxa’s network security appliances and routers. The system employs a hard-coded secret key to sign JSON Web Tokens (JWT) used for authentication. This insecure implementation allows an unauthenticated attacker to forge valid tokens, thereby bypassing authentication controls and impersonating any user. Exploitation of this vulnerability can result in complete system compromise, enabling unauthorized access, data theft, and full administrative control over the affected device. While successful exploitation can severely impact the confidentiality, integrity, and availability of the affected device itself, there is no loss of confidentiality or integrity within any subsequent systems.	N/A	More Details
CVE-2025-	An Execution with Unnecessary Privileges vulnerability has been identified in Moxa’s network security appliances and routers. A critical authorization flaw in the API allows an authenticated, low-privileged user to create a new administrator account, including accounts with usernames identical to existing users. In certain scenarios, this vulnerability could allow an attacker to gain full administrative control over the affected	N/A	More Details

6949	device, leading to potential account impersonation. While successful exploitation can severely impact the confidentiality, integrity, and availability of the affected device itself, there is no loss of confidentiality or integrity within any subsequent systems.		
CVE-2025-6894	An Execution with Unnecessary Privileges vulnerability has been identified in Moxa’s network security appliances and routers. A flaw in the API authorization logic of the affected device allows an authenticated, low-privileged user to execute the administrative `ping` function, which is restricted to higher-privileged roles. This vulnerability enables the user to perform internal network reconnaissance, potentially discovering internal hosts or services that would otherwise be inaccessible. Repeated exploitation could lead to minor resource consumption. While the overall impact is limited, it may result in some loss of confidentiality and availability on the affected device. There is no impact on the integrity of the device, and the vulnerability does not affect any subsequent systems.	N/A	More Details
CVE-2025-6893	An Execution with Unnecessary Privileges vulnerability has been identified in Moxa’s network security appliances and routers. A flaw in broken access control has been identified in the /api/v1/setting/data endpoint of the affected device. This flaw allows a low-privileged authenticated user to call the API without the required permissions, thereby gaining the ability to access or modify system configuration data. Successful exploitation may lead to privilege escalation, allowing the attacker to access or modify sensitive system settings. While the overall impact is high, there is no loss of confidentiality or integrity within any subsequent systems.	N/A	More Details
CVE-2025-11896	In Xpdf 4.05 (and earlier), a PDF object loop in a CMap, via the "UseCMap" entry, leads to infinite recursion and a stack overflow.	N/A	More Details
CVE-2025-62494	A type confusion vulnerability exists in the handling of the string addition (+) operation within the QuickJS engine. * The code first checks if the left-hand operand is a string. * It then attempts to convert the right-hand operand to a primitive value using JS_ToPrimitiveFree. This conversion can trigger a callback (e.g., toString or valueOf). * During this callback, an attacker can modify the type of the left-hand operand in memory, changing it from a string to a different type (e.g., an object or an array). * The code then proceeds to call JS_ConcatStringInPlace, which still treats the modified left-hand value as a string. This mismatch between the assumed type (string) and the actual type allows an attacker to control the data structure being processed by the concatenation logic, resulting in a type confusion condition. This can lead to out-of-bounds memory access, potentially resulting in memory corruption and arbitrary code execution in the context of the QuickJS runtime.	N/A	More Details
CVE-2025-62490	In quickjs, in js_print_object, when printing an array, the function first fetches the array length and then loops over it. The issue is, printing a value is not side-effect free. An attacker-defined callback could run during js_print_value, during which the array could get resized and len1 become out of bounds. This results in a use-after-free.A second instance occurs in the same function during printing of a map or set objects. The code iterates over ms->records list, but once again, elements could be removed from the list during js_print_value call.	N/A	More Details
CVE-2025-62491	A Use-After-Free (UAF) vulnerability exists in the QuickJS engine's standard library when iterating over the global list of unhandled rejected promises (ts->rejected_promise_list). * The function js_std_promise_rejection_check attempts to iterate over the rejected_promise_list to report unhandled rejections using a standard list loop. * The reason for a promise rejection is processed inside the loop, including calling js_std_dump_error1(ctx, rp->reason). * If the promise rejection reason is an Error object that defines a custom property getter (e.g., via Object.defineProperty), this getter is executed during the error dumping process. * The malicious custom getter can execute JavaScript code that calls catch() on the same rejected promise being processed. * Calling catch() internally triggers js_std_promise_rejection_tracker, which then removes and frees the current promise entry (JSRejectedPromiseEntry) from the rejected_promise_list. * Since the list iteration continues using the now-freed memory pointer (el), the subsequent loop access results in a Use-After-Free condition.	N/A	More Details
CVE-2025-62428	Drawing-Captcha APP provides interactive, engaging verification for Web-Based Applications. The vulnerability is a Host Header Injection in the /register and /confirm-email endpoints. It allows an attacker to manipulate the Host header in HTTP requests to generate malicious email confirmation links. These links can redirect users to attacker-controlled domains. This vulnerability affects all users relying on email confirmation for account registration or verification. This vulnerability is fixed in 1.2.5-alpha-patch.	N/A	More Details
CVE-2025-62427	The Angular SSR is a server-rise rendering tool for Angular applications. The vulnerability is a Server-Side Request Forgery (SSRF) flaw within the URL resolution mechanism of Angular's Server-Side Rendering package (@angular/ssr) before 19.2.18, 20.3.6, and 21.0.0-next.8. The function createRequestUrl uses the native URL constructor. When an incoming request path (e.g., originalUrl or url) begins with a double forward slash (//) or backslash (\\), the URL constructor treats it as a schema-relative URL. This behavior overrides the security-intended base URL (protocol, host, and port) supplied as the second argument, instead resolving the URL against the scheme of the base URL but adopting the attacker-controlled hostname. This allows an attacker to specify an external domain in the URL path, tricking the Angular SSR environment into setting the page's virtual location (accessible via DOCUMENT or PlatformLocation tokens) to this attacker-controlled domain. Any subsequent relative HTTP requests made during the SSR process (e.g., using	N/A	More Details

	HttpClient.get('assets/data.json')) will be incorrectly resolved against the attacker's domain, forcing the server to communicate with an arbitrary external endpoint. This vulnerability is fixed in 19.2.18, 20.3.6, and 21.0.0-next.8.		
CVE-2025-62492	A vulnerability stemming from floating-point arithmetic precision errors exists in the QuickJS engine's implementation of TypedArray.prototype.indexOf() when a negative fromIndex argument is supplied. * The fromIndex argument (read as a double variable, d) is used to calculate the starting position for the search. * If d is negative, the index is calculated relative to the end of the array by adding the array's length (len) to d: $$d_{new} = d + \text{len}$$ * Due to the inherent limitations of floating-point arithmetic, if the negative value d is extremely small (e.g., -1×10^{-20}), the addition $d + \text{len}$ can result in a loss of precision, yielding an outcome that is exactly equal to len. * The result is then converted to an integer index k: $k = \text{len}$. * The search function proceeds to read array elements starting from index k. Since valid indices are 0 to $\text{len}-1$, starting the read at index len is one element past the end of the array. This allows an attacker to cause an Out-of-Bounds Read of one element immediately following the buffer. While the scope of this read is small (one element), it can potentially lead to Information Disclosure of adjacent memory contents, depending on the execution environment.	N/A	More Details
CVE-2025-62493	A vulnerability exists in the QuickJS engine's BigInt string conversion logic (js_bigint_to_string1) due to an incorrect calculation of the required number of digits, which in turn leads to reading memory past the allocated BigInt structure. * The function determines the number of characters (n_digits) needed for the string representation by calculating: $$ \\ \text{n\_digits} = (\text{n\_bits} + \text{log2\_radix} - 1) / \text{log2\_radix}$$ $$$$This formula is off-by-one in certain edge cases when calculating the necessary memory limbs. For instance, a 127-bit BigInt using radix 32 (where $\text{log2\_radix}=5$) is calculated to need $\text{n\_digits}=26$. * The maximum number of bits actually stored is $\text{n\_bits}=127$, which requires only two 64-bit limbs ($\text{JS\_LIMB\_BITS}=64$). * The conversion loop iterates $\text{n\_digits}=26$ times, attempting to read 5 bits in each iteration, totaling $26 \times 5 = 130$ bits. * In the final iterations of the loop, the code attempts to read data that spans two limbs: C c = (r->tab[pos] >> shift) | (r->tab[pos + 1] << (JS_LIMB_BITS - shift)); * Since the BigInt was only allocated two limbs, the read operation for r->tab[pos + 1] becomes an Out-of-Bounds Read when pos points to the last valid limb (e.g., $pos=1$). This vulnerability allows an attacker to cause the engine to read and process data from the memory immediately following the BigInt buffer. This can lead to Information Disclosure of sensitive data stored on the heap adjacent to the BigInt object.	N/A	More Details
CVE-2025-62633	Rejected reason: Not used	N/A	More Details
CVE-2025-62634	Rejected reason: Not used	N/A	More Details
CVE-2025-62635	Rejected reason: Not used	N/A	More Details
CVE-2025-11680	Out-of-bounds Write in unfilter_scanline in warmcat libwebsockets allows, when the LWS_WITH_UPNG flag is enabled during compilation and the HTML display stack is used, to write past a heap allocated buffer possibly causing a crash, when the user visits an attacker controlled website that contains a crafted PNG file with a big width value that causes an integer overflow which value is used for determining the size of a heap allocation.	N/A	More Details
CVE-2025-47900	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Microchip Time Provider 4100 allows OS Command Injection.This issue affects Time Provider 4100: before 2.5.	N/A	More Details
CVE-2025-55081	In Eclipse Foundation NextX Duo before 6.4.4, a module of ThreadX, the _nx_secure_tls_process_clienthello() function was missing length verification of certain SSL/TLS client hello message: the ciphersuite length and compression method length. In case of an attacker-crafted message with values outside of the expected range, it could cause an out-of-bound read.	N/A	More Details
CVE-2025-40017	In the Linux kernel, the following vulnerability has been resolved: media: iris: Fix memory leak by freeing untracked persist buffer One internal buffer which is allocated only once per session was not being freed during session close because it was not being tracked as part of internal buffer list which resulted in a memory leak. Add the necessary logic to explicitly free the untracked internal buffer during session close to ensure all allocated memory is released properly.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: media: uvcvideo: Mark invalid entities with id UVC_INVALID_ENTITY_ID Per UVC 1.1+ specification 3.7.2, units and terminals must have a non-zero unique ID. ``` Each Unit and Terminal within the video function is assigned a unique identification number, the Unit ID (UID) or Terminal ID (TID), contained in the bUnitID or bTerminalID field of the descriptor. The value 0x00 is reserved for undefined ID, ``` If we add a new entity with id 0 or a duplicated ID, it will be marked as UVC_INVALID_ENTITY_ID. In a previous attempt commit 3dd075fe8ebb ("media: uvcvideo: Require		

CVE-2025-40016	entities to have a non-zero unique ID"), we ignored all the invalid units, this broke a lot of non-compatible cameras. Hopefully we are more lucky this time. This also prevents some syzkaller reproducers from triggering warnings due to a chain of entities referring to themselves. In one particular case, an Output Unit is connected to an Input Unit, both with the same ID of 1. But when looking up for the source ID of the Output Unit, that same entity is found instead of the input entity, which leads to such warnings. In another case, a backward chain was considered finished as the source ID was 0. Later on, that entity was found, but its pads were not valid. Here is a sample stack trace for one of those cases. [20.650953] usb 1-1: new high-speed USB device number 2 using dummy_hcd [20.830206] usb 1-1: Using ep0 maxpacket: 8 [20.833501] usb 1-1: config 0 descriptor?? [21.038518] usb 1-1: string descriptor 0 read error: -71 [21.038893] usb 1-1: Found UVC 0.00 device <unnamed> (2833:0201) [21.039299] uvcvideo 1-1:0.0: Entity type for entity Output 1 was not initialized! [21.041583] uvcvideo 1-1:0.0: Entity type for entity Input 1 was not initialized! [21.042218] ----------[cut here]------------ [21.042536] WARNING: CPU: 0 PID: 9 at drivers/media/mc/mc-entity.c:1147 media_create_pad_link+0x2c4/0x2e0 [21.043195] Modules linked in: [21.043535] CPU: 0 UID: 0 PID: 9 Comm: kworker/0:1 Not tainted 6.11.0-rc7-00030-g3480e43aeccf #444 [21.044101] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.15.0-1 04/01/2014 [21.044639] Workqueue: usb_hub_wq hub_event [21.045100] RIP: 0010:media_create_pad_link+0x2c4/0x2e0 [21.045508] Code: fe e8 20 01 00 00 b8 f4 ff ff ff 48 83 c4 30 5b 41 5c 41 5d 41 5e 41 5f 5d c3 cc cc cc cc 0f 0b eb e9 0f 0b eb 0a 0f 0b eb 06 <0f> 0b eb 02 0f 0b b8 ea ff ff ff eb d4 66 2e 0f 1f 84 00 00 00 00 [21.046801] RSP: 0018:ffffc9000004b318 EFLAGS: 00010246 [21.047227] RAX: ffff888004e5d458 RBX: 0000000000000000 RCX: ffffffff818fccf1 [21.047719] RDX: 000000000000007b RSI: 0000000000000000 RDI: ffff888004313290 [21.048241] RBP: ffff888004313290 R08: 0001ffffffffffff R09: 0000000000000000 [21.048701] R10: 0000000000000013 R11: 0001888004313290 R12: 0000000000000003 [21.049138] R13: ffff888004313080 R14: ffff888004313080 R15: 0000000000000000 [21.049648] FS: 0000000000000000(0000) GS:ffff88803ec00000(0000) knlGS:0000000000000000 [21.050271] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [21.050688] CR2: 0000592cc27635b0 CR3: 000000000431c000 CR4: 0000000000750ef0 [21.051136] PKRU: 55555554 [21.051331] Call Trace: [21.051480] <TASK> [21.051611] ? __warn+0xc4/0x210 [21.051861] ? media_create_pad_link+0x2c4/0x2e0 [21.052252] ? report_bug+0x11b/0x1a0 [21.052540] ? trace_hardirqs_on+0x31/0x40 [21.052901] ? handle_bug+0x3d/0x70 [21.053197] ? exc_invalid_op+0x1a/0x50 [21.053511] ? asm_exc_invalid_op+0x1a/0x20 [21.053924] ? media_create_pad_link+0x91/0x2e0 [21.054364] ? media_create_pad_link+0x2c4/0x2e0 [21.054834] ? media_create_pad_link+0x91/0x2e0 [21.055131] ? _raw_spin_unlock+0x1e/0x40 [21.055441] ? __v4l2_device_register_subdev+0x202/0x210 [21.055837] uvc_mc_register_entities+0x358/0x400 [21.056144] uvc_register_chains+0x1 ---truncated---	N/A	More Details
CVE-2025-40015	In the Linux kernel, the following vulnerability has been resolved: media: stm32-csi: Fix dereference before NULL check In 'stm32_csi_start', 'csidev->s_subdev' is dereferenced directly while assigning a value to the 'src_pad'. However the same value is being checked against NULL at a later point of time indicating that there are chances that the value can be NULL. Move the dereference after the NULL check.	N/A	More Details
CVE-2025-40013	In the Linux kernel, the following vulnerability has been resolved: ASoC: qcom: audioreach: fix potential null pointer dereference It is possible that the topology parsing function audioreach_widget_load_module_common() could return NULL or an error pointer. Add missing NULL check so that we do not dereference it.	N/A	More Details
CVE-2025-40012	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix warning in smc_rx_splice() when calling get_page() smc_lo_register_dmb() allocates DMB buffers with kzalloc(), which are later passed to get_page() in smc_rx_splice(). Since kmalloc memory is not page-backed, this triggers WARN_ON_ONCE() in get_page() and prevents holding a refcount on the buffer. This can lead to use-after-free if the memory is released before splice_to_pipe() completes. Use folio_alloc() instead, ensuring DMBs are page-backed and safe for get_page(). WARNING: CPU: 18 PID: 12152 at ./include/linux/mm.h:1330 smc_rx_splice+0xaf8/0xe20 [smc] CPU: 18 UID: 0 PID: 12152 Comm: smcapp Kdump: loaded Not tainted 6.17.0-rc3-11705-g9cf4672ecfee #10 NONE Hardware name: IBM 3931 A01 704 (z/VM 7.4.0) Krnl PSW : 0704e00180000000 000793161032696c (smc_rx_splice+0xafc/0xe20 [smc]) R:0 T:1 IO:1 EX:1 Key:0 M:1 W:0 P:0 AS:3 CC:2 PM:0 RI:0 EA:3 Krnl GPRS: 0000000000000000 001cee80007d3001 00077400000000f8 0000000000000005 0000000000000001 001cee80007d3006 0007740000001000 001c000000000000 000000009b0c99e0 0000000000001000 001c0000000000f8 001c000000000000 000003ffcc6f7c88 0007740003e98000 0007931600000005 000792969b2ff7b8 Krnl Code: 0007931610326960: af000000 mc 0,0 0007931610326964: a7f4ff43 brc 15,00079316103267ea #0007931610326968: af000000 mc 0,0 >000793161032696c: a7f4ff3f brc 15,00079316103267ea 0007931610326970: e320f1000004 lg %r2,256(%r15) 0007931610326976: c0e53fd1b5f5 brasl %r14,000793168fd5d560 000793161032697c: a7f4fbb5 brc 15,00079316103260e6 0007931610326980: b904002b lgr %r2,%r11 Call Trace: smc_rx_splice+0xafc/0xe20 [smc] smc_rx_splice+0x756/0xe20 [smc]) smc_rx_recvmsg+0xa74/0xe00 [smc] smc_splice_read+0x1ce/0x3b0 [smc] sock_splice_read+0xa2/0xf0 do_splice_read+0x198/0x240 splice_file_to_pipe+0x7e/0x110 do_splice+0x59e/0xde0 __do_splice+0x11a/0x2d0 __s390x_sys_splice+0x140/0x1f0 __do_syscall+0x122/0x280 system_call+0x6e/0x90 Last Breaking-Event-Address: smc_rx_splice+0x960/0xe20 [smc] ---[end trace 0000000000000000]---	N/A	More Details
CVE-2025-40011	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: Fix null dereference in hdmi teardown pci_set_drvdata sets the value of pdev->driver_data to NULL, after which the driver_data obtained from the same dev is dereferenced in oaktrail_hdmi_i2c_exit, and the i2c_dev is extracted from it. To prevent	N/A	More Details

	this, swap these calls. Found by Linux Verification Center (linuxtesting.org) with Svacer.		
CVE-2025-40010	In the Linux kernel, the following vulnerability has been resolved: afs: Fix potential null pointer dereference in afs_put_server afs_put_server() accessed server->debug_id before the NULL check, which could lead to a null pointer dereference. Move the debug_id assignment, ensuring we never dereference a NULL server pointer.	N/A	More Details
CVE-2025-40009	In the Linux kernel, the following vulnerability has been resolved: fs/proc/task_mmu: check p->vec_buf for NULL When the PAGEMAP_SCAN ioctl is invoked with vec_len = 0 reaches pagemap_scan_backout_range(), kernel panics with null-ptr-deref: [44.936808] Oops: general protection fault, probably for non-canonical address 0xdfffffc0000000000: 0000 [#1] SMP DEBUG_PAGEALLOC KASAN NOPTI [44.937797] KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] [44.938391] CPU: 1 UID: 0 PID: 2480 Comm: reproducer Not tainted 6.17.0-rc6 #22 PREEMPT(none) [44.939062] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [44.939935] RIP: 0010:pagemap_scan_thp_entry.isra.0+0x741/0xa80 <snip registers, unreliable trace> [44.946828] Call Trace: [44.947030] <TASK> [44.949219] pagemap_scan_pmd_entry+0xec/0xfa0 [44.952593] walk_pmd_range.isra.0+0x302/0x910 [44.954069] walk_pud_range.isra.0+0x419/0x790 [44.954427] walk_p4d_range+0x41e/0x620 [44.954743] walk_pgd_range+0x31e/0x630 [44.955057] __walk_page_range+0x160/0x670 [44.956883] walk_page_range_mm+0x408/0x980 [44.958677] walk_page_range+0x66/0x90 [44.958984] do_pagemap_scan+0x28d/0x9c0 [44.961833] do_pagemap_cmd+0x59/0x80 [44.962484] __x64_sys_ioctl+0x18d/0x210 [44.962804] do_syscall_64+0x5b/0x290 [44.963111] entry_SYSCALL_64_after_hwframe+0x76/0x7e vec_len = 0 in pagemap_scan_init_bounce_buffer() means no buffers are allocated and p->vec_buf remains set to NULL. This breaks an assumption made later in pagemap_scan_backout_range(), that page_region is always allocated for p->vec_buf_index. Fix it by explicitly checking p->vec_buf for NULL before dereferencing. Other sites that might run into same deref-issue are already (directly or transitively) protected by checking p->vec_buf. Note: From PAGEMAP_SCAN man page, it seems vec_len = 0 is valid when no output is requested and it's only the side effects caller is interested in, hence it passes check in pagemap_scan_get_args(). This issue was found by syzkaller.	N/A	More Details
CVE-2025-40008	In the Linux kernel, the following vulnerability has been resolved: kmsan: fix out-of-bounds access to shadow memory Running sha224_kunit on a KMSAN-enabled kernel results in a crash in kmsan_internal_set_shadow_origin(): BUG: unable to handle page fault for address: ffffbc3840291000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 1810067 P4D 1810067 PUD 192d067 PMD 3c17067 PTE 0 Oops: 0000 [#1] SMP NOPTI CPU: 0 UID: 0 PID: 81 Comm: kunit_try_catch Tainted: G N 6.17.0-rc3 #10 PREEMPT(voluntary) Tainted: [N]=TEST Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.17.0-0-gb52ca86e094d-prebuilt.qemu.org 04/01/2014 RIP: 0010:kmsan_internal_set_shadow_origin+0x91/0x100 [...] Call Trace: <TASK> __msan_memset+0xee/0x1a0 sha224_final+0x9e/0x350 test_hash_buffer_overruns+0x46f/0x5f0 ? kmsan_get_shadow_origin_ptr+0x46/0xa0 ? __pfx_test_hash_buffer_overruns+0x10/0x10 kunit_try_run_case+0x198/0xa00 This occurs when memset() is called on a buffer that is not 4-byte aligned and extends to the end of a guard page, i.e. the next page is unmapped. The bug is that the loop at the end of kmsan_internal_set_shadow_origin() accesses the wrong shadow memory bytes when the address is not 4-byte aligned. Since each 4 bytes are associated with an origin, it rounds the address and size so that it can access all the origins that contain the buffer. However, when it checks the corresponding shadow bytes for a particular origin, it incorrectly uses the original unrounded shadow address. This results in reads from shadow memory beyond the end of the buffer's shadow memory, which crashes when that memory is not mapped. To fix this, correctly align the shadow address before accessing the 4 shadow bytes corresponding to each origin.	N/A	More Details
CVE-2025-40007	In the Linux kernel, the following vulnerability has been resolved: netfs: fix reference leak Commit 20d72b00ca81 ("netfs: Fix the request's work item to not require a ref") modified netfs_alloc_request() to initialize the reference counter to 2 instead of 1. The rationale was that the requet's "work" would release the second reference after completion (via netfs_{read,write}_collection_worker()). That works most of the time if all goes well. However, it leaks this additional reference if the request is released before the I/O operation has been submitted: the error code path only decrements the reference counter once and the work item will never be queued because there will never be a completion. This has caused outages of our whole server cluster today because tasks were blocked in netfs_wait_for_outstanding_io(), leading to deadlocks in Ceph (another bug that I will address soon in another patch). This was caused by a netfs_pgpriv2_begin_copy_to_cache() call which failed in fscache_begin_write_operation(). The leaked netfs_io_request was never completed, leaving `netfs_inode.io_count` with a positive value forever. All of this is super-fragile code. Finding out which code paths will lead to an eventual completion and which do not is hard to see: - Some functions like netfs_create_write_req() allocate a request, but will never submit any I/O. - netfs_unbuffered_read_iter_locked() calls netfs_unbuffered_read() and then netfs_put_request(); however, netfs_unbuffered_read() can also fail early before submitting the I/O request, therefore another netfs_put_request() call must be added there. A rule of thumb is that functions that return a `netfs_io_request` do not submit I/O, and all of their callers must be checked. For my taste, the whole netfs code needs an overhaul to make reference counting easier to understand and less fragile & obscure. But to fix this bug here and now and produce a patch that is adequate for a stable backport, I tried a minimal approach that quickly frees the request object upon early failure. I decided against adding a second netfs_put_request() each time because that would cause code duplication which obscures the code further. Instead, I added the function netfs_put_failed_request() which frees such a failed request synchronously	N/A	More Details

	under the assumption that the reference count is exactly 2 (as initially set by netfs_alloc_request() and never touched), verified by a WARN_ON_ONCE(). It then deinitializes the request object (without going through the "cleanup_work" indirection) and frees the allocation (with RCU protection to protect against concurrent access by netfs_requests_seq_start()). All code paths that fail early have been changed to call netfs_put_failed_request() instead of netfs_put_request(). Additionally, I have added a netfs_put_request() call to netfs_unbuffered_read() as explained above because the netfs_put_failed_request() approach does not work there.		
CVE-2025-34518	Ilevia EVE X1 Server firmware versions ≤ 4.7.18.0.eden contain a relative path traversal vulnerability in get_file_content.php that allows an attacker to read arbitrary files. Ilevia has declined to service this vulnerability, and recommends that customers not expose port 8080 to the internet.	N/A	More Details
CVE-2025-40005	In the Linux kernel, the following vulnerability has been resolved: spi: cadence-quadspi: Implement refcount to handle unbind during busy driver support indirect read and indirect write operation with assumption no force device removal(unbind) operation. However force device removal(removal) is still available to root superuser. Unbinding driver during operation causes kernel crash. This changes ensure driver able to handle such operation for indirect read and indirect write by implementing refcount to track attached devices to the controller and gracefully wait and until attached devices remove operation completed before proceed with removal operation.	N/A	More Details
CVE-2025-10869	Stored Cross-site Scripting (XSS) in Oct8ne Chatbot v2.3. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by injecting a malicious payload through the creation of a transcript that is sent by email. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user, through /Data/SaveInteractions.	N/A	More Details
CVE-2025-47901	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Microchip Time Provider 4100 allows OS Command Injection.This issue affects Time Provider 4100: before 2.5.	N/A	More Details
CVE-2025-47902	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Microchip Time Provider 4100 allows SQL Injection.This issue affects Time Provider 4100: before 2.5.	N/A	More Details
CVE-2025-55086	In NetXDuo version before 6.4.4, a networking support module for Eclipse Foundation ThreadX, in the DHCPV6 client there was an unchecked index extracting the server DUID from the server reply. With a crafted packet, an attacker could cause an out of memory read.	N/A	More Details
CVE-2025-8052	SQL Injection vulnerability in opentext Flipper allows SQL Injection. The vulnerability could allow a low privilege user to interact with the database in unintended ways and extract data by interacting with the HQL processor. This issue affects Flipper: 3.1.2.	N/A	More Details
CVE-2025-12001	Lack of application manifest sanitation could lead to potential stored XSS.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2018-25118	GeoVision embedded IP devices, confirmed on GV-BX1500 and GV-MFD1501, contain a remote command injection vulnerability via /PictureCatch.cgi that enables an attacker to execute arbitrary commands on the device. VulnCheck has observed this vulnerability being exploited in the wild as of 2025-10-19 08:55:13.141502 UTC.	N/A	More Details
CVE-2025-62658	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in The Wikimedia Foundation MediaWiki WatchAnalytics extension allows SQL Injection.This issue affects MediaWiki WatchAnalytics extension: 1.43, 1.44.	N/A	More Details
CVE-2025-62657	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation MediaWiki PageForms extension allows Stored XSS.This issue affects MediaWiki PageForms extension: 1.44.	N/A	More Details
CVE-2025-62656	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation MediaWiki GlobalBlocking extension allows Stored XSS.This issue affects MediaWiki GlobalBlocking extension: 1.43, 1.44.	N/A	More Details
CVE-2025-8053	Insufficient Granularity of Access Control vulnerability in opentext Flipper allows Exploiting Incorrectly Configured Access Control Security Levels. The vulnerability could allow a low privilege user to interact with the backend API without sufficient privileges. This issue affects Flipper: 3.1.2.	N/A	More Details
CVE-2025-8051	Path Traversal vulnerability in opentext Flipper allows Absolute Path Traversal. The vulnerability could allow a user to access files hosted on the server. This issue affects Flipper: 3.1.2.	N/A	More Details
CVE-2025-	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - LastModified Extension allows Stored XSS.This issue affects Mediawiki	N/A	More Details

62693	- LastModified Extension: from master before 1.39.		
CVE-2025-8049	Insufficient Granularity of Access Control vulnerability in opentext Flipper allows Exploiting Incorrectly Configured Access Control Security Levels. The vulnerability could allow a low-privilege user to elevate privileges within the application. This issue affects Flipper: 3.1.2.	N/A	More Details
CVE-2025-8048	External Control of File Name or Path vulnerability in opentext Flipper allows Path Traversal. The vulnerability could allow a user to submit a stored local file path and then download the specified file from the system by requesting the stored document ID. This issue affects Flipper: 3.1.2.	N/A	More Details
CVE-2025-62697	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in The Wikimedia Foundation Mediawiki - LanguageSelector Extension allows Code Injection.This issue affects Mediawiki - LanguageSelector Extension: from master before 1.39.	N/A	More Details
CVE-2025-62522	Vite is a frontend tooling framework for JavaScript. In versions from 2.9.18 to before 3.0.0, 3.2.9 to before 4.0.0, 4.5.3 to before 5.0.0, 5.2.6 to before 5.4.21, 6.0.0 to before 6.4.1, 7.0.0 to before 7.0.8, and 7.1.0 to before 7.1.11, files denied by server.fs.deny were sent if the URL ended with \ when the dev server is running on Windows. Only apps explicitly exposing the Vite dev server to the network and running the dev server on Windows were affected. This issue has been patched in versions 5.4.21, 6.4.1, 7.0.8, and 7.1.11.	N/A	More Details
CVE-2025-62700	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - MultiBoilerplate Extensionmaste allows Stored XSS.This issue affects Mediawiki - MultiBoilerplate Extensionmaste: from master before 1.39.	N/A	More Details
CVE-2025-62698	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - ExternalGuidance allows Stored XSS.This issue affects Mediawiki - ExternalGuidance: from master before 1.39.	N/A	More Details
CVE-2025-10678	NetBird VPN when installed using vendor's provided script failed to remove or change default password of an admin account created by ZITADEL. This issue affects instances installed using vendor's provided script. This issue may affect instances created with Docker if the default password was not changed nor the user was removed. This issue has been fixed in version 0.57.0	N/A	More Details
CVE-2025-11679	Out-of-bounds Read in lws_upng_emit_next_line in warmcat libwebsockets allows, when the LWS_WITH_UPNG flag is enabled during compilation and the HTML display stack is used, to read past a heap allocated buffer possibly causing a crash, when the user visits an attacker controlled website that contains a crafted PNG file with a big height dimension.	N/A	More Details
CVE-2025-62636	Rejected reason: Not used	N/A	More Details
CVE-2025-11678	Stack-based Buffer Overflow in lws_adns_parse_label in warmcat libwebsockets allows, when the LWS_WITH_SYS_ASYNC_DNS flag is enabled during compilation, to overflow the label_stack, when the attacker is able to sniff a DNS request in order to craft a response with a matching id containing a label longer than the maximum.	N/A	More Details
CVE-2025-62671	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - Cargo Extension allows Stored XSS.This issue affects Mediawiki - Cargo Extension: master.	N/A	More Details
CVE-2025-62670	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - FlexDiagrams Extension allows Stored XSS.This issue affects Mediawiki - FlexDiagrams Extension: master.	N/A	More Details
CVE-2025-62669	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in The Wikimedia Foundation Mediawiki - CentralAuth Extension allows Resource Leak Exposure.This issue affects Mediawiki - CentralAuth Extension: from master before 1.39.	N/A	More Details
CVE-2025-62668	Incorrect Default Permissions vulnerability in The Wikimedia Foundation Mediawiki - GrowthExperiments Extension allows Resource Leak Exposure.This issue affects Mediawiki - GrowthExperiments Extension: from master before 1.39.	N/A	More Details
CVE-2025-62667	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - GrowthExperiments Extension allows Stored XSS.This issue affects Mediawiki - GrowthExperiments Extension: from master before 1.39.	N/A	More Details
CVE-2025-62666	Allocation of Resources Without Limits or Throttling vulnerability in The Wikimedia Foundation Mediawiki - CirrusSearch Extension allows HTTP DoS.This issue affects Mediawiki - CirrusSearch Extension: from master before 1.43.	N/A	More Details
CVE-2025-	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - ImageRating Extension allows Stored XSS.This issue affects Mediawiki	N/A	More Details

62664	- ImageRating Extension: from master before 1.39.		
CVE-2025-62663	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - UploadWizard Extension allows Stored XSS.This issue affects Mediawiki - UploadWizard Extension: from master before 1.39.	N/A	More Details
CVE-2025-62662	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - AdvancedSearch Extension allows Stored XSS.This issue affects Mediawiki - AdvancedSearch Extension: from master before 1.39.	N/A	More Details
CVE-2025-62665	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation Mediawiki - Skin:BlueSky allows Stored XSS.This issue affects Mediawiki - Skin:BlueSky: from master before 1.39.	N/A	More Details
CVE-2025-62375	go-witness and witness are Go modules for generating attestations. In go-witness versions 0.8.6 and earlier and witness versions 0.9.2 and earlier the AWS attestor improperly verifies AWS EC2 instance identity documents. Verification can incorrectly succeed when a signature is not present or is empty, and when RSA signature verification fails. The attestor also embeds a single legacy global AWS public certificate and does not account for newer region specific certificates issued in 2024, making detection of forged documents difficult without additional trusted region data. An attacker able to supply or intercept instance identity document data (such as through Instance Metadata Service impersonation) can cause a forged identity document to be accepted, leading to incorrect trust decisions based on the attestation. This is fixed in go-witness 0.9.1 and witness 0.10.1. As a workaround, manually verify the included identity document, signature, and public key with standard tools (for example openssl) following AWS's verification guidance, or disable use of the AWS attestor until upgraded.	N/A	More Details
CVE-2025-62640	Rejected reason: Not used	N/A	More Details
CVE-2025-62639	Rejected reason: Not used	N/A	More Details
CVE-2025-62638	Rejected reason: Not used	N/A	More Details
CVE-2025-62637	Rejected reason: Not used	N/A	More Details
CVE-2025-11937	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - SecurePoll Extension allows Stored XSS.This issue affects Mediawiki - SecurePoll Extension: master.	N/A	More Details
CVE-2025-11832	Allocation of Resources Without Limits or Throttling vulnerability in Azure Access Technology BLU-IC2, Azure Access Technology BLU-IC4 allows Flooding.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-62410	In versions before 20.0.2, it was found that --disallow-code-generation-from-strings is not sufficient for isolating untrusted JavaScript in happy-dom. The untrusted script and the rest of the application still run in the same Isolate/process, so attackers can deploy prototype pollution payloads to hijack important references like "process" in the example below, or to hijack control flow via flipping checks of undefined property. This vulnerability is due to an incomplete fix for CVE-2025-61927. The vulnerability is fixed in 20.0.2.	N/A	More Details
CVE-2025-40004	In the Linux kernel, the following vulnerability has been resolved: net/9p: Fix buffer overflow in USB transport layer A buffer overflow vulnerability exists in the USB 9pfs transport layer where inconsistent size validation between packet header parsing and actual data copying allows a malicious USB host to overflow heap buffers. The issue occurs because: - usb9pfs_rx_header() validates only the declared size in packet header - usb9pfs_rx_complete() uses req->actual (actual received bytes) for memcpy This allows an attacker to craft packets with small declared size (bypassing validation) but large actual payload (triggering overflow in memcpy). Add validation in usb9pfs_rx_complete() to ensure req->actual does not exceed the buffer capacity before copying data.	N/A	More Details
CVE-2025-11677	Use After Free in WebSocket server implementation in lws_handshake_server in warmcat libwebsockets may allow an attacker, in specific configurations where the user provides a callback function that handles LWS_CALLBACK_HTTP_CONFIRM_UPGRADE, to achieve denial of service.	N/A	More Details
CVE-2025-8349	Cross-site Scripting (XSS) stored vulnerability in Tawk Live Chat. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by uploading a malicious PDF with JavaScript payload through the chatbot. The PDF is stored by the application and subsequently displayed without proper sanitisation when other users access it. This vulnerability can be exploited to steal sensitive user data, such as session	N/A	More Details

	cookies, or to perform actions on behalf of the user.		
CVE-2025-41028	A SQL Injection vulnerability has been found in Epsilon RH by Grupo Castilla. This vulnerability allows an attacker to retrieve, create, update and delete database via sending a POST request using the parameter 'sEstadoUsr' in '/epsilonnetws/WSAvisos.asmx'.	N/A	More Details
CVE-2025-61932	Lanscope Endpoint Manager (On-Premises) (Client program (MR) and Detection agent (DA)) improperly verifies the origin of incoming requests, allowing an attacker to execute arbitrary code by sending specially crafted packets.	N/A	More Details
CVE-2025-31342	An unrestricted upload of file with dangerous type vulnerability in the upload file function of Galaxy Software Services Corporation Vitals ESP Forum Module through 1.3 version allows remote authenticated users to execute arbitrary system commands via a malicious file.	N/A	More Details
CVE-2025-62577	ETERNUS SF provided by Fsas Technologies Inc. contains an incorrect default permissions vulnerability. A low-privileged user with access to the management server may obtain database credentials, potentially allowing execution of OS commands with administrator privileges.	N/A	More Details
CVE-2025-59419	Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.128.Final and 4.2.7.Final, the SMTP codec in Netty contains an SMTP command injection vulnerability due to insufficient input validation for Carriage Return (\r) and Line Feed (\n) characters in user-supplied parameters. The vulnerability exists in io.netty.handler.codec.smtp.DefaultSmtpRequest, where parameters are directly concatenated into the SMTP command string without sanitization. When methods such as SmtpRequests.rcpt(recipient) are called with a malicious string containing CRLF sequences, attackers can inject arbitrary SMTP commands. Because the injected commands are sent from the server's trusted IP address, resulting emails will likely pass SPF and DKIM authentication checks, making them appear legitimate. This allows remote attackers who can control SMTP command parameters (such as email recipients) to forge arbitrary emails from the trusted server, potentially impersonating executives and forging high-stakes corporate communications. This issue has been patched in versions 4.1.129.Final and 4.2.8.Final. No known workarounds exist.	N/A	More Details
CVE-2025-62381	sveltekit-superforms makes SvelteKit forms a pleasure to use. sveltekit-superforms v2.27.3 and prior are susceptible to a prototype pollution vulnerability within the parseFormData function of formData.js. An attacker can inject string and array properties into Object.prototype, leading to denial of service, type confusion, and potential remote code execution in downstream applications that rely on polluted objects. This vulnerability is fixed in 2.27.4.	N/A	More Details
CVE-2025-10576	Potential vulnerabilities have been identified in the audio package for certain HP PC products using the Sound Research SECOMN64 driver, which might allow escalation of privilege. HP is releasing updated audio packages to mitigate the potential vulnerabilities.	N/A	More Details
CVE-2025-10577	Potential vulnerabilities have been identified in the audio package for certain HP PC products using the Sound Research SECOMN64 driver, which might allow escalation of privilege. HP is releasing updated audio packages to mitigate the potential vulnerabilities	N/A	More Details
CVE-2025-40003	In the Linux kernel, the following vulnerability has been resolved: net: mscc: ocelot: Fix use-after-free caused by cyclic delayed work The origin code calls cancel_delayed_work() in ocelot_stats_deinit() to cancel the cyclic delayed work item ocelot->stats_work. However, cancel_delayed_work() may fail to cancel the work item if it is already executing. While destroy_workqueue() does wait for all pending work items in the work queue to complete before destroying the work queue, it cannot prevent the delayed work item from being rescheduled within the ocelot_check_stats_work() function. This limitation exists because the delayed work item is only enqueued into the work queue after its timer expires. Before the timer expiration, destroy_workqueue() has no visibility of this pending work item. Once the work queue appears empty, destroy_workqueue() proceeds with destruction. When the timer eventually expires, the delayed work item gets queued again, leading to the following warning: workqueue: cannot queue ocelot_check_stats_work on wq ocelot-switch-stats WARNING: CPU: 2 PID: 0 at kernel/workqueue.c:2255 __queue_work+0x875/0xaf0 ... RIP: 0010:__queue_work+0x875/0xaf0 ... RSP: 0018:ffff88806d108b10 EFLAGS: 00010086 RAX: 0000000000000000 RBX: 0000000000000101 RCX: 0000000000000027 RDX: 0000000000000027 RSI: 0000000000000004 RDI: ffff88806d123e88 RBP: ffffffff813c3170 R08: 0000000000000000 R09: ffffed100da247d2 R10: ffffed100da247d1 R11: ffff88806d123e8b R12: ffff88800c00f000 R13: ffff88800d7285c0 R14: ffff88806d0a5580 R15: ffff88800d7285a0 FS: 0000000000000000(0000) GS:ffff8880e5725000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fe18e45ea10 CR3: 0000000005e6c000 CR4: 00000000000006f0 Call Trace: <IRQ> ? kasan_report+0xc6/0xf0 ? __pfx_delayed_work_timer_fn+0x10/0x10 ? __pfx_delayed_work_timer_fn+0x10/0x10 call_timer_fn+0x25/0x1c0 __run_timer_base.part.0+0x3be/0x8c0 ? __pfx_delayed_work_timer_fn+0x10/0x10 ? rcu_sched_clock_irq+0xb06/0x27d0 ? __pfx___run_timer_base.part.0+0x10/0x10 ? try_to_wake_up+0xb15/0x1960 ? _raw_spin_lock_irq+0x80/0xe0 ? __pfx__raw_spin_lock_irq+0x10/0x10 tmigr_handle_remote_up+0x603/0x7e0 ? __pfx_tmigr_handle_remote_up+0x10/0x10 ? sched_balance_trigger+0x1c0/0x9f0 ? sched_tick+0x221/0x5a0 ? _raw_spin_lock_irq+0x80/0xe0 ? __pfx__raw_spin_lock_irq+0x10/0x10 ? tick_nohz_handler+0x339/0x440 ? __pfx_tmigr_handle_remote_up+0x10/0x10 __walk_groups.isra.0+0x42/0x150 tmigr_handle_remote+0x1f4/0x2e0 ? __pfx_tmigr_handle_remote+0x10/0x10 ? ktime_get+0x60/0x140 ?	N/A	More Details

	lapic_next_event+0x11/0x20 ? clockevents_program_event+0x1d4/0x2a0 ? hrtimer_interrupt+0x322/0x780 handle_softirqs+0x16a/0x550 irq_exit_rcu+0xaf/0xe0 sysvec_apic_timer_interrupt+0x70/0x80 </IRQ> ... The following diagram reveals the cause of the above warning: CPU 0 (remove) | CPU 1 (delayed work callback) mscc_ocelot_remove() | ocelot_deinit() | ocelot_check_stats_work() ocelot_stats_deinit() | cancel_delayed_work()| ... | queue_delayed_work() destroy_workqueue() | (wait a time) | __queue_work() //UAF The above scenario actually constitutes a UAF vulnerability. The ocelot_stats_deinit() is only invoked when initialization failure or resource destruction, so we must ensure that any delayed work items cannot be rescheduled. Replace cancel_delayed_work() with disable_delayed_work_sync() to guarantee proper cancellation of the delayed work item and ensure completion of any currently executing work before the workqueue is deallocated. A deadlock concern was considered: ocelot_stats_deinit() is called in a process context and is not holding any locks that the delayed work item might also need. Therefore, the use of the _sync() variant is safe here. This bug was identified through static analysis. To reproduce the issue and validate the fix, I simulated ocelot-swit ---truncated---		
CVE-2025-40002	In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Fix use-after-free in tb_dp_dprx_work The original code relies on cancel_delayed_work() in tb_dp_dprx_stop(), which does not ensure that the delayed work item tunnel->dprx_work has fully completed if it was already running. This leads to use-after-free scenarios where tb_tunnel is deallocated by tb_tunnel_put(), while tunnel->dprx_work remains active and attempts to dereference tb_tunnel in tb_dp_dprx_work(). A typical race condition is illustrated below: CPU 0 | CPU 1 tb_dp_tunnel_active() | tb_deactivate_and_free_tunnel()| tb_dp_dprx_start() tb_tunnel_deactivate() | queue_delayed_work() tb_dp_activate() | tb_dp_dprx_stop() | tb_dp_dprx_work() //delayed worker cancel_delayed_work() | tb_tunnel_put(tunnel); | | tunnel = container_of(...); //UAF | tunnel-> //UAF Replacing cancel_delayed_work() with cancel_delayed_work_sync() is not feasible as it would introduce a deadlock: both tb_dp_dprx_work() and the cleanup path acquire tb->lock, and cancel_delayed_work_sync() would wait indefinitely for the work item that cannot proceed. Instead, implement proper reference counting: - If cancel_delayed_work() returns true (work is pending), we release the reference in the stop function. - If it returns false (work is executing or already completed), the reference is released in delayed work function itself. This ensures the tb_tunnel remains valid during work item execution while preventing memory leaks. This bug was found by static analysis.	N/A	More Details
CVE-2025-40001	In the Linux kernel, the following vulnerability has been resolved: scsi: mvsas: Fix use-after-free bugs in mvs_work_queue During the detaching of Marvell's SAS/SATA controller, the original code calls cancel_delayed_work() in mvs_free() to cancel the delayed work item mwq->work_q. However, if mwq->work_q is already running, the cancel_delayed_work() may fail to cancel it. This can lead to use-after-free scenarios where mvs_free() frees the mvs_info while mvs_work_queue() is still executing and attempts to access the already-freed mvs_info. A typical race condition is illustrated below: CPU 0 (remove) | CPU 1 (delayed work callback) mvs_pci_remove() | mvs_free() | mvs_work_queue() cancel_delayed_work() | kfree(mvi) | | mvi-> // UAF Replace cancel_delayed_work() with cancel_delayed_work_sync() to ensure that the delayed work item is properly canceled and any executing delayed work item completes before the mvs_info is deallocated. This bug was found by static analysis.	N/A	More Details
CVE-2025-62380	mailgen is a Node.js package that generates responsive HTML e-mails for sending transactional mail. Mailgen versions through 2.0.31 contain an HTML injection vulnerability in plaintext emails generated with the generatePlaintext method when user generated content is supplied. The plaintext generation code attempts to strip HTML tags using a regular expression and then decodes HTML entities, but tags that include certain Unicode line separator characters are not matched and removed. These encoded tags are later decoded into valid HTML content, allowing unexpected HTML to remain in output intended to be plaintext. Projects are affected if they call Mailgen.generatePlaintext with untrusted input and then render or otherwise process the returned string in a context where HTML is interpreted. This can lead to execution of attacker supplied script in the victim’s browser. Version 2.0.32 fixes the issue.	N/A	More Details
CVE-2025-48044	Incorrect Authorization vulnerability in ash-project ash allows Authentication Bypass. This vulnerability is associated with program files lib/ash/policy/policy.ex and program routines 'Elixir.Ash.Policy.Policy':expression/2. This issue affects ash: from pkg:hex/ash@3.6.3 before pkg:hex/ash@3.7.1, from 3.6.3 before 3.7.1, from 79749c2685ea031ebb2de8cf60cc5edced6a8dd0 before 8b83efa225f657bfc3656ad8ee8485f9b2de923d.	N/A	More Details